



VULNERABILITY SCANNER DETECTION AND PENETRATION TESTING EXPLOIT COVERAGE

Introduction

Vulnerability scanning and penetration testing have become mandatory components of network security programs. While vulnerability scanning provides the identification and reporting of known threats, it is vital to identify which vulnerabilities can be exploited or attacked because these are the greatest threats to networks. Knowing which vulnerabilities are exploitable provides a starting point for prioritizing remediation and for proving the existence of the problem through penetration testing—attempting to penetrate the network by simulating the actions of an attacker.

While the IT security consultant has multiple choices of downloadable vulnerability scanners, only a few penetration testing tools are available. This paper summarizes the comparative analysis of several of the vulnerability scanners and penetration testing tools that are available. The complete details of this analysis including vendor by exploit and vulnerability can be requested at Austin@saintcorporation.com.

A Comparative Analysis

The data in this analysis is referenced by CVE (Common Vulnerabilities and Exposures) Identifiers. CVE Identifiers are unique, common identifiers for publicly known information security vulnerabilities and are used by the industry as a standard method for identifying vulnerabilities.

A total of 555 exploitable vulnerabilities were discovered that had CVE Identifiers from the NVD (National Vulnerability Database). NVD is the U.S. government repository of standards based vulnerability management data. NVD is a product of the NIST Computer Security Division, Information Technology Laboratory, and is sponsored by the Department of Homeland Security's National Cyber Security Division.

In addition to CVE Identifiers, the following identifiers and cross references are also included in the attached detailed report:

- BID# – Security Focus Bugtraq ID provides an identification number, detailed discussion, and announcements for computer security vulnerabilities.
- OSVDB# – Open Source Vulnerability Database provides an identification number and is an open source database for providing information on security vulnerabilities.



- OVAL# – Open Vulnerability and Assessment Language community standard providing security details as it relates to vulnerable configurations within this research.
- CWE# – Common Weakness Enumeration is a formal list of software weaknesses for describing software security flaws in architecture, design, and code. CWE provides a baseline standard for identification, mitigation and prevention efforts in addition to providing a common identifier.
- CVSS – Common Vulnerability Scoring System is an open framework for communicating the characteristics and impacts of vulnerabilities. CVSS serves as a standard measurement system for calculating vulnerability impact.

While most of the products included in this analysis provide their own severity ranking for each vulnerability and/or exploit, the CVSS scoring system is being used since it has become the industry standard for determining the criticality of a vulnerability. CVSS scores range from 0-10, with 10 being the greatest threat. This provides a more granular severity ranking than the high, medium, and low rankings traditionally provided by vulnerability scanners. The ranking and calculation of CVSS scores are described at: <http://nvd.nist.gov/cvss.cfm?calculator&version=2>

While the CVSS scoring system provides a better ranking of criticality, it is still difficult for administrators to assess the real impact of vulnerabilities on a network and know where to begin remediation efforts. With the daunting number of new vulnerabilities that appear each day, it is imperative that vulnerability scanners provide a means for customers to detect which vulnerabilities are potentially exploitable by attackers.

Findings – Vulnerability Scanners

The vulnerability scanners included in this analysis follow:

- SAINT[®] Scanner
- Tenable Network Security –Nessus[®] Scanner
- eEye Retina[®] Scanner
- Nexpose[™] Rapid7 Scanner
- GFI Languard Scanner

SAINT and Nessus appear to be the only heterogeneous scanners with an emphasis on detecting vulnerabilities that can be exploited on a broad range of systems and devices, including both IPv4 and IPv6 protocols. Retina, Rapid7, and GFI focus mostly on Windows related checks, although light coverage is provided for some Linux, Mac, and Unix operating systems and applications. SAINT is the only vulnerability scanner that is capable of launching exploits (penetration testing) and allowing the user to gather evidence of a vulnerability.

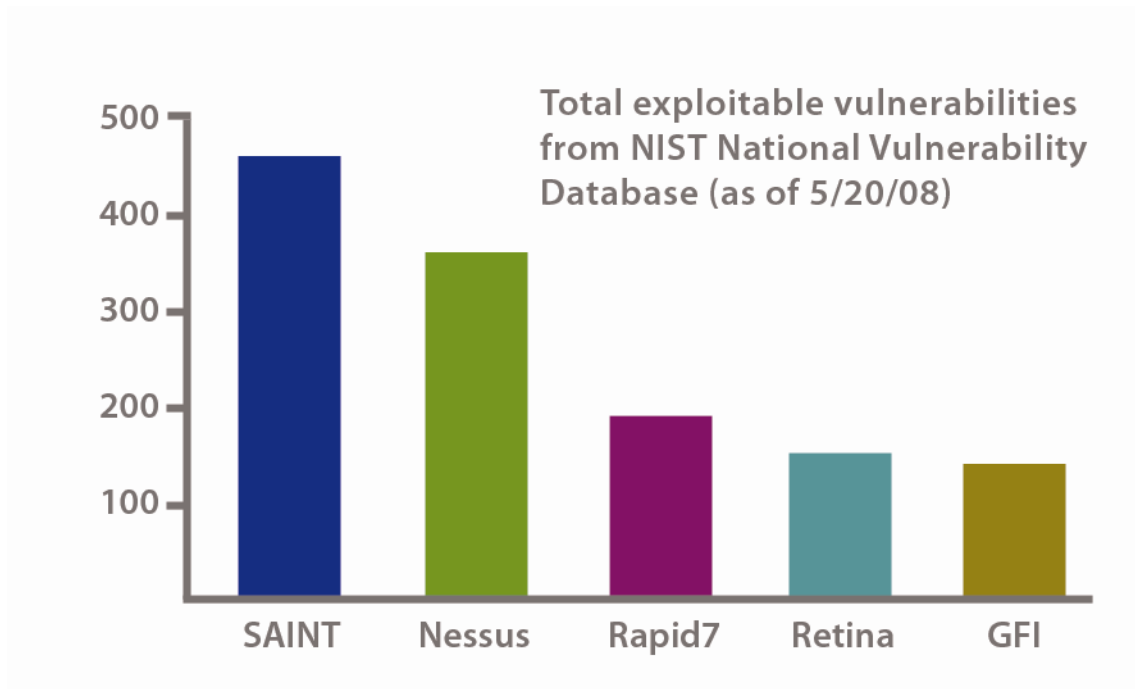


The number of exploitable vulnerabilities for each year from 1999-2008 (based on the date the CVE was published) detected by each scanner is shown in the table below (as of 5/20/2008).

Number of Exploitable Vulnerabilities from NVD Detected

CVE Published Year	SAINT [®] Scanner	Nessus [®] Scanner	Nexpose [™] Rapid 7 Scanner	Retina [®] Scanner	GFI Scanner
2008	36	24	12	16	8
2007	131	84	33	31	26
2006	89	75	43	21	31
2005	78	60	25	18	21
2004	51	48	26	17	18
2003	30	27	27	18	18
2002	18	19	16	17	12
2001	15	12	9	9	9
2000	5	6	4	5	3
1999	5	5	2	3	1
1999-2008 TOTAL	458	360	197	155	147

The total exploitable vulnerabilities are depicted in the bar chart below:



Findings – Penetration testing tools

Penetration testing is the next step in proactive network security. Once the exploitable vulnerabilities have been identified, the network administrator can then assess the security of the network by attempting to penetrate it by simulating the actions of an attacker. The penetration test can gather evidence of a vulnerability including reading and writing files, executing commands, or taking screen shots. Penetration testing focuses on high-severity vulnerabilities and there are no false positives.

The following penetration testing tools are included in this research:

- SAINTexploit™
- Core Impact
- Metasploit™

An exploit is a program designed to demonstrate the presence of a specific vulnerability usually by executing commands on the target. Penetration testing works by running a series of exploits that are chosen based on the target's operating system and running services.

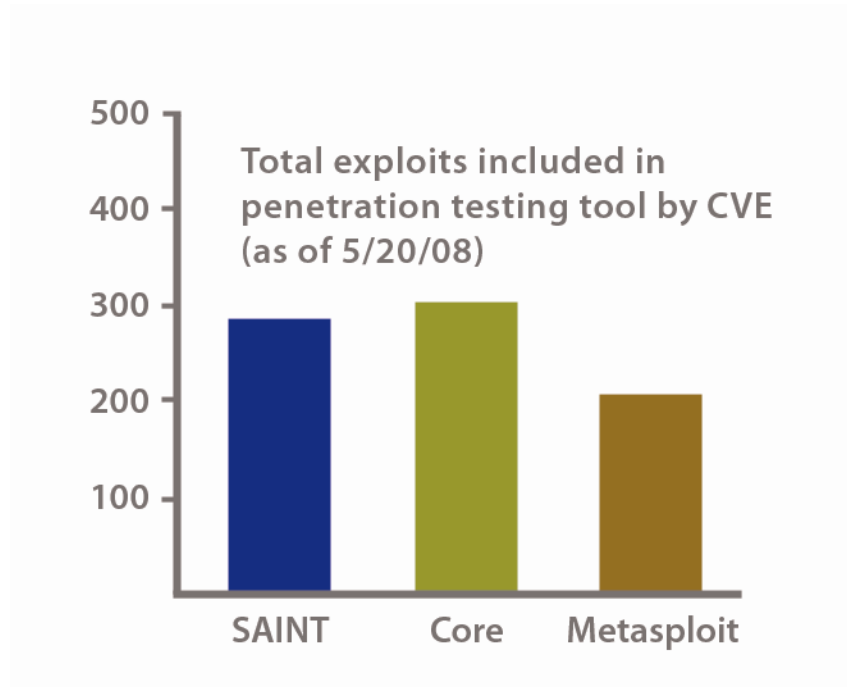
The number of exploits (by CVE Identifier) available in each penetration testing tool (based on the date the CVE was published) is shown in the table below (as of 5/20/08):



Total Exploits from NVD Included in Penetration Testing Tool

CVE Published Year	SAINTexploit™	Core Impact	Metasploit™
2008	26	29	2
2007	87	93	45
2006	64	47	51
2005	57	33	49
2004	24	30	30
2003	9	31	19
2002	6	23	6
2001	6	14	8
2000	1	5	1
1999	2	3	3
1999–2008 TOTAL	282	308	214

The total exploits are depicted in the bar chart below:



Conclusion

New vulnerabilities are announced every day and a growing percentage of new vulnerabilities are exploitable. A vulnerability scanner that integrates exploits and penetration testing provides the ideal solution, saving both time and money. SAINTEC is the only integrated vulnerability scanner and penetration testing tool available.

SAINTEC provides more than just vulnerability coverage. Vulnerability scanners are good for identifying potential problems in the network, detecting security flaws, providing a snapshot of risk exposure, and detailing remedies. SAINTEC is the only product that goes further to identify which vulnerabilities are the greatest threats to your network—the vulnerabilities that are exploitable—and lets you perform penetration testing from the same easy-to-use interface as the vulnerability scanner.

SAINTEC provides more than just patching—you need to know how and where your network can be attacked. Few organizations have the resources to correct all of their network vulnerabilities. Therefore, it is important to identify the greatest threats and tackle those first. By identifying which vulnerabilities are exploitable, SAINTEC shows you where to begin your remediation efforts. Furthermore, penetration testing is increasingly becoming a more common requirement for government compliance.

As shown in the comparative analysis results above, SAINTEC is a top competitor in both vulnerability scanning and penetration testing. With over 10 years as a leading vulnerability scanner, and integrated penetration testing, SAINTEC provides the greatest coverage for protecting your network.