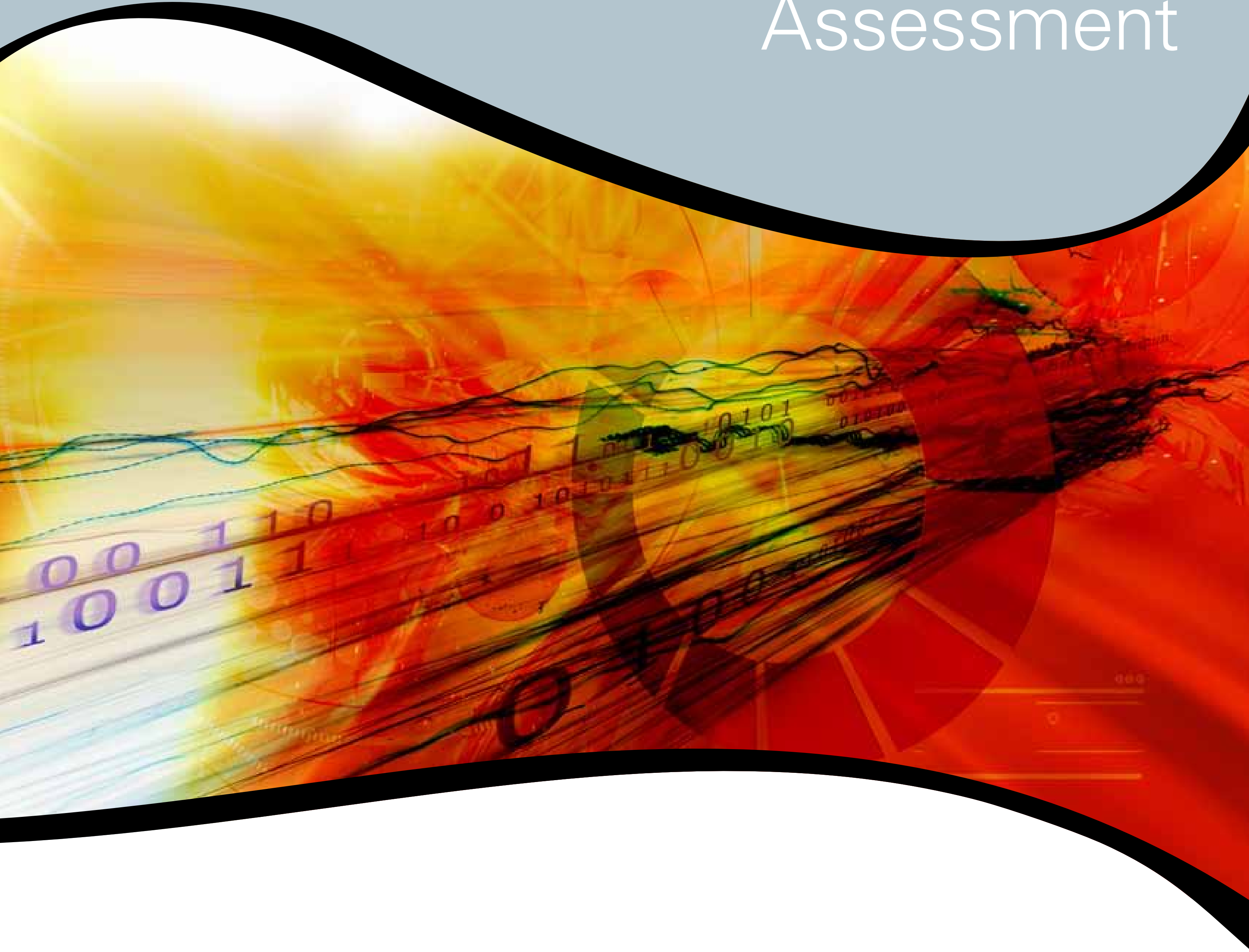
Tools

Information Assurance
Tools Report

Sixth Edition
May 2, 2011

Vulnerability Assessment



IATAC

Distribution Statement A

Approved for public release; distribution is unlimited.

REPORT DOCUMENTATION PAGE	*Form Approved* *OMB No. 0704-0188*

1. REPORT DATE *(DD-MM-YYYY)* 05-02-2011	**2. REPORT TYPE** Report	**3. DATES COVERED** *(From - To)* 05-02-2011

4. TITLE AND SUBTITLE Information Assurance Tools Report – Vulnerability Assessment. Sixth Edition	***5a. CONTRACT NUMBER*** SPO700-98-D-4002-0380
	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S) Revision by Karen Mercedes Goertzel, with contributions from Theodore Winograd	***5d. PROJECT NUMBER***
	5e. TASK NUMBER N/A
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) IATAC 13200 Woodland Park Road Herndon, VA 20171	***8. PERFORMING ORGANIZATION REPORT NUMBER***
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) Defense Technical Information Center 8725 John J. Kingman Road, Suite 0944 Fort Belvoir, VA 22060-6218	***10. SPONSOR/MONITOR'S ACRONYM(S)***
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT
A/ Distribution Approved for public release; distribution is unlimited.

13. SUPPLEMENTARY NOTES
IATAC is operated by Booz Allen Hamilton, 8283 Greensboro Drive, McLean, VA 22102

14. ABSTRACT

This Information Assurance Technology Analysis Center (IATAC) report provides an index of automated vulnerability assessment tools. It summarizes pertinent information, providing users a brief description of available automated vulnerability assessment tools and contact information for each. IATAC does not endorse, recommend, or evaluate the effectiveness of any specific tool. The written descriptions are based solely on vendors' claims and Security Content Automation Protocol (SCAP) Product Validation Report contents and are intended only to highlight the capabilities and features of each automated vulnerability assessment product.

15. SUBJECT TERMS
IATAC Collection, Firewall

16. SECURITY CLASSIFICATION OF:			***17. LIMITATION OF ABSTRACT***	***18. NUMBER OF PAGES***	***19a. NAME OF RESPONSIBLE PERSON*** Tyler, Gene
a. REPORT UNCLASSIFIED	***b. ABSTRACT*** UNCLASSIFIED	***c. THIS PAGE*** UNCLASSIFIED	None	142	**19b. TELEPHONE NUMBER** *(include area code)* 703-984-0775

Table of Contents

Network Scanners

Host Scanners

Database Scanners

Web Application Scanners

Multilevel Scanners

Automated Penetration Test Tools

Vulnerability Scan Consolidators

SECTION 1 ▶ **Introduction**

The Information Assurance Technology Analysis Center (IATAC) provides the Department of Defense (DOD) with emerging scientific and technical information to support information assurance (IA), cyber security, and defensive information operations (IO). IATAC is one of ten Information Analysis Centers (IACs) sponsored by DOD and managed by the Defense Technical Information Center (DTIC). IACs are formal organizations chartered by DOD to facilitate the use of existing scientific and technical information. Each IAC is staffed by scientists, engineers, and information specialists. IACs establish and maintain comprehensive knowledge bases that include historical, technical, scientific, and other data and information, which are collected worldwide. Information collections span a wide range of unclassified, limited-distribution, and classified information appropriate to the requirements of sponsoring technical communities. IACs also collect, maintain, and develop analytical tools and techniques, including databases, models, and simulations.

IATAC's mission is to provide DOD with a central point of access for information on emerging technologies in IA and cyber security. These include technologies, tools, and associated techniques for detection of, protection against, reaction to, and recovery from information warfare and cyber attacks that target information, information-based processes, information systems, and information technology. Specific areas of study include IA and cyber security threats and vulnerabilities, scientific and technological research and development, and technologies, standards, methods, and tools through which IA and cyber security objectives are being or may be accomplished.

As an IAC, IATAC's basic services include collecting, analyzing, and disseminating IA scientific and technical information; responding to user inquiries; database operations; current awareness activities [*e.g.,* the *IAnewsletter, IA Digest, Cyber Events Calendar, Technical Inquiry Production Report (TIPR), IATAC Web site (including a chart showing all DOD IA policies),* and *IA Research Update*]; and publishing State-of-the-Art Reports, Critical Review and Technology Assessments, and IA Tools Reports.

The IA Tools Database is one of the knowledge bases maintained by IATAC. This knowledge base contains information on a wide range of intrusion detection, vulnerability analysis, firewall applications, and antimalware tools. Information for the IA Tools Database is obtained from information available *via* open-source methods, including direct interface with various agencies, organizations, and vendors. Periodically, IATAC publishes a Tools Report to summarize and elucidate a particular subset of the tools information in the IATAC IA Tools Database that addresses a specific IA or cyber security challenge. To ensure applicability to the community that performs research and development (R&D) for the warfighter (and specifically Program Executive Officers and Program Managers in the R&D community), the topic areas for IA Tools Reports are solicited from the DOD IA community or based on IATAC's careful ongoing observation and analysis of the IA and cyber security tools and technologies about which those community expresses a high level of interest.

Inquiries about IATAC capabilities, products, and services may be addressed to:

Gene Tyler, Director
13200 Woodland Park Road, Suite 6031
Herndon, VA 20171
Phone: 703/984-0775
Fax: 703/984-0773
Email: *iatac@dtic.mil*
URL: *http://iac.dtic.mil/iatac*
SIPRNET: *https://iatac.dtic.mil*

1.1 Purpose

This IA Tools Report is intended to serve as a reference catalogue of current vulnerability assessment tools found in the IATAC Tools Database and available as commercial products, freeware, or open source software and were reviewed during the period 2 February – 2 May 2011 and represents a best effort to capture all/relevant tools and corresponding information. To provide a context for this catalogue, Section 2 of this Report provides a brief background on information and communications technology (ICT) system and network vulnerability assessment, with a focus on the role of automation and tools. This overview is followed by the extensive listing of the tools themselves.

Each entry in the tools catalogue summarizes the characteristics and capabilities of the vulnerability assessment tool, and identifies some key attributes, such as level of ICT infrastructure at which the tool operates (*e.g.,* network, operating system, application), format in which the tool is distributed (hardware appliance or software), whether the tool has been validated as conforming to the National Institute of Standards and Technology (NIST) Security Content Automation Protocol (SCAP) standard, and other information that could be helpful to readers looking to do an initial downselect of vulnerability assessment tools that are most likely to satisfy their requirements, and that warrant further investigation. Following the tools catalogue (which comprises the bulk of this Report), Section 4 identifies a number of vulnerability assessment tools whose capabilities are offered under an on-demand "software as a service" (SaaS) delivery model, since SaaS vulnerability assessment options are becoming increasingly prevalent. Not included are vulnerability assessment services offered under more traditional managed service outsourcing or consulting contracts.

The information about individual tools included in this Report is intended only to highlight the capabilities and features of each tool. Research for this Report did not include any qualitative evaluation of the tools' quality or efficacy. The inclusion of any tool in this Report does not constitute an endorsement or recommendation of that tool by IATAC, DTIC, or DOD. The tool descriptions in Section 3 are based solely on information about the tools discovered on their suppliers' Web sites augmented, in some cases, by information found in the NIST National Vulnerability Database (NVD) SCAP-Validated Products List or the Open Vulnerability Assessment Language (OVAL®), Common Vulnerabilities and Exposures (CVE®), or Common Weakness Enumeration (CWE) Products Lists published by The MITRE Corporation. It is left to the readers of this Report to perform the additional research or evaluations required for them to determine which tool(s), if any, best satisfy their requirements. Technical questions concerning this report may be addressed to *iatac@dtic.mil.*

1.2 Report Organization

This report is organized into five sections and two appendix(ices), as follows:

Section 1	Introduction to IATAC, purpose, organization, scope, and assumptions for this Report.
Section 2	Overview of automated vulnerability assessment tools—including descriptions of the various types of automated vulnerability assessment tools currently available, a discussion of the attributes that distinguish vulnerability assessment tools from other tools used in ICT and network vulnerability and risk management, and a discussion of relevant standards being mandated for vulnerability assessment automation.
Section 3	Catalogue of descriptions of current vulnerability assessment tools, categorized by type. The preface to this catalogue provides a legend to the information provided about each tool in its catalogue entry, and a description of the research methodology used to compile the catalogue entries.
Section 4	Representative listing of vulnerability assessment tools made available via on-demand SaaS offerings.
Section 5	List of resources to additional detailed information about IT and network vulnerability assessment and assessment tools.
Appendix A	Abbreviations, acronyms, and glossary.
Appendix B	List of obsolete open source vulnerability assessment tools of possible interest.

1.3 Scope

This Report focuses on vulnerability assessment tools, which this Report defines as: *automated tools the primary purpose of which is to:*

- *Proactively detect vulnerabilities in elements of deployable or deployed information systems and/or networks before those vulnerabilities are exploited (by contrast with tools that are used to forensically analyze such systems/networks after an intrusion or compromise);*
- *Analyze all detected vulnerabilities to assess their potential impact on the security posture of the system/network element in which the vulnerabilities are found, and quantify the level of risk that impact poses on the overall system/network.*

From now on, the system and network elements assessed by a tool will be referred to as the targets of that tool.

A number of other types of automated, semi-automated, and manual process-assistive tools exist that can be, and often are, used to find and/or analyze vulnerabilities in information systems and networks. However, in all cases these tools deviate from our definition of a vulnerability assessment tool in some way, and thus are considered out of scope for this Report. Such out-of-scope tools include:

- **Tools for manual security testing of deployable/ deployed targets**—Tools such as proxies, fuzzers, fault injectors, and other manual penetration testing tools are considered out of scope because they are not automated, and require major human intervention to be useful, and thus do not satisfy the "automated" criterion for vulnerability assessment tools. Also they are very narrow in focus and/or limited in capability, which renders them only marginally useful, on their own, for performing holistic vulnerability detection.

Note, however, that several suppliers distribute automated penetration testing tool suites and frameworks that combine multiple narrow-focus security/penetration testing tools with multiple non-security analysis tools (of the type described below, and considered out of scope), integrate those tools through a central management "dashboard", and automate them—or at least provide the user (tester) with the means to automate them—through scripting of test scenarios and predefinition of test data/payloads. These automated penetration (pen) testing tool suites provide many of the capabilities found in active vulnerability scanners. And not only are many of them being extensively automated, but their suppliers have (re)designed to clarify and simplify their user interfaces and overall functionality, thus increasing their potential utility to analysts and auditors who are not expert penetration testers. For this reason, automated pen testing tool suites/frameworks are considered in scope for this Report.

- **Tools whose primary purpose is not location, analysis, and assessment of vulnerabilities**—Even if the primary function of a tool coincidentally reveals the presence of vulnerabilities, or enables the user to either infer the presence of vulnerabilities or to assume the adequate mitigation of vulnerabilities, it is out of scope because that is not its primary purpose. Such tools include:
  - **Compliance validation tools**—The main purpose of compliance validation tools is to verify a target's compliance with some sort of regulation, policy, or guideline, such as a security configuration guideline, [1] a policy or regulation mandating a certain set of security controls, [2] or a set of patch management requirements. [3] Compliance tools

[1] Well-known Government examples of secure configuration guides include the U.S. Government Configuration Baseline (USGCB), formerly known as the Federal Desktop Core Configuration (FDCC), the Defense Information Systems Agency (DISA) Secure Technical Implementation Guides (STIGs), and the National Security Agency (NSA) Security Configuration Guides.

[2] Familiar examples of which include DOD Instruction (DODI) 8500.2, "Information Assurance (IA) Implementation"; NIST Special Publication (SP) 800-53, "Recommended Security Controls for Federal Information Systems" (required for compliance with the Federal Information Security Management Act [FISMA]), and the Payment Card Industry Data Security Standard (PCI DSS).

[3] For example, the patch management requirements of the DOD IA Vulnerability Alert (IAVA) process.

are not vulnerability assessment tools, however, because they do not seek the presence of vulnerabilities. Instead, they are predicated on the assumption that if a target complies with the relevant mandated security configuration attributes, security controls, and software patches, its vulnerabilities will have been sufficiently mitigated. The problem inherent with this assumption is that at any point in time, patches, secure configurations, and security controls can only mitigate vulnerabilities known to or anticipated by the authors of those policies, regulations, and guidelines. Which leaves unknown and novel vulnerabilities unmitigated. The threat landscape will always evolve and expand faster than policies, guidelines, and regulations can be updated, or patches written, tested, and distributed. For this reason, more direct means for locating and mitigating vulnerabilities must augment the verification of compliance with security configurations, controls, and patches. For all these reasons, compliance validation tools are out of scope for this Report.

- **Continuous monitoring tools and intrusion detection systems (IDS)**—The main purpose of these tools is to detect changes in a system's behavior, or in the patterns of network traffic payloads or application data inbound to or outbound from the target, that could indicate either the immediate presence of attack activity, or the results or byproducts of attack activity. Such behavior or traffic changes often have the result of revealing previously unknown vulnerabilities and/or causing new vulnerabilities to emerge. In addition, the user of the tool can often infer from the success of a given attack that a previously unknown (or known but unmitigated) vulnerability or vulnerabilities had to have been present to be exploited by the attacker. However, revelation/inference of vulnerabilities is only a byproduct of the tools' main purpose, which is to reveal the attack indicators and patterns; moreover, any vulnerabilities they do reveal do not become known until after they have been exploited. Thus, such tools are out of scope.
- **Vulnerability mitigation tools**—While the use of tools such as patching tools and configuration lock-down scripts strongly suggests that vulnerabilities must be present that need mitigation, such tools do not seek, analyze, or assess those vulnerabilities, and are thus out of scope.
- **General network and operating system analysis tools and scanners**—Utilities and tools such as host, finger, Nmap, Ethereal, NetScanTools, Wireshark, *etc.*, are used in examining and understanding the attributes, architecture, configuration, or operation of a target. However, they do not explicitly detect or analyze/assess vulnerabilities in that target, and are thus out of scope.
- **Developer security testing tools**—Tools intended for use by application or system developers, testers, or integrators to detect and analyze flaws, defects, and weaknesses in the architecture, design, or code of a target before that target is deployable, *e.g.,* during its development life cycle. An example of such a tool is a static source code analyzer. Such tools are out of scope because they are not intended to be used on deployable or deployed systems or components; in most cases it would be impractical or even impossible to use them on deployable/deployed systems.
- **Known-malicious intrusion and monitoring tools**—This Report excludes individual "black hat" tools, such as sniffers, spyware, keystroke loggers, bots, and Trojan Horse programs that are designed by hackers to help them find vulnerabilities to exploit. However there are a number of vulnerability assessment tools of which sniffers and other "non-intrusive" (*i.e.,* surreptitious) monitoring agents are legitimate components. It is not possible to determine the original pedigree of all such sniffers/agents; in the case of some open source tools, especially automated penetration testing tool suites, it is possible that some of their components did start out as hacker-originated tools, but have been turned to "white hat" use.

- **Obsolete tools**—By "obsolete", we mean tools that have not been updated since 31 December 2008 and/or which do not appear to be currently supported by their suppliers (vendors or open source developers). This said, some open source tools are so widely used and highly thought of that Appendix B lists them for information purposes—including Uniform Resource Locators (URLs) to their distribution pages on the Web.

1.4 Assumptions

The authors have written this IA Tools Report with the following assumptions about the reader's knowledge. The reader is presumed to be familiar with the basic concepts of ICT system and infrastructure security risk management, including vulnerability management and vulnerability assessment. Readers who lack familiarity with any of these concepts are encouraged to consult some or all of the following resources before reading the remainder of this Report.

Suggested Resources on Security Risk Management

- NIST Special Publication (SP) 800-30, "Risk Management Guide for Information Technology Systems", July 2002. *http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf* (accessed 29 April 2011).
- NIST SP 800-37, "Guide for Applying the Risk Management Framework to Federal Information Systems, Revision 1, February 2010. *http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf* (accessed 29 April 2011).
- NIST SP 800-39, "Managing Information Security Risk: Organization, Mission, and Information System View", March 2011. *http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf* (accessed 29 April 2011).
- Department of Homeland Security. "Continuous Asset Evaluation, Situational Awareness, and Risk Scoring Reference Architecture Report (CAESARS)". *http://www.dhs.gov/files/publications/gc_1285952885143.shtm* (accessed 29 April 2011).

Suggested Resources on Vulnerability Management

- NIST SP 800-40, "Creating a Patch and Vulnerability Management Program", Version 2.0, November 2005. *http://csrc.nist.gov/publications/nistpubs/800-40-Ver2/SP800-40v2.pdf* (accessed 29 April 2011).
- Derek Isaacs. "DOD IAVA [IA Vulnerability Alert] Management", ISSA [4] Journal, August 2006. *http://www.issa.org/Library/Journals/2006/August/Isaacs%20-%20IAVA%20Management.pdf* (accessed 29 April 2011).
- Cathleen Brackin. "Vulnerability Management: Tools, Challenges and Best Practices", System Administration Networking, and Security (SANS) Reading Room, 15 October 2003. *http://www.sans.org/reading_room/whitepapers/threats/vulnerability-management-tools-challenges-practices_1267* (accessed 29 April 2011).
- Mark Nicolett. "How to Develop and Effective Vulnerability Management Process", Gartner Research Report Number G00124126, 1 March 2005. *http://www85.homepage.villanova.edu/timothy.ay/DIT2160/IdMgt/how_to_develop_.pdf* (accessed 29 April 2011).

Suggested Resources on Vulnerability Assessment

- NIST SP 800-115, "Technical Guide to Information Security Testing and Assessment", September 2008. *http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf* (accessed 29 April 2011).
- Houghton, Ken. "Vulnerabilities and Vulnerability Scanning". SANS Institute Reading Room, 2003. *http://www.sans.org/reading_room/whitepapers/threats/vulnerabilities-vulnerability-scanning_1195* (accessed 28 April 2011).
- Cole, Ph.D., Eric, SANS Institute. "Five Axioms of Vulnerability Scanning". *http://www.youtube.com/watch?v=kqzYZBcU75Y* (accessed 28 April 2011).

Additional resources are listed in Section 5.

[4] Information System Security Association

SECTION 2 ▶ Background

2.1 The Role of Vulnerability Assessment in ICT System Risk Management

According to NIST SP 800-37, vulnerability analysis and assessment is an important element of each required activity in the NIST Risk Management Framework (RMF). This RMF comprises six steps, into each of which vulnerability analysis and assessment is to be integrated:

- Step 1: Categorize Information Systems.
- Step 2: Select Security Controls.
- Step 3: Implement Security Controls.
- Step 4: Assess Security Controls.
- Step 5: Authorize Information Systems.
- Step 6: Monitor Security Controls.

Vulnerability assessment tools help in that integration, by automating the detection, identification, measurement, and understanding of vulnerabilities found in ICT components at various levels of a target ICT system or infrastructure. A vulnerability is an attribute or characteristic of a component that can be exploited by either an external or internal agent (hacker or malicious insider) to violate a security policy of (narrow definition) or cause a deleterious result in (broad definition) either the component itself, and/or the system or infrastructure of which it is a part. Such "deleterious results" include unauthorized privilege escalations or data/resource accesses, sensitive data disclosures or privacy violations, malicious code insertions, denials of service, *etc.*

Such tools are often referred to as vulnerability *scanners,* because their means of vulnerability detection is to scan targets (usually network services and nodes, and the operating systems, databases, and/or Web applications residing on those nodes) in an attempt to detect known, and in some cases also unknown, vulnerabilities.

2.2 How Vulnerability Assessment Tools Work

Vulnerability assessment tools generally work by attempting to automate the steps often employed to exploit vulnerabilities: they begin by performing a "footprint" analysis to determine what network services and/or software programs (including versions and patch levels) run on the target. The tools then attempt to find indicators (patterns, attributes) of, or to exploit vulnerabilities known to exist, in the detected services/software versions, and to report the findings that result. Caution must be taken when running exploit code against "live" (operational) targets, because damaging results may occur. For example, targeting a live Web application with a "drop tables" Standard Query Language (SQL) injection probe could result in actual data loss. For this reason, some vulnerability assessment tools are (or are claimed to be) entirely passive. Passive scans, in which no data is injected by the tool into the target, do nothing but read and collect data. In some cases, such tools use vulnerability *signatures, i.e.,* patterns or attributes associated with the likely presence of a known vulnerability, such as lack of a certain patch for mitigating that vulnerability in a given target. Wholly passive tools are limited in usefulness (compared with tools that are not wholly passive) because they can only surmise the presence of vulnerabilities based on circumstantial evidence, rather than testing directly for those vulnerabilities.

Most vulnerability assessment tools implement at least some intrusive "scanning" techniques that involve locating a likely vulnerability (often through passive scanning), then injecting either random data or simulated attack data into the "interface" created or exposed by that vulnerability, as described above, then observing what results. Active scanning is a technique traditionally associated with penetration testing, and like passive scanning, is of limited utility when performed on its own, as all the injected exploits would be "blind", *i.e.,* they would be launched at the target without knowing its specific details or susceptibility to the exploits. For this reason, the majority of vulnerability assessment tools combine both passive and active scanning; the passive scanning is used to discover the vulnerabilities that the target is most likely to contain, and the active scanning is used to verify that those vulnerabilities are, in fact, both present and exposed as well as exploitable. Determining that vulnerabilities are exploitable increases the accuracy of the assessment tool by eliminating the *false positives, i.e.,* the instances in which the scanner detects a pattern or attribute indicative of a likely vulnerability that which, upon analysis, proves to be either (1) not present, (2) not exposed, or (3) not exploitable. It is the combination of passive and active scanning, together with increased automation, that has rendered automated penetration testing suites more widely useful in vulnerability assessment.

Most vulnerability assessment tools are capable of scanning a number of network nodes, including networking and networked devices (switches, routers, firewalls, printers, *etc.*), as well as server, desktop, and portable computers. The vulnerabilities that are identified by these tools may be the result of programming flaws (*e.g.,* vulnerabilities to buffer overflows, SQL injections, cross site scripting [XSS], *etc.*), or implementation flaws and misconfigurations. A smaller subset of tools also provide enough information to enable the user to discover design and even architecture flaws.

The reason for "specialization" of vulnerability assessment tools, *e.g.,* network scanners, host scanners, database scanners, Web application scanners, is that to be effective, the tool needs to have a detailed knowledge of the targets it will scan. A network scanner needs to know how to perform and interpret a network footprint analysis that involves first discovering all active nodes on the network, then scanning them to enumerate all of the available network services (*e.g.,* File Transfer Protocol [FTP], Hyper Text Transfer Protocol [HTTP]) on each host. As part of this service enumeration process, the scanner attempts to identify vulnerabilities through grabbing and analyzing banners, and checking open port status, protocol compliance, and service behavior, and through direct injection of exploits targeting known vulnerabilities (listed in the tool's built-in vulnerability database) into any open port it has found.

A host-based vulnerability assessment tool needs full knowledge of the software and software patches installed on the target host, down to specific version/release and patch levels. It thus requires full access to that host in order to scan the host and discover all of its software programs/patches, and to perform various configuration checks. Most often, this requires the installation (on the target hosts) of software agents that collect the information for that host, and report it back to a central scan server, which aggregates all of the data received from all of the agents, analyzes it, then determines what exploits from its vulnerability database should be attempted on each target host to discover and validate the existence of known/suspected vulnerabilities on that target. Unlike remote network scanning, agent-based host scanners can test for both client-side and server-side vulnerabilities.

Web application and database vulnerability scanners look for vulnerabilities that are traditionally ignored by network- or host-level vulnerability scanners. Even custom-developed Web application and/or database application often use common middleware (*e.g.,* a specific supplier's Web server, such as Microsoft® Internet Information Server [IIS] or Apache®), backends (*e.g.,* Oracle® or PostgreSQL), and technologies (*e.g.,* JavaScript®, SQL) that are known or considered likely to harbor certain types of vulnerabilities that cannot be identified *via* signature-based methods used by network- and host-based vulnerability analysis tools. Instead, Web Application scanners and database scanners directly analyze the target Web application or database, and attempt to perform common attacks against it, such as SQL injections, XSS, least privilege violations, *etc.*

The growing power and size of computing platforms able to host more complex scanning applications and their larger databases (used for storing vulnerability databases and collected findings), along with simultaneous increases in network throughput and available bandwidth, allowing for more scan-related traffic, have been enablers in the growing category of multilevel vulnerability assessment tools. Multilevel scanners seek and assess vulnerabilities at multiple layers of the ICT infrastructure, in essence combining the capabilities of two or more of the other scanner types (network and host, host and database, host and application, *etc.*). This consolidation of scanners into a single tool parallels the trend towards consolidating multiple security-relevant analysis, assessment, and remediation functions into a single vulnerability management system that, in turn, may be part of an even larger enterprise security management system.

The type and level of detail of a vulnerability assessment tool's findings varies from tool to tool. Some tools attempt to detect only a narrow set of widely-known vulnerabilities and provide little information about those it discovers. Others attempt to detect a much larger number of vulnerabilities and weaknesses (*i.e.,* anomalies that are only suspected to be exploitable as vulnerabilities), and provides a great deal of information about its findings, including potential impacts of level of risk posed by the discovered vulnerabilities, suggested remediations for them (*e.g.,* necessary reconfigurations or patches), and prioritization of those remediations based on their perceived or assessed impact and/or risk.

Vulnerability assessment tools are most useful when applied during two phases in a target's lifecycle: (1) just before deployment of a system, and (2) reiteratively after its deployment. The most sophisticated vulnerability assessment tools not only identify vulnerabilities, analyze their likely impact, and determine and prioritize mitigations, they can also retrieve or generate and apply those remediations/patches in real time, and follow up with ongoing periodic automated and/or event-driven (*ad hoc*) reassessments to ensure that no new vulnerabilities have emerged, or old ones resurfaced, during the evolution of the target or its threat environment. The ability of a tool to not only assess but also remediate and continuously monitor the system for vulnerabilities "promotes" it from a vulnerability assessment tool to a vulnerability *management* system.

2.3 Standards for Vulnerability Assessment Tools

The challenge of security risk management, and larger security management, has expanded exponentially, both in difficulty and scope with the size, proliferation, reach, and complexity of systems and networks and their underlying technologies, and the rapidity of evolution of the threats (with all of their associated attack methods and supporting attack technologies) to those systems and networks. In an attempt to automate as many security management processes as possible, over the past decade or so individual researchers and vendors have done their best to adjust by expanding their risk/security management-related solutions from individual tools, to (somewhat) integrated tool suites, and finally to fully-integrated enterprise security management systems. But yet another obstacle remains to be overcome, which is the ability of supplier's tools/suites/systems to consume, comprehend, render a "common security picture" from tools/suites/systems of other suppliers. In its standards definition role, NIST has been collaborating with DOD, National Security Agency NSA), and the Office of Management and Budget (OMB), with support of a large number of technologists in other government organizations and industry to define a complete set of standard protocols and languages that security tools and systems can use to encapsulate and exchange their information with other security tools and systems. Among these standards are NIST's SCAP—a standard defining what security content is needed for automating technical control compliance, vulnerability checking, and security measurement activities, and a growing number of standards developed, in large part, through community development efforts spearheaded by The MITRE Corporation. These include standards for enumerating, describing, measuring/quantifying, and encapsulating data about security weaknesses, vulnerabilities, configurations, threats, attack patterns, malicious code, and intrusion events, *etc.*, in networks, systems, applications, databases, *etc.* These standards can be investigated at MITRE's Making Security Measurable Web site at *http://measurablesecurity.mitre.org* (accessed 29 April 2011).

The subset of these standards that is directly relevant to the encapsulation and exchange of data among vulnerability assessment tools includes SCAP which points to several MITRE standards as its required means for encapsulating, exchanging, or ranking vulnerability information generated or consumed by vulnerability analysis tools. The vulnerability assessment-specific standards it points to are OVAL, CVE, and Common Vulnerability Scoring System (CVSS) for all vulnerability assessment tools, CWE for those tools that assess vulnerabilities in software, and eXtensible Configuration Checklist Description Format (XCCDF), Common Configuration Enumeration (CCE), and Common Platform Enumeration (CPE) for vulnerability assessment tools that analyze security configurations as part of their vulnerability detection process.

There have been (and still are) other less successful efforts outside the SCAP realm to define standards for use in automating vulnerability assessment. The most notable of these include the efforts of the Organization for the Advancement of Structured Information Standards' (OASIS') Application Vulnerability Description Language (AVDL) [5] Technical Committee and the Open Web Application Security Project's (OWASP's) Application Security Verification Standard (ASVS) Project. [6] The United Kingdom (UK) National Infrastructure Security Co-ordination Centre (NISCC) Capability Development and Research (CD&R) Group's IA Metadata Team's worked for a time to define the Vulnerability and Exploit Description and Exchange Format (VEDEF) for exchanging CVE, OVAL, and Common Malware Enumeration (CME - now Malware Attribute Enumeration and Characterization [MAEC]) data, and the Susceptibility and Flaw Definition (SFDEF), a metadata interchange format for CWE data.

SCAP is being mandated across United States (U.S.) government (and is being considered for adoption outside government and outside the U.S. as well). It has been and is being implemented within many vulnerability assessment tools, vulnerability assessment systems, risk management systems, and enterprise security management systems. The same is true of the individual standards it mandates (*e.g.,* CVE, CPE, CVSS) which, because they are not U.S. government-defined, are gaining traction outside the U.S. as well, especially among tool suppliers that wish to market to the U.S. government. A number of vulnerability assessment tools explicitly search for vulnerabilities catalogued in the CVE and CWE, and for other vulnerabilities whose descriptions have been encoded in OVAL. Others rely on CVSS metrics to quantifiably rank (or "score") the vulnerabilities they detect.

Because of its status as a mandate, SCAP validation is noted for those tools listed in Section 3 that appear on the NIST NVD's SCAP-Validated Products List. Also noted is whether a given tool conforms to any of the vulnerability assessment-specific standards mandated by SCAP (OVAL, CVE, CVSS) or to CWE.

[5] See OASIS AVDL Technical Committee Web page for more information. *http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=avdl* (accessed 29 April 2011).

[6] See OWASP ASVS Project Web page. *https://www.owasp.org/index.php/Category:OWASP_Application_Security_Verification_Standard_Project* (accessed 29 April 2011).

SECTION 3 ▸ Vulnerability Analysis Tools

Section 3 provides summaries of pertinent information about available vulnerability assessment tools, including vendor contact information. The information in the tool descriptions is drawn primarily from the tool supplier from its Web site and product literature. In a few cases, additional information was derived from the NIST NVD and SCAP Web sites and the MITRE OVAL, CVE, and CWE Web sites. The information provided about each tool is intended only to highlight the capabilities and features of the tool. It is left to readers to perform the additional research and evaluations required to determine which tools best address their needs.

As noted in Section 1.3, this Report lists only tools that are currently available, and that have been updated by their suppliers within the past two years. Tools that have not been updated since 2008 or before are not included (though a list of older open source tools is provided in Appendix B for informational purposes).

This tool listing is organized into seven sections, according to tool type:

- Network Scanners
- Host Scanners
- Database Scanners
- Web Application Scanners
- Multilevel Scanners
- Automated Penetration Test Tools
- Vulnerability Scan Consolidators.

Within each section, the tools are listed alphabetically by supplier name (if branded) or tool name (if open source). Vulnerability management systems that incorporate vulnerability assessment tools are categorized according to the type of vulnerability assessment tool they incorporate. The description of such tools in this Report focuses only on their vulnerability scanning/analysis capabilities. The broader capabilities of vulnerability management system products are not described, as they are out of scope for this Report.

Legend for the Tables

Following each tool description, a table in the format below provides certain standard information about the tool. Each information field in the table is explained below.

If a field in the table for a particular tool contains no information, that means either that the field was not relevant for that tool, or that the information could not be found on the supplier's Web site on one of the NIST or MITRE Web sites noted above.

Tool Identifier
(supplier + tool name + current version number, if known)

Type	The type of tool, or category in which this tool belongs, *e.g.,* "Web Application Scanner"
Target(s)	The specific item(s) or item type(s) that tool is designed to analyze, *e.g.,* Windows® operating systems, Cisco® routers
Format	The format in which the tool can be purchased: Appliance or Software. If the tool is distributed on an appliance, unless explicitly noted, the appliance is presumed to include an operating system and hardware, so those fields in the tool's table will be left blank.
OS	The operating system(s) (OS) on which a software (*vs.* appliance-based) tool runs. This field will also identify any other software that is required for the product to run (*e.g.,* database, .NET framework, browser).

Tool Identifier

(supplier + tool name + current version number, if known)

Hardware	The type and speed of central processing unit (CPU), amount of random access memory (RAM) and free disk space (indicated as "disk"), and any other hardware prerequisites (*e.g.,* network interface card [NIC], monitor with certain resolution ("res.") for running the tool software.)
License	Type of license under which the tool is distributed: Commercial, Shareware, Open Source, or Freeware
SCAP Validated	If the tool has been validated by NIST as SCAP-compliant, this field will include the URL of the tool's SCAP validation data. Otherwise, this field will be blank. This field will be left blank for tools still undergoing SCAP validation; in such cases, SCAP may be listed in the next field as one of the standards with which the tool complies.
Standards	Relevant standards to which the tool conforms. This will include only standards directly relevant to vulnerability analysis, *i.e.,* SCAP, OVAL, CVE, CWE, and CVSS. Standards for configuration checking (*e.g.,* XCCDF, FDCC) and other types of analyses are not included. For tools not compliant with any such standards, this field will be blank. Entries in this field are based on supplier claims of standards compliance because some supplier claims are in the process of being validated by the responsible standards bodies, and so the tools do not yet appear on validated products lists.
Supplier	Full name of the organization or individual that developed and distributes the tool. For suppliers that are non-U.S.-based, the country in which they are headquartered (or, for individuals, in which they reside) will be noted in parentheses.
Information	URL to the supplier's information about the tool

Research Methodology

The methodology for discovering the tools listed in Section 3 (as well as those in Appendix B) of this edition of the IATAC Vulnerability Assessment IA Tools Report was to begin with the list of tools in the previous edition. For each of those tools, the authors of this edition visited the Web site of the supplier (vendor or developer) indicated in the previous edition. Anyone comparing the new edition of this Tools Report with the previous edition will be struck by how many of the tools in the previous edition do not appear in this edition. This is in large part because the security products market is so volatile. As we investigated tools from the previous edition, the authors rapidly discovered that quite a few of the companies that had sold them had been purchased by other companies. For example, McAfee purchased Fortify, and International Business Machines (IBM) purchased Internet Security Systems (ISS). In some cases, the new owner of a tool kept that tool in its product under its original name (*e.g.,* AppScan® is a tool that has undergone numerous changes-of-ownership; it was originally developed by Sanctum [a subsidiary of Perfecto Technologies, Limited (Ltd.)], which was then purchased by Watchfire Corporation; Watchfire was then purchased by IBM, which also purchased Rational Corporation, and established the "IBM/Rational" brand for its software and application development products. Thereafter, AppScan became and IBM/Rational product while still retaining its original product name). On the other hand, when IBM acquired ISS, it dropped the ISS product name while retaining Proventia; so the network vulnerability scanner formerly referred to as "ISS" is now the IBM® Proventia® Network Enterprise Scanner. All of this is intended to illustrate that various pedigree and provenance trails had to be followed to determine the actual fate of some of the tools in the previous edition that now exist in renamed, and often extended or modified, forms.

Once all tools and suppliers from the previous edition were researched, the authors studied the product lists on the NVD/SCAP, and MITRE OVAL, CVE, and CWE Web sites. OVAL, CVE, and CWE (all standard mandated for SCAP compliance) are directly relevant to automated vulnerability detection. A number of tools not included in the previous version of this Report were discovered in this way, and are included in Section 3. The third way in which tools were discovered was through targeted boolean Google searches, including following various "trails" when one Web page pointed us to another. The final way in which we discovered new tools was to review tools lists in other online and downloadable vulnerability assessment tool papers, evaluations, *etc.* We investigated these for any tools not already discovered through our other searches. A few significant tools were discovered this way.

For all tools discovered, the authors investigated the supplier's Web site to find the information required to provide a useful précis of the tool's features and capabilities, and to fill in the entries in the information table that follows the abstract on each tool in its entry in Section 3. In most cases, this necessitated downloading product spec sheets to augment the information published on the "splash" page for the tool on the supplier's Web site. In the case of open source tools, the only source of information was often the scant amount available *via* an open source repository Web page for the tool. In some cases, the repository page also pointed to a separate, more informative open source project Web site, but this was by no means always the case. For this reason, there is usually less information provided about open source tools than about commercial tools. In some cases, additional information of value was also found in the SCAP validation report for those tools that are SCAP validated; however, unlike Common Criteria certification reports, which are extremely informative, SCAP validation reports are very narrowly focused on the ways in which the validated tool satisfies the specific requirements of SCAP, *i.e.,* how the tool uses OVAL, CVE, CVSS, and other standards that are required for SCAP compliance. General information on how the tool operates is not included in these compliance reports, beyond a sentence or two. But for tools about which no other source of substantive information was available, the SCAP validation report information had to suffice.

In a few cases, the only literature available about the tool was not in English. In such cases, the authors relied on Google Translate to provide at least a gist of what the Web page or product literature. There is an indication in each tool listing in Section 3, next to the URL for finding further information on the tool, when that information is only available in a foreign language.

Aside from a few open source instances, the authors expunged all "obsolete" tools from the new edition of this Report, *i.e.,* tools not updated since 2008 (an indication that the tool is no longer actively supported by its supplier). The exceptions are listed, without descriptions but with URLs for further information, in Appendix B.

SaaS offerings of vulnerability assessments using various tools were discovered in the course of researching the tools and suppliers, and through boolean Google searches like those used for finding additional tools. Since this is a Tools report rather than a Services report, the authors did not attempt to provide an exhaustive listing of such SaaS offerings, as they did with the listing of tools. Rather, the number of offering listed in Section 4 is intended to be large enough to be representative of the growing trend towards offering vulnerability assessment tools *via* SaaS rather than direct product sale or licensing. As with Appendix B, Section 4 does not provide descriptions of the offerings, beyond indicating the type of vulnerability scan offered, the vendor, the tool(s) used (if this could be discovered), and a URL to more information.

Trademark Disclaimer

The authors have made a best effort to indicate registered trademarks where they apply, based on searches in the U.S. Patent and Trademark Office Trademark Electronic Search System (PTO TESS) for "live" registered trademarks for all company, product, and technology names. There is a possibility, however, that due to the large quantity of such names in this report, some registered trademarks may have been overlooked. We apologize in advance for the inadvertent exclusion of any registered trademarks and invite the trademark registrants to contact the IATAC to inform us of their trademark status so we can appropriately indicate these trademarks in our next revision or errata sheet. Note that we have not indicated non-registered and non-U.S. registered trademarks due to the inability to research these effectively.

Non-Endorsement Disclaimer

Inclusion of any tool in this report does not constitute an endorsement, recommendation, or evaluation of that tool by IATAC, DTIC, or DOD.

NETWORK SCANNERS

Beyond Security® Automated Vulnerability Detection System

Abstract

Beyond Security Automated Vulnerability Detection System (AVDS) is a network vulnerability assessment appliance for equipment, operating systems, and applications hosted on networks of 50 to 200,000 nodes. Scanning is by IP (Internet Protocol) address range, with an inspection of each target for security weaknesses. With each scan, AVDS automatically discovers any new equipment and services that should be added to its inspection schedule. AVDS tests every node based on its characteristics, and reports the node's responses to reveal security issues. AVDS generates detailed reports specifying network security weaknesses. The tool relies on a database of tests for 10,000 known vulnerabilities tests that is updated daily to add new vulnerabilities discovered by AVDS developers and by corporate and private security teams around the world. AVDS can be scheduled to perform automated vulnerability scans daily, weekly, monthly, or *ad hoc*. It analyzes its recorded results to report vulnerability trends across the entire wide area network (WAN) or local area network (LAN), as well as trends for a single Internet Protocol (IP) address or group of IP addresses. AVDS reports also provide exact remediations for individual vulnerabilities, and recommendations on how to fix and improve the security of the network overall. AVDS comprises two types of appliances: (1) the Information Server, which stores the scan results in a local MySQL database, and manages all associated Local Security Scanners; (2) the Local Security Scanner, which performs the actual vulnerability scans (one Local Security Scanner can scan up to 2,500 nodes, eight at a time). Multiple Local Security Scanners can be centrally managed by the same Information Server.

Beyond Security Automated Vulnerability Detection System

Type	Network Scanner
Target(s)	Hosts: Windows (95/98/NT 4.0/ 2000/ XP/ 2003 Server); UNIX (Solaris®, AIX® [Advanced Interactive eXecutive], HP-UX® [Hewlett-Packard UniX], Unixware®, OpenBSD [Open Berkeley Software Distribution], NetBSD, Mac OS [Macintosh OS 10]® X, Linux®); Novell® NDS [Netware Directory Services]; AS [Application System] 400; VMS); Digital Equipment Corporation Virtual Memory System] DEC VMS; Security systems: Antivirus servers, IDS, firewalls; Network devices: routers, switches, hubs, wireless access points, modems, voice-over-IP devices; Servers: remote access servers, Web servers, database servers, mail servers, FTP servers, proxy servers; Applications: in SQL, Active Server Pages (ASP), PHP Hypertext Preprocessor (PHP), Common Gateway Interface (CGI) scripting languages
Format	Appliance
OS	Included
Hardware	Included
License	Commercial
SCAP Validated	
Standards	CVE
Supplier	Beyond Security (U.S./Israel)
Information	*http://www.beyondsecurity.com/ vulnerability-assessment.html*

Black Falcon/Net Security Suite Falcon Vulnerability Analysis

Abstract

Black Falcon/Net Security Suite's Falcon Vulnerability Analysis (FAV) is a tool for auditing networked hosts and devices, analyzing, classifying, and reporting the vulnerabilities detected in the scanned nodes; scans can target virtual LANs, network segments, or individual workstations, servers, routers, printers, *etc.* (designated by media access control [MAC] or IP address). FAV vulnerability scans test targets for all CVEs, and the tool validates the vulnerabilities it detects through use of controlled attacks (also consistent with CVE), thereby eliminating potential false positives. The tool correlates the results of its analyses, and can verify their degree of compliance with or deviation from mandated security standards and regulations. Results from repeated scans of the same target can be compared as well. The scanner's database of CVEs, CVSS scores, and sampling algorithms is updated daily. FAV is sold as an appliance. FAV requires installation of an administrative console (can run on Windows, Linux, UNIX, or Mac OS X) and a Web browser to display reports.

Black Falcon/Net Security Suite Falcon Vulnerability Analysis

Type	Network Scanner
Target(s)	Wired and wireless network devices, OSs, Web applications/services, databases
Format	Scanner: Appliance Console: Software
OS	Console: Windows, Linux, UNIX, Mac OS X
Hardware	
License	Commercial
SCAP Validated	
Standards	CVE, CVSS
Supplier	BlackFalcon/Net Security Suite (Colombia)
Information	*http://www.netsecuritysuite.com/fav.html*

DragonSoft Vulnerability Management

Abstract

DragonSoft Vulnerability Management (DVM) is designed for mid-sized to large businesses to perform network vulnerability scanning, vulnerability evaluation, centralized risk assessment, reporting, and risk remediation. DVM analyzes and examines potential vulnerability descriptions, then scans network assets to spot those vulnerabilities. DVM comprises (1) Security Scanner with network vulnerability audit, password audit, and denial of service test capabilities that can perform more than 4,500 vulnerability definition checks, and (2) Vulnerability Risk Management, which provides a central management platform for both internal and external host vulnerability mitigation and management, and supports compliance audits for International Organization for Standardization (ISO) 27001:2005, SOX, HIPAA, Payment Card Industry Digital Security Standards (PCI DSS), and other regulations/standards. The reports and graphical tables pinpoint where to implement patches and other remediations. Users can set up to 50 customized policies, and can store reports to ODBC.

DragonSoft Vulnerability Management

Type	Network Scanner
Target(s)	Network services, network devices (gateways, routers, switches), Hosts (Windows NT®/2000/2003/XP®), UNIX (Solaris, FreeBSD®, AIX), Linux hosts, SQL databases (MySQL®, PostgreSQL, MiniSQL, Oracle®, SQL Server®, Database 2 [DB2®]), Web sites (HTTP) including Web directory exploration, electronic mail (Email) Servers, file servers, Samba Servers
Format	Software
OS	Windows 2000/XP/2003 running Internet Explorer (IE) 5.0+ or Firefox® 3.0+
Hardware	512 Megabytes (MB) RAM, 40GB disk, Compact Disc/Digital Video Disk-Read Only Memory (CD/DVD-ROM), fast Ethernet/wireless NIC
License	Commercial
SCAP Validated	
Standards	CVE, CVSS
Supplier	Dragon Soft Security Associates, Incorporated (Inc.) (Taiwan)
Information	*http://www.dragonsoft.com/product/engDVM_01.php*

eEye® Retina® Network

Abstract

eEye Retina Network security scanner identifies known and zero day vulnerabilities to protect an organization's networked assets. The Retina Scanner supports security risk assessment and regulatory audits. Key features include: (1) discovery and scanning of all remote and local assets in the network infrastructure; (2) non-intrusive scanning engine to enable scanning network devices (including wireless devices), OSs, Web applications/services, and databases with minimal impact on network performance; OS discovery uses Internet Control Message Protocol (ICMP), registry, Networked Basic Input/Output System (NetBIOS), Nmap® signature database, and eEye's proprietary OS fingerprinting for OS identification; auditing of non-Windows devices includes Secure Shell (SSH) tunneling to perform local vulnerability assessment of UNIX, Linux, Cisco, and other non-Windows devices; (3) prioritization of vulnerabilities to expedite mitigation and patching; Fix-It function can be used to remotely correct security issues such as registry settings, file permissions, *etc.* (4) vulnerability database continually updated by eEye's research team; (5) supports definition of corporate policy-driven scans for auditing of complex internal security policies; (6) open architecture allows for customization of audits and integration of third-party tests and tools; (7) Retina reconciles the input/output data on each Transmission Control Protocol (TCP) port to determine which protocols and services are running, including Secure Socket Layer (SSL), and automatically adjusts for custom or unconventional machine configurations; (8) Scheduler function allows user to set the scanner to run on a regular periodic basis. Retina Network vulnerability scanning is also offered in a free SaaS package, Retina Community, that allows free vulnerability assessments and SCAP configuration compliance scans across the operating systems, applications, devices, and virtual environments at up to 32 target IP addresses, with reports generated in eXtensible Markup Language [XML], comma-separated values [CSV], and Portable Document Format [PDF]).

eEye Retina

Type	Network Scanner
Target(s)	Wired and wireless network devices, OSs, Web applications/services, databases
Format	Software
OS	Windows (2000 Pro/Server, XP; Server 2003; Vista Service Pack (SP) 2, Server 2008 SP2/Server 2008 R2 [64-bit only], 7); all running *Microsoft .NET* Framework 2.0
Hardware	1.4 GigaHerz (GHz) Pentium®, 512MB RAM, 80MB disk, NIC with TCP/IP enabled
License	Commercial
SCAP Validated	*http://nvd.nist.gov/validation_eeye.cfm*
Standards	SCAP, OVAL, CVE, CVSS
Supplier	eEye Digital Security®
Information	*http://www.eeye.com/Products/Retina/Network-Security-Scanner*

Fortinet® FortiScan 4.1.0

Abstract

Fortinet FortiScan provides a centrally managed, enterprise-scale continuous monitoring and compliance auditing solution for operating systems. Compliance policies (NIST SCAP, FDCC, PCI DSS, *etc.*) are available out-of-the-box and are regularly updated. FortiScan runs on the FortiScan-1000C hardware appliance, and requires FortiScan Asset Agents to be deployed on all targeted hosts. The scanner performs endpoint vulnerability scanning to identify security vulnerabilities and find compliance exposures on networked hosts and servers. Detected vulnerabilities can be displayed by status, severity, asset severity, and asset criticality, and statistics can also be displayed (*e.g.,* total number of vulnerability alerts raised, internally resolved, externally resolved, accepted, or unresolved within a given timeframe); known vulnerability references can also be displayed by vendor (of element containing the vulnerability). The scanner also performs network discovery, asset prioritization, profile-based scanning, patch management, vulnerability remediation, and vulnerability and audit reporting. A centralized administration console facilitates management of multiple FortiScan appliances across the enterprise network. A single FortiScan appliance can scan up to 5,000 hosts (running FortiScan agents) and up to 60 database instances (all running FortiScan agents).

Fortinet FortiScan 4.1.0

Type	Network Scanner
Target(s)	
Format	Appliance and Software (agents)
OS	Agent: Windows (2000/XP/Vista®/Server 2003/Server 2008); Linux (Red Hat Enterprise Servers (ES) 3.0-5.0); UNIX (Solaris 8-10) Console: Internet Explorer (IE) 7.0-8.0; Firefox 3.x
Hardware	Agent: 500 Kilobytes (KB) disk Console: 1280x1024 res. monitor
License	Commercial
SCAP Validated	
Standards	SCAP
Supplier	Fortinet, Inc.
Information	*http://www.fortinet.com/products/fortiscan/*

FuJian RongJi RJ-iTOP

Abstract

FuJian RongJi RJ-iTOP network vulnerability scanner scans for more than 2,260 vulnerabilities across 22 CVE categories. It can detect vulnerabilities and backdoors in host operating systems, network equipment, and databases. Scan performance can be optimized through automatic adjustment of the number of concurrent scanning threads. The scanner comes with a default scanning policy, but also enables user definition of custom scanning strategies. The scanner can target a single IP address, multiple IP addresses, or a whole network segment, and can be scheduled to perform periodic automatic scans without human intervention. The scanner outputs customizable, multi-format reports tailored to the needs of different roles (*e.g.,* executives, security experts, technical staff). The reports include solutions for fixing bugs and vulnerabilities, including links to relevant Web sites and information on repair methods. RJ-iTOP can be purchased in one of three appliance formats: one hand-held, one mobile, and one 1U rackmount appliance, or as software.

FuJian RongJi RJ-iTOP

Type	Network Scanner
Target(s)	OSs (AIX, OS/400, HP-UX, Solaris, Tru64® UNIX, Red Hat Linux, Bluepoint Linux, Xterm, Red Flag Linux, Slackware, FreeBSD, NetBSD, Santa Cruz Operation (SCO) UNIX, Windows NT/2000/XP/98/Me®, Novell® Netware 5); Network devices (switches, routers, firewalls, IDS/IPS, *etc.*), Databases (Oracle, SQL Server, MySQL, *etc.*), network services
Format	Appliance or Software
OS	Windows 2000
Hardware	866 MHz Pentium III, 256MB RAM, 400MB disk, 10/100 million bits per second (Mbps) Ethernet NIC
License	Commercial
SCAP Validated	
Standards	CVE
Supplier	FuJian RongJi Software Company, Ltd./ Yung-Based Enterprise Network Security Division (China)
Information	*http://www.rj-itop.com/* (in Chinese only)

GFI LANguard® 9.6

Abstract

GFI LANguard is a network security scanner and patch management solution that assists in patch management, vulnerability management, network and software auditing, asset inventorying, change management, risk and compliance analysis. GFI LANguard scans computers, identifies and categorizes security vulnerabilities, recommends a remediation course of action and provides tools to assist in the remediation. During LANguard security audits, more than 15,000 vulnerability checks are made of OSs, virtual environments, and installed applications, one IP address at a time. GFI LANguard can perform multi-platform scans (Windows, Mac OS X, Linux, virtual machines). GFI LANguard includes its own vulnerability assessment database that includes checks for 2,000+ CVEs and SANS Top 20 vulnerabilities. The database is regularly updated with information from Bugtraq, SANS, CVE, Microsoft security updates, and GFI Software's and other community-based information repositories. GFI LANguard includes a graphic threat level indicator that provides a weighted assessment of the vulnerability status of a scanned computer or group of computers, and whenever possible, a Web link for more information on a particular security issue. The tool enables the user to create simple custom vulnerability checks through a set-up wizard, or complex vulnerability checks *via* the wizard's Python/Virtual Basic Script (VBScript)-compatible scripting engine. Using the wizard, users can configure scans for different types of information, such as open shares on workstations, security audit and password policies, and machines missing a particular patch or service pack. GFI LANguard can be used to both scan for and remediate various types of vulnerabilities, such as finding and closing unnecessary open ports to detect/prevent port hijacking, detecting and disabling unused local user and group accounts, identifying blacklisted software programs and flagging them with a high level vulnerability alert. GFI LANguard also scans all devices connected to Universal Serial Bus (USB) or wireless links, and issues alerts of detected suspicious activity. Scan results can be exported in XML format. GFI also offers a freeware version, intended for personal use, and capable of scanning up to five IP addresses. The freeware version of GFI LANguard provides all functions found in the commercial version with the exception of patch management for non-Microsoft applications.

GFI LANguard 9.6

Type	Network Scanner
Target(s)	UNIX (must run Secure Shell [SSH]), Windows (must run Windows Management Instrumentation [WMI])
Format	Software
OS	Windows (2000 Professional SP4+/Server SP4+/Advanced SP4+/Small Business SP2; Server 2003 Standard/Enterprise/Small Business SP1; Server 2008 Standard/Enterprise/Small Business; Vista Business/Enterprise/Ultimate, XP Professional SP2+, 7 Ultimate) running .NET Framework 2.0 and SQL Server 2000+, Microsoft Data Engine/SQL Server Express, or Access®
Hardware	1-10 targets: 1GHz CPU, 1 gigabyte (GB) RAM, 1GB disk; 11-500 targets: 2GHz CPU, 2GB RAM, 2GB disk; 501-1,000 targets: Two 3GHz quad core CPUs, 4GB RAM, 10GB disk
License	Commercial (Freeware version available)
SCAP Validated	
Standards	OVAL, CVE
Supplier	GFI Software
Information	*http://www.gfi.com/lannetscan*

GFI Sunbelt Network Security Inspector Suite 2.0

Abstract

GFI Sunbelt Software Network Security Inspector (SNSI) is a network vulnerability scanner that can test for more than 4,000 multi-platform vulnerabilities. SNSI can scan by machine, IP address range, port, or service. It can target Windows, Mac OS X, UNIX, Linux, as well as Cisco router and HP printer devices. Scanning can also be based on access-levels, including credentialed and null based. Ad hoc scans can target one or many machines and/or specific vulnerabilities. The scanner identifies all network devices, and performs configuration checks on ports, services, users, shares, and groups. Vulnerability audits include security configurations, OS and application vulnerabilities, null passwords, patch-level related vulnerabilities, known hacking tools, malware, common worms, peer-to-peer (P2P) software checks, and other checks. Scanning is non-disruptive; the scanner never employs malicious vulnerability attacks and uses only standard networking protocols and application programmatic interfaces (APIs). The scanner's test database is derived from the latest CVEs, SANS/Federal Bureau of Investigation (FBI) Top 20 vulnerabilities, and Computer Emergency Response Team/Coordination Center (CERT/CC), Microsoft Cyber Incident Response Capability, and US-CERT advisories. The tool's vulnerability database provides informational resources and remediation recommendations. Once scanned, all targeted systems are evaluated and prioritized according to asset value and vulnerability criticalities, then rated by risk severity to help focus and prioritize remediation efforts. SNSI is Common Criteria Certified at Evaluation Assurance Level (EAL) 2.

GFI Sunbelt Network Security Inspector Suite 2.0

Type	Network Scanner
Target(s)	Windows (2000, 2003, 2008, XP/XP Embedded, Vista all editions [32/64-bit]); Linux (Red Hat Enterprise 2.1-5.x, Fedora 6/7, Mandriva® 7.0/7.1, Software-und System Entwicklung [SuSE®] Open/Enterprise 9.0-10.3); UNIX (Solaris 2.5+, Mac OS X, HP-UX 10.x+, Tru64 4.0F+, OpenBSD 3.8+); Cisco (IOS® [Internetwork Operating System], CatOS, PIX®), HP networked printers
Format	Software
OS	Scanner: Windows *running .NET* 2.0 Console: Windows XP Professional SP2+ or Server 2003 SP1+ running a PDF viewer (*e.g.,* Adobe® Acrobat® Reader)
Hardware	1GB RAM (2GB+ recommended), 20GB disk; 1024x768 res. monitor; TCP/IP NIC
License	Commercial
SCAP Validated	
Standards	CVE
Supplier	GFI Software
Information	*http://www.sunbeltsoftware.com/business/sunbelt-network-security-inspector/*

Global DataGuard® Unified Enterprise Security: Vulnerability Scanner Module

Abstract

The Vulnerability Scanner Module (VSM) of the Global DataGuard Unified Enterprise Security suite is an on-demand scanning and vulnerability management tool that researches thousands of different types of vulnerabilities and provides regular security scans that are integrated and correlated with data and alerts from other appliances, including alerts produced by the behavioral analysis and correlation engine. The alerts are further prioritized and escalated based on attacks against detected vulnerabilities. The VSM is integrated with a penetration testing tool that allows the user to exploit detected vulnerabilities, iteratively as the network changes, enabling ongoing research of new potential security issues throughout the network infrastructure. The VSM also uses an asset database to help keep track of resources, and to organize and retrieve information for remediation of vulnerabilities. A trend analysis report option allows the user to quantitatively analyze the remediation program generated by the tool. The VSM module's reporting features produce individual vulnerability reports for each scanned device, with associated risk levels (informational, low, high, severe) and appropriate links to CVEs, patches, and remediation steps. With optional VSM software, the user can also design and generate custom vulnerability assessment reports that use format with color-coded charts. The VSM's research, tracking, analysis and reporting features also enable the user to generate PCI DSS compliance reports. The VSM supports four on-demand scanning options: (1) Light scanning, which includes limited port scans to identify common vulnerabilities such as those within Domain Name System (DNS), Web (HTTP), or FTP, and Simple Message Transfer Protocol (SMTP); (2) Heavy scanning, which entails full port scans that look for all known vulnerabilities and potential risk areas; (3) Denial of Service scans that identify all dangerous vulnerabilities on the appropriate ports; (4) Scheduled scans, with customizable scanning options for immediate, daily, weekly, monthly, quarterly and annual scans. VSM also provides a private Web portal that allows customers to view alerts, scans, and run reports in real time.

Global DataGuard Unified Enterprise Security: Vulnerability Scanner Module

Type	Network Scanner
Target(s)	
Format	Appliance
OS	
Hardware	
License	Commercial
SCAP Validated	
Standards	OVAL, CVE, CVSS
Supplier	Global DataGuard, Inc.
Information	*http://www.globaldataguard.com/products/vm.php*

Greenbone Security Feed and Security Manager 1.4

Abstract

Greenbone Security Feed is a stream of small procedures designed to detect known and unknown security vulnerabilities. These procedures are executed either by Security Feed's built-in scan engine, which can be hosted on Greenbone Security Manager, or by OpenVAS, to scan devices and hosts connected to a network. Tests are derived from CVE and Bugtraq® alerts and combined with aggregated compliance rulesets. Security Feed also provides controls for its scanning agents, and embedded Nmap Scripting Engine test routines. Greenbone Security Manager is a dedicated Vulnerability Management appliance that interoperates with Greenbone Security Feed to control and collect results from the vulnerability and compliance scans provided by Security Feed. Greenbone Security Explorer, a JavaScript® plug-in for Firefox 3.6 or IE 8, can be purchased to provide a map-based view of Greenbone Security Manager scan findings.

Greenbone Security Feed and Security Manager 1.4

Type	Network Scanner
Target(s)	Windows, Linux (Debian, Fedora, Mandriva, Red Hat, SuSE, Ubuntu) UNIX (Solaris, HP-UX), Cisco, and other vendors' active network devices
Format	Appliance or Software
OS	SuSE Linux Enterprise Server Version 11 SP1 running OpenVAS Scanner Version 3.0.0
Hardware	
License	Commercial
SCAP Validated	
Standards	OVAL, CVE
Supplier	Greenbone Networks Gesellschaft mit beschränkter Haftung (GmbH) (Germany)
Information	*http://www.greenbone.net/solutions/gbn_feed.html* *http://www.greenbone.net/solutions/gbn_manager.html*

Hangzhou DPtech Scanner1000

Abstract

Hangzhou DPtech Scanner1000 vulnerability scanning system detects, alerts, and automatically patches (through integration with Microsoft Window Update Services patch manager) and repairs vulnerabilities, performs asset risk management and vulnerability auditing. The Scanner's "smart association scan engine" technology employs a variety of scanning methods to find, assess, and validate each vulnerability. The scanner's library of vulnerability signatures is continually updated to ensure timeliness and accuracy of scans. The tool can detect both network-level vulnerabilities (*e.g.,* unnecessary open ports, weak passwords) and application-level vulnerabilities, including XSS, SQL injection and other injections (Web 2.0/Asynchronous JavaScript And XML [AJAX] injections, cookie injections, *etc.*), remote file retrievals, file uploads, weak passwords (including passwords in forms), data leaks, Google hacks, Trojan horse threats. It also supports SSL encryption to enable authenticated scans. Scans can be scheduled to run automatically, or can be invoked manually (for *ad hoc* scanning); the user can preconfigure scanning depth, login parameters (for authenticated scanning), and domain name/IP address ranges to be scanned. Reports include vulnerability reports, comparative reports (scan results of same target over time), with support for statistical analyses and export of reports to multiple formats. The DPtech scanner comes in two appliances, the smaller Scanner1000-MS and the larger Scanner1000-GS.

Hangzhou DPtech Scanner1000

Type	Network Scanner
Target(s)	Terminal equipment, routers, switches, network services (SMTP/Post Office Protocol 3 [POP3], FTP, SNMP), servers and clients running Windows, Linux, UNIX, Web applications (HTTP/HTTP Secure [HTTPS] Web servers, plug-ins)
Format	Appliance
OS	
Hardware	
License	Commercial
SCAP Validated	
Standards	CVE
Supplier	Hangzhou DPtech Technologies Company (Co.), Limited (Ltd.) (China)
Information	*http://www.diputech.com/Products_Technology.php?id=102&m=7* (in Chinese only)

IBM® Proventia® Network Enterprise Scanner 2.3

Abstract

IBM Proventia Network Enterprise Scanner running IBM Internet Scanner Software identifies, prioritizes, tracks, and reports security vulnerabilities on more than 1,500 device types and more than 3,400 service types. Proventia Network Enterprise Scanner enables responsibility for remediation to be assigned for specific assets. Its multisource discovery capability uses a variety of asset identification techniques for detecting newly-connected devices and previously undiscovered assets. The specific tests run are non-impactful, yet can analyze the effects of a real attack without exposing the network to real threats. The scanner supports automated, continuous assessment as well as *ad hoc*, targeted scans. The scanner's asset-centric scan policy ensures policy association with assets rather than with scanner. Results can be grouped and reported by geography, network layout, business system, or any other useful grouping of assets. Enterprise Scanner uses CVSS to determine the severity of discovered vulnerabilities. The vulnerability signature database is frequently updated with new vulnerabilities recommended by the IBM Internet Security Services (ISS) X-Force® research team. Network Enterprise Scanner also enables automatic ticket creation *via* a flexible rule-based system. The scanner can also be integrated with Microsoft Active Directory®, Boulett Moores Cloer [BMC®] Remedy® Help Desk, and existing asset management systems *via* the IBM Proventia Management SiteProtector system. Two appliance formats are available, a 1U rack mount and a desktop appliance. Up to five network segments can be scanned from a single Proventia Network Enterprise Scanner appliance. The Enterprise Scanner 750 can scan up to 3,000 nodes per appliance; the Enterprise Scanner 1500 can scan up to 10,000 nodes per appliance.

IBM Proventia Network Enterprise Scanner 2.3

Type	Network Scanner
Target(s)	Networked devices and Windows hosts
Format	Appliance
OS	Included
Hardware	Included (1U rackmount and smaller desktop formats)
License	Commercial
SCAP Validated	
Standards	CVE
Supplier	IBM
Information	*http://www-01.ibm.com/software/tivoli/products/network-enterprise-scanner/*

Infiltration Systems Infiltrator 2009

Abstract

Infiltrator audits networked hosts for vulnerabilities, exploits, and information enumerations. Infiltrator can reveal and catalog information on scanned computers, such as installed software, shares, users, drives, hot fixes, NetBIOS and SNMP information, open ports, *etc*. Infiltrator can audit each computer's password and security policies, alerting the user when changes should be made to increase security. All results can be captured in a report by the tool's report generator. Infiltrator includes 19 network utilities for footprinting, scanning, enumerating and gaining access to machines. Included utilities are ping sweep, who is lookups, email tracing, brute force cracking tools, share scanning, network enumerating, *etc*.

Infiltration Systems Infiltrator 2009

Type	Network Scanner
Target(s)	
Format	Software
OS	Windows 2000/XP
Hardware	128MB RAM, 3MB Disk
License	Shareware
SCAP Validated	
Standards	
Supplier	Infiltration Systems/Spytech® Software and Design, Inc.
Information	*http://www.infiltration-systems.com/infiltrator.shtml*

Inverse Path TPOL

Abstract

Inverse Path TPOL is a compliance tool for evaluating baseline security of any UNIX based network, based on analyses to detect vulnerabilities defined in OVAL. TPOL enables users to import standard OVAL definitions from any source of vulnerabilities to be sought, and to automatically test the network for presence of those vulnerabilities. TPOL also supports editing and export of OVAL-compliant vulnerability definitions and a wizard for building new definitions. TPOL is scalable to support scanning of networks from very small to enterprise-wide with multiple cluster groups. TPOL's operation is completely agent-less.

Inverse Path TPOL

Type	Network Scanner
Target(s)	Any Portable Operating System Interface for unIX (POSIX)-compliant UNIX system
Format	Software
OS	UNIX
Hardware	128MB RAM, 3MB disk
License	Shareware
SCAP Validated	
Standards	OVAL
Supplier	Inverse Path S.r.l. [Società Responsabilità Limitata] (Italy)
Information	*http://www.inversepath.com/products.html*

Lumension® Scan

Abstract

Lumension Scan is a stand-alone network-based scanning solution that performs an assessment of all the devices connected to your network, both managed and unmanaged. Once all assets are identified, Lumension Scan detects weaknesses on these devices before they can be exploited. Lumension Scan provides: (1) identification and inventory of all devices on the network; (2) scans of all devices for software and configuration-based vulnerabilities; (3) risk-based prioritization of identified threats; (4) continuously-updated vulnerability database for orderly remediation; (5) actionable reports of scan results. The scanner operates by first inventorying all network-connected devices and hosts. It then scans a subset of those (supported targets) for vulnerabilities and configurations (*e.g.,* missing patches). Discovered vulnerabilities are then prioritized and mitigations are identified to assist in the remediation process. Finally, numerous options for reports can be generated, including executive, administrative, and compliance reports.

Lumension Scan

Type	Network Scanner
Target(s)	Cisco (IOS, CatOS, PIX [Private Internet eXchange]); HP (HP-UX 10.x+, Tru64 4.0F+, networked printers), Linux (Fedora® 6/7, Mandriva 7.0/7.1, Red Hat Enterprise 3/4/5, SuSE Open/Enterprise (9/10.0/10.1/10.2/10.3, Oracle Linux 4/5); Mac OS X; UNIX (OpenBSD 3.8+, Solaris 2.5+); Windows (2000, XP, XP Embedded, 2003, 2008, 2008 R2, Vista, 7) (The scanner can discover other network devices, but cannot assess their vulnerabilities.)
Format	Software
OS	Windows (XP Professional SP3+, Vista SP2+, 7, Server 2003 SP2+, Server 2003 R2 SP2+, Server 2008 SP2+; all 32-bit) running Microsoft SQL Server 2008
Hardware	2GHz Pentium-compatible CPU, 2GB RAM, 20GB disk, 100baseT NIC with Internet access, 1024x768 res. monitor
License	Commercial
SCAP Validated	
Standards	
Supplier	Lumension Security, Inc.
Information	*http://www.lumension.com/vulnerability-management/vulnerability-assessment-software.aspx*

McAfee® Vulnerability Manager

Abstract

McAfee Vulnerability Manager scans all networked assets, including smartphones and printers, including assets located in air-gapped and critical infrastructure environments. For secure networks with no external connections, the tool can be installed on a laptop or virtual scanner and used to discover and scan these assets. For dynamic or portable assets, the tool's asset-centric scanning defines scan groups by combinations of IP address ranges, organizations, system types, or other identifiers. The tool also supports shared, centralized credentials for scanning credentialed systems. Vulnerability Manager is also Federal Information Processing Standard (FIPS) 140-2-validated (for SSL cryptographic functions). Vulnerability Manager performs system-level and application-level assessments that include database banners, policy settings, registry keys, file and drive permissions, and running services. It can scan more than 450 operating system versions for vulnerabilities. Vulnerability Manager includes predefined checks with frequent updates for zero-day threats. The user can also write custom scripts and checks for scanning proprietary and legacy programs. McAfee Vulnerability Manager performs deep Web application scanning that includes checks for vulnerabilities in the 2010 OWASP Top 10 and CWE 25. McAfee Vulnerability Manager also enables administrators to manage Web applications as if they were traditional network based assets—they can be grouped, and assigned criticalities, asset owners, and personalities. The tool's inspections also detect malicious content, including Trojans, viruses, and other malware. Some organizations centralize, some prefer a distributed environment. The console enables the user to monitor the progress of hundreds of remote scanning engines in a consolidated view of vulnerability status for the entire network; the user can also define separate scan environments and aggregate selected data after the fact. Through an open API, McAfee Vulnerability Manager can be integrated with in-house or third-party products, including trouble ticketing, remediation, security information and event management (SIEM), and configuration and patch management systems. Beyond identifying vulnerabilities, the tool can direct patching efforts through its single correlated, actionable vulnerability status view. Vulnerability Manager also visualizes and ranks the risk potential of new threats based on existing network configuration data and risk scores. The tool also uses the McAfee FoundScore risk formula algorithm that considers asset criticality, risk ratings of discovered vulnerabilities, resource type, and other variables to calculate a risk grade for each asset. Assets to be graded can be selected based on criticality and scanned with one click. As the scans run, McAfee Vulnerability Manager displays the target's software or confirms that appropriate intrusion prevention is in place. Failed scans and systems not scanned are documented, along with those determined to be "not vulnerable". Both scans and reports can be tailored in many ways, to support data analysis; the McAfee ePolicy Orchestrator query and report engine can also be used to aggregate, filter, organize, and distribute scan results. McAfee also provides a Vulnerability Assessment SaaS.

McAfee Vulnerability Manager

Type	Network Scanner
Target(s)	
Format	Appliance or Software
OS	Windows 2003 Server (32-bit) SP2+; can run on VMware® VI3/vSphere Elastic Sky X (ESX/ESXi); must have Microsoft SQL Server 2005 SP2+ with all hot fixes/patches
Hardware	x86 2GHz+ multi-core (quad-core recommended) CPU, 2GB RAM (4GB recommended), 80GB+200GB disk
License	Commercial
SCAP Validated	*http://nvd.nist.gov/validation_mcafee.cfm*
Standards	SCAP, OVAL, CVE, CVSS
Supplier	McAfee
Information	*http://www.mcafee.com/us/products/vulnerability-manager.aspx*

nCircle® IP360

Abstract

nCircle IP360 is a component of nCircle's security risk and compliance management suite. Using agentless technology, IP360 profiles all networked devices and tests for the presence of more than 40,000 conditions (OSs, applications, vulnerabilities, configurations). IP360 includes integrated Web application scanning to identify security risk in Web applications. IP360 provides, as an option, the nCircle Perimeter Profiler (a cloud-based virtualized appliance) to scan Internet facing assets for network, operating system, and Web application vulnerabilities, in the same way it scans assets on the internal network. Another option for IP360 is nCircle Focus, a reporting tool that enables security analysts to identify systems vulnerable to a specific threat(s), location and ownership of vulnerable systems, comprehensive host information (including OS, applications/versions, open ports, protocols, and host tracking information), and current and historic vulnerability trend status for specific systems. The IP360 command and control API, XML remote procedure call (XML RPC) over HTTPS enables external programs/systems to access its endpoint intelligence, providing for integration with asset management systems, Microsoft Active Directory, SIEM systems, and network behavioral analysis solutions. The API supports two-way data flows, and control of IP360 functions from the external systems with full support for user authentication, authorization, auditing, and multiple control sessions (including command-line control of IP360 functions). nCircle IP360 attained a Common Criteria EAL3 certification in May 2005. nCircle also provides network vulnerability scanning through its HITRUST Security and Configuration Audit Service.

nCircle IP360

Type	Network Scanner
Target(s)	
Format	Appliance
OS	
Hardware	
License	Commercial
SCAP Validated	*http://nvd.nist.gov/validation_ncircle.cfm*
Standards	SCAP, OVAL, CVE, CVSS
Supplier	nCircle Network Security, Inc.
Information	*http://www.ncircle.com/index.php?s=products_ip360*

netVigilance SecureScout® SecureScout Easybox 2.0 Scanner

Abstract

The netVigilance SecureScout Easybox (formerly EagleBox) Scanner appliance employs the same vulnerability assessment and management technology as other SecureScout editions. Easybox users can customize localization, reporting, scan scheduling, and software loading. Customer scanning profiles are built with advance calendaring, resource grouping, prioritization of vulnerabilities, and load adjustment. The Web interface to the SecureScout Easybox Manager (separate appliance) allows security administrators to securely access and control Easybox from any browser. This interface can be customized to a user-defined look and feel. Easybox Scanner can also interface with Easybox Ticketer, which provides interfaces to trouble ticketing systems such as Remedy and netVigilance SecureScout WinRT.

netVigilance SecureScout Easybox 2.0 Scanner

Type	Network Scanner
Target(s)	
Format	Appliance
OS	
Hardware	
License	Commercial
SCAP Validated	*http://nvd.nist.gov/validation_ncircle.cfm*
Standards	CVE
Supplier	netVigilance, Inc.
Information	*http://www.netvigilance.com/easybox*

netVigilance SecureScout® (Enterprise Edition)

Abstract

netVigilance SecureScout (Enterprise Edition) (formerly Secure Scout NX) probes the entire enterprise network to identify vulnerabilities and outline remediations. The network scan can be performed from a remotely located central SecureScout console, which manages the remote test engines and probes. Vulnerabilities across distributed networks can be repeatedly scanned and reported to the central console. Scans also collect detailed firewall configuration information for incoming and outgoing packets. This enables reverse engineering of any firewall's filtering rules. The scanner is also capable of actively probing all types of network-connected machines, and can determine differences between the rules/protocols implemented in the scanned nodes and the enterprise's written security policies. And, as with all SecureScout scanners, the test case database is continually updated with new vulnerabilities in a wide range of systems and services, researched by SecureScout's security experts. All test cases are CVE-compliant.

netVigilance SecureScout (Enterprise Edition)

Type	Network Scanner
Target(s)	
Format	Software
OS	Windows (2000 Pro/Standard Server/ Advanced Server with SP3/SP4; XP Pro SP1-SP3; Server 2003 Standard/ Enterprise SP0-SP2); all versions: 32-bit only; running Microsoft SQL Server 2000 Desktop Engine SP3 (provided by netVigilance with SecureScout shipment)
Hardware	(Based on Easybox configuration) 2GHz Pentium IV, 256MB RAM, 10/100/1000Mbps NIC
License	Commercial
SCAP Validated	
Standards	CVE
Supplier	netVigilance, Inc.
Information	*http://www.netvigilance.com/ enterpriseedition*

netVigilance SecureScout® (Windows Edition)

Abstract

The architecture of netVigilance SecureScout (Windows Edition) (formerly Secure Scout SP) is based on distributed remote agents on different network segments, that enable multiple scans to be conducted in parallel, with the results being collated in a central database (open database format). SecureScout (Windows Edition) is a multi-user solution; individual users have access to scans of their own network segments, including retrieving reports and managing scheduling and loading. In this way, the vulnerability assessment can be divided among several users, sites, and/or organizations, with different scans being protected by strong access controls and encryption. The scanner's differential reporting capability enables users to benchmark the network's security level at various points in time. Customer scanning profiles can be built with advance calendaring, resource grouping, prioritization of vulnerabilities, and load adjustment. SecureScout SP allows you to configure scanning profiles. Scanning results are available in an open database format. As with other SecureScout products, SecureScout (Windows Edition)'s test case database is frequently updated based on SecureScout security experts' research into new vulnerabilities.

netVigilance SecureScout (Windows Edition)

Type	Network Scanner
Target(s)	
Format	Software
OS	Windows (2000 Pro/Standard Server/ Advanced Server with SP3/SP4; XP Pro SP1-SP3; Server 2003 Standard/ Enterprise SP0-SP2); all versions: 32-bit only; running SQL Server 2000 Desktop Engine SP3 (provided by netVigilance with SecureScout shipment)
Hardware	(Minimum requirements, based on Easybox configuration) 2GHz Pentium IV, 256MB RAM, 10/100/1000Mbps NIC
License	Commercial
SCAP Validated	
Standards	CVE
Supplier	netVigilance, Inc.
Information	*http://www.netvigilance.com/ windowsedition*

NGSSecure NGS Typhon III

Abstract

Next Generation Security (NGS) Typhon III is a non-intrusive vulnerability scanner that provides security auditing, *via* pause-and-resume scanning, of all hosts on a network, from routers and printers to Web and database servers. Typhon III exposes weak passwords in a variety of protocols, and performs a broad range of checks for common vulnerabilities, exploits, and configuration errors, including the SANS Top 20, worms, rootkits, phishing and pharming attacks, data theft, and SQL injection. Typhon III can audit Web applications *via* its integrated Web spider, which locates every page and script on a Web site, including hidden, unlinked, and test files, and tests for SQL injection and XSS flaws. Reports can be generated in plaintext, Rich Text Format (RTF), Hyper Text Markup Language (HTML), XML, and ODBC source formats. One-click fixes generate lockdown scripts for registries.

NGSSecure NGS Typhon III

Type	Network Scanner
Target(s)	TCP/IP network services; Web protocols, NetBIOS, Lightweight Directory Access Protocol (LDAP) servers, Network File System (NFS) servers, UNIX servers, Cisco ISO, Lexmark® Printer Admin, MySQL, SQL Server , Oracle, DB@, Windows, IE
Format	Software
OS	Windows
Hardware	
License	Commercial
SCAP Validated	
Standards	
Supplier	NGSSecure (UK)
Information	*http://www.ngssecure.com/ngssecure/services/information-security-software/ngs-typhon-III.aspx*

NileSOFT Secuguard NSE

Abstract

NileSOFT Secuguard NSE is an agent-based network vulnerability assessment tool that automatically detects the system's IP address and OS to automatically generate a security scan policy for the system. The automatically generated scan policy provides for an automated scan procedure; policies can target specific individuals, groups, operating systems, *etc.* Additionally, multiple Windows, UNIX, and Linux hosts or network devices (*e.g.,* routers) can be scanned simultaneously by a single agent, and multiple multi-host scans can be managed from a single console; the system also supports multiple consoles operating in parallel. Vulnerabilities detected include operating system and network service level vulnerabilities. Scan reports show the risk level, description, impact, and remedy for each detected vulnerability, along with references to further information. More than 14 different reports are provided (sorted by group, risk level, *etc.*), with graphs/tables generated by Crystal Reports 9. Reports can be exported to HTML, RTF, plaintext, Microsoft Word (.doc) and Excel® (.xls), PDF, and other formats. Updates of scan modules can be automatic, prescheduled for a specific time each day, or can be offline (for updating modules that have no Internet access). One or more update servers can be installed on closed networks.

NileSOFT Secuguard NSE

Type	Network Scanner
Target(s)	
Format	Software
OS	Console: Windows (NT/95/98/2000/Me/XP), UNIX, Linux Agents: Linux, Solaris
Hardware	Hardware Console: 30MB disk Agent: 10MB disk
License	Commercial
SCAP Validated	
Standards	CVE
Supplier	NileSOFT (South Korea)
Information	*http://www.nilesoft.co.kr/eng/product/nse.htm*

NSasoft Nsauditor

Abstract

NSasoft Nsauditor is a network security auditor and vulnerability scanner that scans, detects, and corrects potential security risks on the network. Nsauditor allows monitoring network computers for problems that might be exploited as vulnerabilities, checking the enterprise network for potential methods that a hacker might use to attack it, and creating a report of problems found; the tool creates its audit report in HTML and XML formats. Nsauditor also includes a packet filtering firewall, realtime network monitor, and network IDS, along with other network analysis, monitoring, and management utilities.

NSasoft Nsauditor

Type	Network Scanner
Target(s)	
Format	Software
OS	Windows 7/2000/XP/2003/Vista
Hardware	
License	Commercial
SCAP Validated	
Standards	
Supplier	NSasoft Limited KLiability Corporation (LLC) (Armenia)
Information	*http://www.nsauditor.com/network_security/network_security_auditor.html*

Safety-Lab Shadow Security Scanner

Abstract

Safety-Lab Shadow Security Scanner is able to detect vulnerabilities in networked computers associated with the many TCP/IP network services and applications (*e.g.,* FTP, SSH, Telnet, SMTP, LDAP, HTTPS, SSL, *etc.*) and Windows Registry services. It can perform simultaneous scans of up to 10 hosts per network scanning session. The tool architecture is ActiveX®-based, enabling its out-of-the-box capabilities to be extended by developers using Visual C++, C++ Builder, or Delphi. Non-developers can use the tool's API and BaseSDK [software developer's kit] wizard to control the tool's operation, change its properties or functions, or create 95% of the same new audits that can be added through developer programming. Scan results (session logs) are saved in HTML by default, but the tool can be configured to save them in XML, PDF, RTF, or Compiled HTML (CHM) format.

Safety-Lab Shadow Security Scanner

Type	Network Scanner
Target(s)	Networked hosts running UNIX, Linux, FreeBSD, OpenBSD, NetBSD, Solaris, Windows (95/98/Me/NT/2000/XP, with or *without .NET*); Cisco, HP, and other (not identified) networking devices
Format	Software
OS	Windows 95/98/ME/NT/2000/XP/2003/Vista/7
Hardware	Included
License	Commercial
SCAP Validated	
Standards	
Supplier	Safety-Lab (Russia)
Information	*http://www.safety-lab.com/en/products/securityscanner.htm*

Security System Analyzer 2.0 Beta

Abstract

Security System Analyzer is a free, non-intrusive OVAL, Federal Desktop Core Configuration (FDCC), XCCDF, and SCAP scanner. It can identify vulnerabilities and security discrepancies through its OVAL interpreter and large database of OVAL vulnerability definitions. Findings can be output in XML or HTML.

Security System Analyzer 2.0 Beta

Type	Network Scanner
Target(s)	Networked hosts running Windows (XP, Vista, 7); IE 7/8, Vista and XP Firewalls
Format	Software
OS	
Hardware	
License	Open source
SCAP Validated	
Standards	OVAL, CVE
Supplier	NETpeas, Societe Anonyme (SA) (Morocco)
Information	*http://code.google.com/p/ssa*

StillSecure® VAM 5.5

Abstract

StillSecure VAM identifies, tracks, and manages the repair of network vulnerabilities across the enterprise wired and wireless network segments. The system, which includes VAM Server and VAM Console, provides (1) device discovery/inventory, with new devices automatically added to appropriate existing scan lists/groups; (2) vulnerability scanning of devices (identified by IP address, OS, Dynamic Host Configuration Protocol (DHCP) device, group, scanner name, discovery date, device priority, NetBIOS identifier, *etc.*) using a rule set of more than 9,000 vulnerability tests, (3) repair/mitigation management with threat prioritization and repair scheduling and assignment; (4) compliance reporting using the optional Security Point of View reporting module; (5) LDAP/Active Directory integration (for user authentication). StillSecure scans can be remote launched from within other security tools/servers *via* the VAM Integration Framework, through which it can be integrated with trouble ticketing, patch management, asset inventory, vulnerability scanning, IDS or Intrusion Prevention System (IPS), network management, change management, security information management, and other such systems. StillSecure also provides a software developer's kit for custom development of additional extensions (StillSecure will also develop custom connections on request). VAM's Extensible Plug-in Architecture also enables customization of the repair/mitigation workflow through user-created scripts. The system also supports daily archiving of the VAM database, which can be offloaded to other media or devices, plus integration with third-party backup tools. StillSecure VAM has been certified at Common Criteria EAL2, and has been FIPS 140-2-validated (for VAM's SSL connections).

StillSecure VAM Server 5.5

Type	Network Scanner
Target(s)	TCP/UDP/IP networks and networked hosts running Linux (including Red Hat), Solaris, HP-UX, AIX, Windows
Format	Server: Appliance or Software Console: Software
OS	Server: Included (hardened Linux with MySQL database and Java® Database Connectivity) Console: Linux or Windows running Firefox 0.9.3+ or Mozilla® 1.7+ or Windows running IE 6.0+ (browser must support 128-bit encryption)
Hardware	VAM Server: 1.3GHz minimum (2GHz recommended) Intel Pentium® 4, 512MB RAM (1GB recommended), 36GB disk, 10/100baseT NIC (3Com or Intel), CD-ROM drive
License	Commercial
SCAP Validated	
Standards	
Supplier	StillSecure®
Information	*http://www.stillsecure.com/vam/risk.php*

Xacta® IA Manager

Abstract

Xacta IA Manager is a continuous risk management framework that automates asset discovery and inventory, configuration security assessment, SCAP and FDCC compliance auditing, and OVAL-based vulnerability assessment across the enterprise. Xacta IA Manager is hardware intensive; each of the server components is distributed across two hardware platforms, one of which hosts the application and the second of which hosts the associated database. In addition, software agents must be installed on every platform to be targeted in Xacta IA Manager vulnerability and configuration/compliance scans. The components of Xacta IA Manager that perform vulnerability scans are Xacta Detect and Xacta HostInfo, cooperating with Xacta Asset Manager (IA Manager's central repository for asset and configuration management information). Xacta Detect provides a set of integrated scanning utilities to manage configuration and vulnerability scans, with multiple Xacta Detect servers aggregating information from across the enterprise network for delivery to Xacta Asset Manager. Xacta HostInfo is the agent software that runs on every target host to locally execute the scanning scripts (which are, in fact, OVAL definitions) and returning the results in HTML format to the Xacta Detect server. The results for each vulnerability found include a hyperlinked reference to additional information in the NVD, indexed by CVE identifier; the NVD provides the CVSS base score associated with the vulnerability. Xacta Detect + HostInfo also enable SCAP and FDCC security configuration compliance checking by executing rules provided in SCAP-based benchmarks and providing results in an XCCDF-formatted output file. Xacta Detect can be set to perform continuously scanning of endpoint systems for patches and vulnerabilities, or scans can be scheduled at user-programmable intervals, based on time or event triggers. Xacta IA Manager also includes Xacta Publisher and Xacta Templates, which together can automatically generate correctly-formatted compliance reports and Certification and Accreditation (C&A) documents in support of Defense IA C&A Process (DIACAP), and compliance auditing for NIST SP 800-53, Committee for National Security Systems (CNSS) Policy #22, Federal Information Security Management Act (FISMA), International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 27002, *etc.* The OS and hardware requirements described below are for Xacta Detect, Asset Manager, and HostInfo components only. Requirements for the other components of Telos Xacta IA Manager can be found at the second URL in the table below.

Telos Xacta IA Manager

Type	Network Scanner
Target(s)	Networked hosts running Windows 2000/XP/2003/2008/Vista; Mac OS X 10.4 (HostInfo legacy versions available for UNIX, Red Hat Enterprise Linux, Solaris)
Format	Software
OS	Asset Manager Application: Windows Server 2003 64-bit/2008 64-bit Asset Manager Database: Windows Server 2003/2008 or UNIX running SQL Server 2005/2008 or Oracle 10g/11g Detect Server Application: Windows Server 2003/2008 Detect Server Database: Windows Server 2003/2008 or UNIX running Microsoft SQL Server 2005/2008 or Oracle 10g/11g HostInfo Agents: Windows 2000/XP/2003/2008/Vista; Mac OS X 10.4 running Java Runtime Environment (JRE)1.5+
Hardware	Asset Manager Application: 2.6GHz+ dual core CPUs; 8GB RAM; 200GB disk Asset Manager Database: 2.6GHz+ dual core CPUs; 8GB RAM (up to 10,000 targets)/16GB RAM (for > 10,000 targets); 300GB disk Detect Server Application: 2.6GHz+ dual core CPUs; 8GB RAM; 100GB disk Detect Server Database: 2.6GHz+ dual core CPUs; 8GB RAM; 200GB disk
License	Commercial
SCAP Validated	*http://nvd.nist.gov/validation_telos.cfm*
Standards	SCAP, OVAL, CVE, CVSS
Supplier	Xacta Corporation/Telos® Corporation

Information	*http://www.telos.com/cybersecurity/grc/continuous-assessment/index.cfm* *http://www.telos.com/cybersecurity/grc/features/index.cfm*

ZOHO® ManageEngine® Security Manager Plus Network Security Scanner component

Abstract

The core functions of the Network Security Scanner component of ZOHO ManageEngine Security Manager Plus are vulnerability scanning and detection of industry-known vulnerabilities in network assets, and recommendation of vulnerability remediation solutions. Security Manager Plus can scan assets and asset groups, display complete security information about vulnerable assets, e-mail scan reports, and implement appropriate remediation solutions provided. Assets and groups of assets can be scanned by hostname, IP address, or address range, or scans can be targeted to find selected groups of vulnerabilities. The scanner enables the user to enter asset login credentials which allows scanning of access-controlled assets, and to schedule periodic scans for assets and asset groups. The console presents a pie-chart depicting percentages of assets affected by high, medium, and low risk vulnerabilities, as well as the percentage of assets with "for your information" issues that are not considered risks now, but which could be exploitable by emerging threats. The console also provides suggested remediations for detected vulnerabilities, and generates audit reports by asset or vulnerability group. The tool can run unattended, and send a notification upon scan completion. Reports can be selectively sent to administrators, IT managers, auditors, and others. Security Manager Plus can also be configured to automatically generate and email trouble tickets when certain pre-defined criteria are met. The console dashboard displays the most vulnerable assets and asset groups, the most prevalent vulnerabilities found in the network, and the latest known vulnerabilities (based on the most recent scan database update). Security Manager Plus comprises two components: Server and Agent. The agents must be installed on all target systems.

ZOHO ManageEngine Security Manager Plus Network Security Scanner component

Type	Network Scanner
Target(s)	TCP/IP networks
Format	Software
OS	Server: 32-bit Windows Vista (Business/Ultimate), XP Pro, Server 2008, Server 2003, Red Hat Linux (7.2/8.0/9.0), Enterprise Linux AS/ES (2.1, 3.0, 4.0), Debian® GNU Linux 3.0/3.1 Agent: 32 or 64-bit Windows 7, Server 2008 (SP1/SP2/R2), Server 2003, XP Pro, NT SP6a (WS/Server), 2000 Pro/Server
Hardware	Server: 1.8 GHz 32-bit Pentium, 512 MB RAM, 10GB+200MB disk, 56 thousand bits per second [bps] (Kbps)+ Internet connection (for updates) Agent: 1.8 GHz Pentium, 256MB RAM; 50MB disk
License	Commercial
SCAP Validated	
Standards	
Supplier	ZOHO Corporation/ManageEngine
Information	*http://www.manageengine.com/products/security-manager/network-security-scanner.html*

HOST SCANNERS

Assuria Auditor and Auditor RA

Abstract

Assuria Auditor is an agent-based system that uses a built-in knowledge base of known security vulnerabilities, security control configurations, up-to-date patch checks, and security best practice information to perform thousands of individual checks across a wide range of operating platforms. The knowledge base can be extended through a customization interface that enables addition of new checks, modification of existing checks, and creation of custom policies. Reports include explanations of the implications of each vulnerability and step-by-step instructions on remediation, along with CVE and Bugtraq identifier (ID) references, and CVSS scores where appropriate. Assuria Auditor also performs security configuration checks that conform with ISO 27001, PCI DSS, Sarbanes-Oxley, and numerous other standards and regulations. The tool can also be configured to check compliance with internal policies and build standards. Change detection features allow assessment and reporting of suspicious or potentially troublesome changes; assessments can be applied to whole systems and subsystems (*i.e.,* baselines) or to specific resources, down to individual files, folders, and executables (*i.e.,* file integrity monitoring). Assuria Auditor RA provides the same functionality in an agentless architecture, using remote scanning, including remote credentialed scanning.

Assuria Auditor and Auditor RA

Type	Host Scanner
Target(s)	Auditor: Windows (NT, 2000, Server 2003/2008/2008 R2); UNIX (Solaris 7-10x86 for SPARC®); [Scalable Performance ARChitecture] AIX 5.1-6.1; HP-UX for PA-RISC [Reduced Instruction Set Computer] or Itanium 11+); Linux (Red Hat Enterprise 3/4, SuSE Enterprise X86 and 10 IBM Z series); VMware ESX 3.5/4.1 Auditor RA: Windows (Server 2003 32-bit, Server 2008 64-bit, Server 2008 R2 64-bit, 7); Linux (Red Hat ES 3/4 32 & 64-bit, ES 5 64-bit only, SuSE Linux Enterprise systems); VMware ESX/ESXi 4
Format	Software
OS	Auditor Agents: Windows (NT, 2000, Server 2003/2008/2008 R2); UNIX (SPARC Solaris 7-10x86); IBM AIS 5.1-6.1; HP-UX PA-RISC or Itanium 11+); Linux (Red Hat Enterprise 3/4, SuSE Enterprise X86 and 10 IBM Z series); VMware ESX 3.5/4.1 Auditor/Auditor RA Console: Windows Server 2003/2008/2008 R2 x64 running Microsoft SQL Server 2005/2008
Hardware	
License	Shareware
SCAP Validated	
Standards	CVE, CVSS
Supplier	Assuria, Ltd. (UK)
Information	*http://www.assuria.com/products-new/assuria-auditor.html* *http://www.assuria.com/products-new/assuria-auditor-ra.html*

Infiltration Systems Infiltrator for Home Users

Abstract

Infiltrator for Home Users provides the same security scanning and auditing features as the networked Infiltrator 9000 scanner, but is installed and licensed for use on a single computer. Infiltrator for Home Users can quickly audit a home computer for vulnerabilities, exploits, and information enumerations. Infiltrator can reveal and catalog information on the scanned computer, such as installed software, shares, users, drives, hot fixes, NetBIOS and SNMP information, open ports, *etc.* Infiltrator can audit the computer's password and security policies, alerting the user when changes should be made to increase security. All results can be captured in a report by the tool's report generator. Infiltrator includes 19 utilities for footprinting, scanning, enumerating and gaining access to home computers. Included utilities are ping sweep, who is lookups, email tracing, brute force cracking tools, share scanning, network enumerating, *etc.*

Infiltration Systems Infiltrator for Home Users

Type	Host Scanner
Target(s)	
Format	Software
OS	Windows 2000/XP
Hardware	128MB RAM, 3MB disk
License	Shareware
SCAP Validated	
Standards	
Supplier	Infiltration Systems/Spytech Software and Design, Inc.
Information	*http://www.infiltration-systems.com/infiltrator-home.shtml*

Microsoft® Attack Surface Analyzer

Abstract

Microsoft Attack Surface Analyzer was developed by the Microsoft Security Engineering group. It is the same tool used by Microsoft's internal product groups to catalogue changes made to operating system attack surface by the installation of new software. Attack Surface Analyzer takes a snapshot of the system's state before and after the installation of new product(s) and displays the changes to a number of key elements of the Windows attack surface. This allows (1) software developers to view changes in the attack surface resulting from the introduction of their code on to the Windows platform; (2) information technology (IT) professionals to assess the aggregate attack surface change caused by the installation of an organization's line of business applications; (3) security auditors to evaluate the risk posed by installing a particular piece of software on the Windows platform; (4) IT security incident responders and forensic investigators to gain a better understanding of changes in the state of a system's security from the time a baseline scan was taken of the system during its deployment phase.

Microsoft Attack Surface Analyzer

Type	Host Scanner
Target(s)	Windows 7, Vista, Server 2008 R1/R2
Format	Software
OS	Windows 7
Hardware	x86, IA64, x64
License	Freeware
SCAP Validated	
Standards	
Supplier	Microsoft Corporation
Information	*http://www.microsoft.com/downloads/en/details.aspx?FamilyID=1283b765-f57d-4ebb-8f0a-c49c746b44b9*

NileSOFT Secuguard SSE

Abstract

NileSOFT Secuguard SSE is a host-based vulnerability assessment tool that uses an internal agent installed on the scan target to scan the system for known vulnerabilities, and provide the user with remedies and additional information. The scanner's capabilities include password cracking, support for various scan policies (individual, group, operating system, *etc.*), detecting vulnerabilities and user errors, file integrity checks. The scanner's findings include risk level, description, impact, remedy, and references to further information for each detected vulnerability. Simultaneous multi-target scans can be controlled from a single console, and multiple consoles can be deployed on the same network, with different privileges set according to server administrator rights. Fully automated scans can be scheduled in advance, with email sent to the user when the scan has completed. Scan report findings can be sorted by 14 parameters, including vulnerability group, target operating system, risk level, *etc.* Scan report graphs/tables are generated by Crystal Reports 9, and report content can be exported in HTML, RTF, plaintext, Word, Excel, PDF, and other formats. Scan modules are automatically updated by the update server (update time can be scheduled), and offline updates can also be supported for non-Internet-connected scanners; update servers can be installed on closed networks.

NileSOFT Secuguard SSE

Type	Host Scanner
Target(s)	UNIX (UNIXware 7.x, OpenUNIX, FreeBSD, Solaris 2.x, AIX 4.x-5.x, HP-UX 10.x-11.x, Tru64, other UNIX versions), Linux (Red Hat 6.x-7.x, Power Linux, OpenLinux), Windows (NT, 2000, XP, Server 2003)
Format	Software
OS	Console: Windows NT/2000/XP Agent: see list of targets
Hardware	Console: 300MB disk (500MB recommended) Agent: 50MB disk (100MB recommended)
License	Commercial
SCAP Validated	
Standards	CVE
Supplier	NileSOFT (South Korea)
Information	*http://www.nilesoft.co.kr/eng/product/sse.htm*

Numara® Vulnerability Manager

Abstract

Numara Vulnerability Manager is one part of a fully integrated line of IT asset management solutions that make up the Numara Asset Management Platform. Numara Vulnerability Manager automates the entire vulnerability management process from detection to remediation to verification. It uses a built-in, continually-updated CVSS and CVE library of vulnerabilities to perform comprehensive vulnerability assessments and analyses. The tool's "scan, click, and fix" technology enables the user to perform scans, vulnerability analyses, and prioritization and execution of remediation actions from the same central console. Numara Vulnerability Manager includes an integrated reporting solution with pre-defined standards-/regulatory-compliance formatted reports, executive dashboards, and flexible report customization options. Numara Vulnerability Manager can find and remediate the following vulnerability types: abnormal usage, brute forcing, buffer overflow, denial of service, and Trojan horses, information gathering and "fingering" abuses, misconfiguration, default password settings, and others.

Numara Vulnerability Manager

Type	Host Scanner
Target(s)	Windows, Mac OS, Linux, UNIX, IOS, CatOS
Format	Software
OS	Master server: Windows (2000/03/08/7 (Standard/Web/Enterprise/Small Business Editions)/ XP/Vista, 32 & 64-bit); Linux (Red Hat Enterprise 4/5, SuSE 10, CentOS 4/5, Debian 5); can run on VMware ESXi, VMware Infrastructure, and Microsoft Hyper-V Core Server 2008 R2 with same OS/database Database server: Same OSs, with SQL Server 2005/2008 R2 (Express, Standard, Enterprise) 32/64-bit; Oracle 9i or 10g; PostgreSQL 8/9 Client and Relay: Windows 2000 Pro SP4, Server 2000/2003/2008 (Standard, Web, Enterprise, Small Business), XP, Vista SP1, 7 32 & 64-bit; Linux (Red Hat Enterprise 4/5, SuSE 10/11, CentOS 4/5, Debian 4, Ubuntu 10.04); Console requires JRE 1.6+ (included with tool software); on Windows 64-bit OS JRE 1.6 update 17+
Hardware	Master Server, <500 targets: Pentium 2.2GHz Core 2 Duo x86, 2GB RAM, 50GB disk; 500-2,000 targets: 3.2GHz Pentium Core 2 Duo x64, 4GB RAM, 100GB disk; 2,001-10,000 targets: 3.2GHz Xeon® Dual Core x86, 4GB RAM, 100GB disk; >10,000 targets: enquire Separate Database Server, <500 targets: not needed; 500-2,000 targets: 3.2GHz Pentium Core 2 Duo x64, 4GB RAM, 80GB disk; 2,001-10,000 targets: 3.2GHz Xeon® Dual Core x86, 4GB RAM, 80GB disk; >10,000 targets: enquire Relay (1 per every 2,000 nodes), <500 targets: not needed, but if desired, Pentium D, 1GB RAM, 10GB disk; 500-10,000 targets: 2.2GHz Pentium Core 2 Duo x86, 2GB RAM, 50GB disk; >10,000 targets: enquire
License	Commercial
SCAP Validated	
Standards	
Supplier	Numara Software, Inc.
Information	*http://www.numarasoftware.com/asset_management/vulnerability_manager/*

Proland Protector Plus Windows Vulnerability Scanner

Abstract

Proland Protector Plus Windows Vulnerability Scanner checks a Windows system for known vulnerabilities, lists the vulnerabilities detected with their risk levels, and the download locations of the patch(es) to install to remediate them. It also creates the log file for future reference.

Proland Protector Plus Windows Vulnerability Scanner

Type	Host Scanner
Target(s)	
Format	Software
OS	Windows Vista, XP, 2000 Pro/Server, 2003 Server, 7
Hardware	
License	Freeware
SCAP Validated	
Standards	
Supplier	Proland Software (India)
Information	*http://www.pspl.com/download/winvulscan.htm*

SoftRun Inciter Vulnerability Manager

Abstract

SoftRun Inciter Vulnerability Manager is a vulnerability assessment tool that profiles basic system information (computer name, operating system, IP and MAC addresses), then detects the security vulnerability of computer systems to hacking attacks and other crimes in cyber space. Inciter Vulnerability Manager provides users with information that enables them to arrange highly sophisticated security management policies by identifying the security risk status of scanned systems. Scans can be customized to include or exclude various targets, to search for vulnerabilities of a certain type (identified by CVE ID). The tool generates vulnerability scan reports that include significance of detected vulnerabilities, vulnerability IDs (CVE, Microsoft Bulletin, Security Focus Bugtraq, SANS), and detailed descriptions, with links to relevant Web-based information on each vulnerability. Reports can also be generated that give the number of all detected vulnerabilities, and that sort vulnerabilities according to severity. The scan results can also be exported as plaintext.

SoftRun Inciter Vulnerability Manager

Type	Host Scanner
Target(s)	Microsoft operating systems and applications
Format	Software
OS	Windows (2000, Server 2003/2008, XP, Vista)
Hardware	
License	Commercial
SCAP Validated	
Standards	CVE
Supplier	SoftRun, Inc. (South Korea)
Information	*http://www.softrun.com/en/vulnerability_info.asp*

ThreatGuard® Secutor

Abstract

ThreatGuard's Secutor is a family of SCAP compliance auditing and patch and vulnerability scanning tools. The basic Secutor product, Secutor Prime performs vulnerability assessments of operating systems and major applications, identifying each detected vulnerability by CVE name, with a NVD Web page link for each. The tools also automatically determine whether all required security patches are in place. The tool is updated automatically to ensure its application and assessment content remain current. The tool also performs security configuration auditing, and can directly consume NIST-developed SCAP content files, and provide a mapping of its security checks to CCE identifiers. It automatically generates FDCC deviation reports in XML and HTML, as well as runtime notes that can be used by auditors/security engineers to verify and validate the tool's assessment findings. Deviations can be tracked across multiple targets, and reports generated, from a single desktop. ThreatGuard guarantees that it will add any new government-required reporting capabilities free of charge. In addition to the base functions of Secutor Prime, Secutor Magnus is fully automated to perform continuous assessments and can support virtualization containers to operate "in the cloud." Magnus, as well as Secutor Auditor, Prime Pro, and CAT also perform agentless network-based assessments, and consume OVAL notes metadata as the basis for the vulnerability assessments they perform; they can also perform assessments of non-Windows targets. Magnus and CAT also support Abuse Reporting Format. Secutor MD is intended for use in healthcare/medical establishments, and adds to Secutor Prime the ability to assess targets' compliance with Health Insurance Portability and Accountability Act (HIPAA). Secutor Prime, Prime Pro, and MD also support automated remediation of vulnerable desktops.

ThreatGuard Secutor

Type	Host Scanner
Target(s)	Windows; UNIX (Solaris, HP-UX); Linux (Red Hat Enterprise); Cisco IOS
Format	Software
OS	Windows 2003, 2008 Server, XP, Vista
Hardware	
License	Commercial
SCAP Validated	*http://nvd.nist.gov/validation_threatguard.cfm*
Standards	SCAP, CVE, OVAL, CVSS
Supplier	ThreatGuard, Inc.
Information	*http://threatguard.com/products/*

Key Resources VAT

Abstract

Key Resources VAT is designed to probe IBM z/Series z/OS® environments for vulnerabilities and identifies violations of the IBM z/OS statement integrity ("integrity exposures"). VAT flags integrity exposures found in supervisor call interfaces, operating system exits, program call routines, linkage index interfaces, and programs authorized by the system's Authorized Program function. VAT provides assurance that statement integrity vulnerabilities cannot be exploited by system users or third-party applications to bypass the security controls implemented for z/OS by IBM RACF® or External Security Manager from CA (formerly Computer Associates), *e.g.,* CA-ACF2 (Advanced Communications Function Version 2) ; CA-Top Secret. VAT automatically generates a list of integrity exposures that can then be reported to IBM, third-party vendors, or the organization's internal development or support team.

Key Resources VAT

Type	Host Scanner
Target(s)	IBM z/Series z/OS
Format	Software
OS	IBM z/OS
Hardware	IBM mainframe running z/OS
License	Commercial
SCAP Validated	
Standards	
Supplier	Key Resources, Inc.
Information	*http://www.vatsecurity.com/VAT_Software.html*

DATABASE SCANNERS

Application Security AppDetectivePro

Abstract

AppDetectivePro is an agentless database vulnerability scanner. AppDetectivePro's Database Discovery module can operate without database logins or other knowledge to scan and identify every database on the network by vendor and release level. AppDetectivePro's policy-driven scanning engine identifies vulnerabilities and misconfigurations, including default or weak passwords, missing patches, poor access controls, and many other conditions. Auditors can choose between credential-less scanning for a "hackers eye view" of the database, or credentialed scanning facilitated by an authenticated read-only database account. AppDetectivePro includes built-in templates to satisfy requirements of various regulatory and "mandated guidance" compliance initiatives (*e.g.,* NIST 800-53/FISMA, PCI DSS, others). AppDetectivePro's Pen Test scan does not perform intrusive tests or risky attack simulations; instead, it generates a detailed view of vulnerabilities that could allow an outsider to access the database system. More extensive assessment of database configuration settings are provided by the authenticated Audit scan that identifies all security holes that could allow an outsider access to a database, and provides a detailed view of potential avenues of insider privilege abuse. AppDetectivePro's User Rights scan-based review determines each user's effective privileges, and identifies the data each user can access, the access rights they have (read, write, delete) to that data, and how those access privileges were granted. AppDetectivePro also supports centralization of audit procedures across the organization *via* its Work Plan and Policy Questionnaire, which enable the auditor to capture all control information in a questionnaire, to input password policy controls, to run scans against password parameters, and to independently determine whether a given control is compliant or not. AppDetectivePro's reporting system can generate inventory reports, summary and detailed vulnerability reports, user rights reports, policy reports, and others. Reports can be output in PDF, Excel, Word, SAP [Systeme, Anwendungen, Produkte] Crystal, HTML, XML, and plaintext formats.

Application Security AppDetectivePro

Type	Database Scanner
Target(s)	SQL databases
Format	Software
OS	Windows XP Pro SP2+/Vista/7, running IE 7+, *Optional:* SQL Server 2005/2008
Hardware	1GHz CPU (2GHz recommended), 1GB RAM (2GB recommended), 300MB disk
License	Commercial
SCAP Validated	
Standards	CVE
Supplier	Application Security, Inc.
Information	*http://www.appsecinc.com/products/appdetective/*

DBAPPSecurity MatriXay 3.6

Abstract

MatriXay's database was developed through analysis of typical security vulnerabilities as well as popular attack techniques in Web applications. MatriXay 3.6 performs vulnerability scanning, as well as penetration testing and Trojan detection. The tool's vulnerability scanning can target multiple Web applications, including those with back-end databases, to detect typical Web vulnerabilities (*e.g.,* SQL injection, Xpath injection, XSS, HTML form weak passwords, *etc.*). The tool's Web Trojan detection capabilities can automatically locate numerous linked Trojans and analyze them to determine whether they have the ability to replicate and propagate to other hosts. The tool's penetration testing capability analyzes the target Web application and backend database using a combination of vulnerability discovery and hacker attack methods, including SQL injection. This capability can be used to perform security audits of databases, and to simulate hijacking attacks that exploits weaknesses in the Web application-database interface to obtain database configuration information.

DBAPPSecurity MatriXay 3.6

Type	Database Scanner (with limited pen testing)
Target(s)	Oracle, Microsoft SQL Server, Microsoft Access, IBM DB2
Format	Software
OS	
Hardware	
License	Commercial
SCAP Validated	
Standards	
Supplier	DBAPPSecurity Inc. (China)
Information	*http://www.dbappsecurity.com/Webscan.html*

Fortinet FortiDB

Abstract

Fortinet's FortiDB-400B, 1000C, and 2000B appliances provide scalable database vulnerability assessment and compliance auditing. FortiDB can be deployed with or without FortiDB Agents. Scanning begins with auto-discovery of every database on the network regardless of subnet boundaries, and ends with reporting that includes remediation advice for discovered security weaknesses, and identification of sensitive data in scanned databases.

Fortinet FortiDB

Type	Database Scanner
Target(s)	
Format	Appliance or Software
OS	AIX and Solaris 10, Red Hat Enterprise Linux, Windows XP/Vista/Server 2003, VMware
Hardware	
License	Commercial
SCAP Validated	
Standards	
Supplier	Fortinet, Inc.
Information	*http://www.fortinet.com/products/fortidb/*

Imperva® Scuba

Abstract

Scuba by Imperva is a free, lightweight Java utility that scans databases for known vulnerabilities and configuration flaws. It automates over 350 tests for Oracle, SQL Server, DB2, and Sybase® databases—the same configuration tests and vulnerability assessments developed by the Imperva Application Defense Center research team for Imperva's SecureSphere suite of Data Security Solutions. Scuba is a passive database scanner: it does not exploit vulnerabilities. This means that rather than risking a server crash by actually sending data to potentially vulnerable stored procedure input, Scuba may combine a software version test with a test for the existence of the vulnerable stored procedure and for the users and permissions related to that stored procedure. In this way, Scuba can locate configuration flaws (*e.g.,* weak passwords) across the five main configuration assessment categories: known software flaws, system configuration, privilege management, critical operating system files, and regulatory compliance, along with known security vulnerabilities, and missing critical patches. Scuba's checks and tests provide coverage through its "point-in-time" analysis of the security posture of the database. Scuba analyzes and prioritized all discovered risks, and captures them in both summary reports that indicate overall risk level and detailed reports that capture all test results; reports are issued in Java or HTML formats.

Imperva Scuba

Type	Database Scanner
Target(s)	Oracle, DB2, SQL Server, Sybase
Format	Software
OS	Client: Windows 98/NT/2000/XP running Java JRE 1.5+
Hardware	
License	Freeware
SCAP Validated	
Standards	
Supplier	Imperva Inc. (U.S./Israel)
Information	*http://www.imperva.com/products/dle_downloads-and-evaluations-overview.html*

McAfee Repscan and McAfee Vulnerability Manager for Databases

Abstract

Designed for auditors, penetration testers, database administrators, and security analysts, McAfee Repscan (formerly Sentrigo® Repscan) performs more than 3,000 security checks across databases and database applications, including checks for SQL Injection and buffer overflow vulnerabilities, hard-coded passwords (more than 115 database tables are checked for the presence of password information), deprecated functions, *etc.* The tool also detects weak, shared, and default passwords, nonsecure PL/SQL Code, changed database objects (including rootkits), altered data (including modifications of privilege and user tables), forensic traces from common security and hacker tools. The tool also employs penetration testing and brute force techniques to find known backdoors. It can scan from one to several hundred databases simultaneously. In addition to its security auditing features, Repscan provides a database browser that enables the user to view details about hundreds of databases anywhere on the network, and check their configurations. Repscan's discovery tools identify databases on the network down to individual tables containing sensitive information. A "one-click" feature reveals the patch levels of all scanned databases. Scan reports include expert recommendations and automatically-generated SQL fix scripts for many high-priority vulnerabilities, as well as out-of-the-box standard regulatory compliance reports (PCI, Installed Software, Forensic, *etc.*), plus custom compliance audit reporting. Repscan's command line interface also enables automation (through scheduling) and scripting of scans and tests. As of this writing, McAfee (which acquired Sentrigo in 2011) has not announced plans to end support for Repscan, although the company has only fully integrated Sentrigo's Hedgehog DBScanner into its product line as McAfee Vulnerability Manager for Databases) into its product line. Vulnerability Manager for Databases provides the same database discovery, vulnerability scanning, penetration testing, and reporting features found in Repscan, but unlike Repscan, Vulnerability Manager is intended for use by large enterprises, and is fully integrated with McAfee ePolicy Orchestrator (which is a prerequisite to run Vulnerability Manager). Also unlike Repscan, Vulnerability Manager for Databases enables automatic rules creation (through ePolicy Orchestrator) to generate protections against discovered database vulnerabilities, distribute centralized updates, and manage tests, including the addition of custom tests. Multiple user roles can be defined for Vulnerability Manager users, thereby maintaining appropriate separation of duties, and reports can be scheduled for distribution to selected users based on their assigned roles. Vulnerability Manager for Databases also archives its results to support monitoring of changes and trend analysis over time, thereby enabling continuous improvement and preventing regression. Vulnerability Manager can also be integrated with enterprise user authentication systems (including Active Directory).

McAfee Repscan and McAfee Vulnerability Manager for Databases

Type	Database Scanner
Target(s)	Oracle 9.1+, SQL Server 2005 SP1+, DB2 8.1+ (on Linux, UNIX, Windows), MySQL 4.0+
Format	Software
OS	Repscan: Windows XP
Hardware	Vulnerability Manager: Windows Server 2003 SP2+/2005 SP1+ running McAfee ePolicy Orchestrator 4.5; Console: Firefox 2.0+, IE 7.0+
License	Vulnerability Manager: 2GB+ RAM; 1GB free disk space
SCAP Validated	Commercial
Standards	
Supplier	
Information	*http://www.sentrigo.com/repscan* *http://www.mcafee.com/us/products/vulnerability-manager-databases.aspx*

NGSSecure NGS SQuirreL for DB2, SQL Server, Oracle, Informix, Sybase ASE

Abstract

NGS SQuirreL for DB2 tracks down weak access points in DB2 databases and their security infrastructures, and scans for security threats and potential vulnerabilities. It allows the user to assess levels of security risk and remediate identified problems *via* one-click fixes that generate lockdown scripts. The user can also generate custom remediations. The "check database" architecture enables the user to view and edit core checks, and to create custom checks, user references, and user reference types. NGS SQuirreL for DB2 performs full auditing with audit permissions on custom tables and views. The tool supports quick, normal, and full audits, with viewing of all checks supported for all three audit types. NGS SQuirreL for DB2 automatically updates itself with newly discovered vulnerability signatures. Reports can be generated in plaintext, XML, or static or dynamic HTML. NGS SQuirreL for Informix and SQuirreL for Sybase Adaptive Server Enterprise (ASE) provide comparable capabilities tailored for assessing security of IBM Informix and Sybase ASE databases. NGS SQuirreL for SQL Server provides the same viewing and editing features as SQuirreL for DB2. It enables the user to administer and manage logins, roles, databases, and extended stored procedures, and checks for backdoors, compromised servers, start-up and stored procedures, and weak passwords. As with SQuirreL for DB2, it supports one-click vulnerability fixes and automatic updating of vulnerability signatures, as well as flexible scanning through manual selection of groups of checks to be run (all checks are viewable). Reports can be generated in plaintext, RTF, XML, and static/dynamic HTML, or output to an external database. NGS SQuirreL for Oracle provides scanning, editing/viewing, vulnerability signature updating, one-click remediation, and reporting capabilities similar to those of the other SQuirreL editions plus password quality auditing (compatible with Cyber-Ark® Enterprise Password Vault), permission auditing (custom tables and views), vulnerability mitigation, user, profile, and role management, and system/object privilege management. It scans Oracle Transparent Network Substrate listeners for vulnerabilities, including denial of service and remote server compromises. It also provides built-in compliance auditing for PCI DSS, FISMA, SANS Top 20, and other regulations and benchmarks. The scanner can parse Oracle environment parameters and provide alerts on any incorrect configurations.

NGSSecure NGS SQuirreL for DB2, SQL Server, Oracle, Informix, Sybase ASE

Type	Database Scanner
Target(s)	DB2 7x-9x SQL Server 2000+ Oracle 7r3-11g Informix® Dynamic Server 9x-11x Sybase ASE versions through 15.5
Format	Software
OS	Windows
Hardware	
License	Commercial
SCAP Validated	
Standards	
Supplier	NGSSecure (UK)
Information	*http://www.ngssecure.com/ngssecure/services/information-security-software/ngs-squirrel-for-db2.aspx* *http://www.ngssecure.com/ngssecure/services/information-security-software/ngs-squirrel-for-sql-server.aspx* *http://www.ngssecure.com/ngssecure/services/information-security-software/ngs-squirrel-for-oracle.aspx* *http://www.ngssecure.com/ngssecure/services/information-security-software/ngs-squirrel-for-informix.aspx* *http://www.ngssecure.com/ngssecure/services/information-security-software/ngs-squirrel-for-sybase-ase.aspx*

Safety-Lab Shadow Database Scanner

Abstract

Safety Lab Shadow Database Scanner performs vulnerability audits of SQL databases. After completing a database management system scan, Shadow Database Scanner analyzes the data it has collected, locates vulnerabilities and possible errors in server configuration options, and suggests possible ways of correcting those errors. Shadow Database Scanner can also detect faults with MiniSQL, and can track more than 300 audits per target. The tool's ActiveX-based architecture enables developers familiar with VC++, C++ Builder or Delphi to expand the capabilities of the Scanner, or to integrate Shadow Database Scanner into other products that provide ActiveX support. The Shadow Database Scanner API enables the user to fully control the scanner, or to change its properties and functions, while the BaseSDK [software developers kit] wizard guides the user through the process of new audit creation, allowing him/her to add more than 95% of all possible new audit types. The scanner's Rules and Settings Editor can limit scans to specific ports and services. The tool can be tuned by the administrator to set scanning depth and other options that will optimize scanning speed without affecting scan quality. Detailed scan session logs (reports) can be saved in HTML, XML, PDF, RTF, and CHM formats.

Safety-Lab Shadow Database Scanner

Type	Database Scanner
Target(s)	SQL Server, Oracle, DB2, MiniSQL, MySQL, Sybase, SAP DB, Lotus® Domino
Format	Software
OS	Windows 95/98/Me/NT/2000/XP/2003/Vista/7
Hardware	
License	Commercial
SCAP Validated	
Standards	
Supplier	Safety-Lab (Russia)
Information	*http://www.safety-lab.com/en/products/6.htm*

WEB APPLICATION SCANNERS

Acunetix® Web Vulnerability Scanner

Abstract

Acunetix Web Vulnerability Scanner crawls Web sites, including Sites hosting Flash content, analyzes Web applications and SOAP-based Web services and finds SQL injection, Cross site scripting, and other vulnerabilities. Acunetix Web Vulnerability Scanner includes an automatic JavaScript analyzer that enables security analysis of AJAX and Web 2.0 applications, as well as Acunetix's AcuSensor Technology that can pinpoint the following vulnerabilities among others: version check; Web server configuration checks; parameter manipulations, multirequest parameter manipulations, file checks, unrestricted file upload checks, directory checks, text searches, weak HTTP passwords, hacks from the Google Hacking Database, port scanner and network alerts, other Web vulnerability checks, and other application vulnerability tests. Acunetix Web Vulnerability Scanner is able to automatically fill in Web forms and authenticate against Web logins, enabling it to scan password-protected areas. Additional manual vulnerability tests are supported by the Web Vulnerability Scanner's built-in penetration testing tools, *e.g.,* Buffer overflows, Sub-domain scanning. The penetration test tool suite includes (1) HTTP Editor for constructing HTTP/HTTPS requests and analyzing the Web server's response; HTTP Sniffer for intercepting, logging, and modifying HTTP/HTTPS traffic and revealing data sent by a Web application; HTTP fuzzer, for sophisticated fuzz testing of Web applications input validation and handling of unexpected and invalid random data, W(virtual) Script scripting tool for scripting custom Web attacks; Blind SQL Injector for automated database data extraction. Acunetix Web Vulnerability Scanner includes a reporting module that can generate compliance reports for PCI DSS and other regulations/standards. The scanner is offered in Small Business, Enterprise, and Consultant editions.

Acunetix Web Vulnerability Scanner

Type	Web Application Scanner (with manual pen testing)
Target(s)	
Format	Software
OS	Windows XP, Vista, 2000, 2003 Server, 2008 Server, 7 running IE 6+
Hardware	1GB RAM, 250MB disk
License	Commercial
SCAP Validated	
Standards	
Supplier	Acunetix Ltd. (Cyprus)
Information	*http://www.acunetix.com/vulnerability-scanner/*

Casaba Watcher 1.5.1

Abstract

To avoid manual inspection of a Web application for many security issues (*e.g.,* cookie settings, SSL configuration, information leaks, *etc.*), Watcher automates security analysis and provides hot-spot detection to help pen-testers focus in on the weaknesses that can lead to major exploits. Watcher is implemented as an add-on to the Fiddler Web Debugging Proxy, which provides a proxy framework for HTTP debugging. Because it is a passive scanner, Watcher can be used safely in Cloud environments as its testing is unlikely to damage the shared infrastructure (although this is not 100% guaranteed). Watcher is not a pen testing tool; it does not attack Web applications with loads of intrusive requests, or modify inputs to the application. Unlike many Web crawlers and Web application scanners, Watcher generates no dangerous traffic. It analyzes normal user interaction and makes educated reports on the security of the application based on those observations. Watcher is intended for use by development/test staff that are already capable of using Fiddler.

Casaba Watcher 1.5.1

Type	Web Application Scanner
Target(s)	IIS
Format	Software
OS	Windows XP, Vista, 7, running Fiddler *(http://www.fiddler2.com/fiddler2/)*
Hardware	
License	Freeware
SCAP Validated	
Standards	
Supplier	Casaba Security, LLC
Information	*http://www.casaba.com/products/watcher/* *http://Websecuritytool.codeplex.com/*

Cenzic® Hailstorm® Enterprise Application Risk Controller

Abstract

Cenzic Hailstorm Enterprise Application Risk Controller (ARC) can run Web application vulnerability scans against multiple Web servers using pre-defined and user-customized scanning templates. Hailstorm Enterprise ARC can be configured to crawl and scan each Web server application automatically or as guided by the user; manual crawling may be the only way certain types of Web applications, such as AJAX applications, can be crawled and "learned" by the tool. Using Cenzic's Stateful Assessment technology and SmartAttacks database of 111 categories of Web attacks (with all signatures viewable and written in JavaScript), which is updated weekly, unlike vulnerability (*vs.* attack) signature-based scanners, Cenzic Hailstorm emulates a hacker, automating penetration testing by embedding a Mozilla browser directly into the scanner. This approach enables Hailstorm to test for vulnerabilities that other automated scanners cannot detect, such as Privilege Escalation and Session Hijacking, and to test for unlimited number of zero-day variants of known vulnerabilities. In addition, Hailstorm performs tests for OWASP Top 10 and SANS Top 20 vulnerabilities, and tests for compliance with regulations such as PCI DSS and others. Hailstorm also calculates arbitrary Hailstorm Application Risk Metric (HARM) Scores (quantitative risk scores) from scan results, and assigns a score to each vulnerability found; numerical HARM scores have the potential to provide more granular indications than quantitative text-based risk scores (*e.g.,* "high", "medium", "low") about which vulnerabilities need to be remediated first. The Hailstorm Enterprise ARC dashboard displays the applications tested, trends in vulnerabilities, applications most at risk, and remediation trends across the enterprise. The product is designed to be used in "continuous assessment" mode, constantly scanning applications and tracking changes in the overall risk exposure from each. This Web application vulnerability-management approach is useful in environments in which the application as tested last month has changed due to upgrades, patches, and other fixes.

Hailstorm Enterprise Application Risk Controller

Type	Web Application Scanner
Target(s)	IIS
Format	Software
OS	Windows 7 Pro, XP Professional SP3, Server 2008/2008 R2, Server 2003; *running .NET* Framework 3.5 SP1 and IIS 5.0+ with IIS lockdown tool 2.1
Hardware	Multi-core (2+) 400MHz+ Intel or Advanced Micro Devices (AMD) CPU, 4GB RAM; 50GB disk
License	Commercial
SCAP Validated	
Standards	CWE
Supplier	Cenzic
Information	*http://www.cenzic.com/products/cenzic-hailstormEntARC/*

Cenzic Hailstorm Professional

Abstract

Cenzic Hailstorm Professional is a single-platform scanner that shares many of the features of Hailstorm Enterprise ARC, but is limited to scanning the Web server and applications on the platform on which the tool is hosted. It can be configured to crawl and scan a Web client (browser) application automatically or as guided by the user. Using Cenzic's Stateful Assessment technology and SmartAttacks database of 111 categories of Web attacks, which is updated weekly, unlike signature-based scanners, Cenzic Hailstorm emulates a hacker, automating penetration testing by embedding a Mozilla browser directly into the scanner. This approach enables Hailstorm to test for vulnerabilities such as Privilege Escalation and Session Hijacking, and to test for unlimited number of zero-day variants of known vulnerabilities. In addition, Hailstorm performs tests for OWASP Top 10 and SANS Top 20 vulnerabilities, and tests for compliance with regulations such as PCI DSS and others. As with Hailstorm Enterprise ARC, Hailstorm Professional calculates arbitrary HARM Scores from scan results, and assigns a HARM Score to each vulnerability found.

Cenzic Hailstorm Professional

Type	Web Application Scanner
Target(s)	Microsoft IIS
Format	Software
OS	Windows 7 Pro/XP Pro SP3
Hardware	Multi-core (2+) 400MHz+ Intel or AMD CPU, 3GB RAM, 20GB disk
License	Commercial
SCAP Validated	
Standards	CWE
Supplier	Cenzic
Information	*http://www.cenzic.com/products/cenzic-hailstormPro/*

eEye Retina Web

Abstract

eEye Retina Web security scanner scans large, complex Web sites, Web applications, and Web services Simple Object Access Protocol [SOAP]/Web Services Definition Language [WSDL] identification and parsing to discover and identify Web application vulnerabilities, privacy and data security policy violations, and site exposure risks. The scanner ranks threat priority, and graphical HTML-format reports (XML and database formats optional) that indicate site security posture by vulnerabilities and threat level, with remediation time and cost estimates; reports can also segregate findings by server, responsible developer, database, *etc.* In addition to reporting vulnerabilities, data in Retina Web Security Scanner reports include interactive site maps that clarify the Web site architecture *e.g.,* from where is the site receiving data, to where is it sending data, what specific URLs/links are vulnerable, *etc.*

eEye Retina

Type	Web Application ScannerWeb Application Scanner
Target(s)	Web sites, applications, services (SOAP/WSDL only)
Format	Software
OS	Windows 2000 Pro/Server, XP, Server 2003, Vista (all 32-bit); must *run .NET* Framework 2.0/3.0, IE 6.0+
Hardware	1.4GHz Pentium IV or compatible, 1GB RAM (command line mode)/2GB RAM (graphical user interface mode); 500MB+ free disk space; 1024x768+ res. monitor; Internet access
License	Commercial
SCAP Validated	
Standards	
Supplier	eEye Digital Security®
Information	*http://www.eeye.com/Products/Retina/Web-Security-Scanner.aspx*

Grabber

Abstract

Grabber is a Web application scanner. It detects some kinds of vulnerabilities in Web sites. The software is designed to scan small Web sites such as personals, forums, *etc.* It is not designed to be used on a large Web application as it would take too long to run and would flood the target's network. Because it's a small tool, the set of vulnerabilities Grabber searches for is limited to XSS, SQL injection (including blind SQL injection), file inclusions, backup file presence, AJAX parameters retrieval, server-side JavaScript name/parameter retrieval. The tool also performs hybrid analysis/white box (source code) and black box testing for PHP applications, uses a JavaScript source code analyzer (JavaScript *lint*) to evaluate the quality and correctness of the JavaScript, and generates files [*session_id, time(t)*] for *next stats* analysis. Reports are output in XML format.

Grabber

Type	Web Application Scanner
Target(s)	
Format	Software
OS	Executable: any Windows platform that supports Python (with BeautifulSoup and PyXML); Source code: presumably will run on any platform that supports Python
Hardware	
License	Open source
SCAP Validated	
Standards	
Supplier	Romain Gaucher
Information	*http://rgaucher.info/beta/grabber/*

Hacktics® Seeker®

Abstract

Hacktics Seeker uses Behavioral Runtime Intelligent Testing Engine (BRITE) technology to perform searches for application vulnerabilities. BRITE enables Seeker to learn the application's behavior from the inside, and to identify problematic code. After identifying vulnerabilities, Seeker automatically generates and executes exploits against those vulnerabilities to verify that they do, in fact, exist and are not false positives; the results of this exploit-based analysis is captured in a video that the auditor can view. In addition to standard vulnerabilities, Seeker identifies complex logical vulnerabilities such as parameter tampering, unauthorized access, and flow bypass, as well as data transfer vulnerabilities, such as lack of encryption or storage of sensitive data. Seeker can detect vulnerabilities that involve two or more steps across separate URLs, and provides coverage of the OWASP Top 10 vulnerabilities. Other analysis features include: (1) analysis of code execution, memory behavior, and data flow; (2) Smart Attack Tree algorithm that tests only relevant code; (3) correlation between multiple application tiers and asynchronous components, enabling identification of byzantine (complex) vulnerabilities that are distributed across multiple code segments. Seeker has an intuitive user interface and is designed to be fully automated and usable by novices, and does not require expert technical or security knowledge.

Hacktics Seeker

Type	Web Application Scanner
Target(s)	
Format	Software
OS	
Hardware	
License	Commercial
SCAP Validated	
Standards	
Supplier	Hacktics (Israel)
Information	*http://www.hacktics.com*

HP WebInspect®

Abstract

HP WebInspect performs Web application and Web service security testing and assessment of complex Web applications using platform-independent dynamic security analysis of running applications. HP WebInspect identifies security vulnerabilities using assessment technologies, such as simultaneous crawl and audit and concurrent application scanning. WebInspect also provides automated penetration tests (*e.g.,* SQL injection and XSS). WebInspect uses multiple analysis methods and intelligent security testing engines to confirm exploitable security vulnerabilities. HP WebInspect statically analyzes client-side scripting code (JavaScript, Flash, Silverlight, *etc.*) to understand the attack surface and functions of the Web application and the vulnerabilities introduced by interactive Web application functionality. WebInspect's findings can be cooperatively analyzed with those of HP Fortify's static analysis of the source code of the Web application. WebInspect can also be integrated with HP Assessment Management Platform 8.00/8.10/9.00, HP Quality Center 9.2/10.0, HP Application Lifecycle Management 11.0, or IBM/Rational ClearQuest® v7.1.

HP WebInspect

Type	Web Application Scanner (with automated pen testing)
Target(s)	
Format	Software
OS	Windows 7/Server 2008 R2 (32-/64-bit) (Recommended), XP Professional SP3/ Server 2003 SP2 (32-bit), Vista SP2 (32-/64-bit), all running SQL Server Express Edition 2005 SP3/2008 SP2/2008 R2; SQL Server 2008 R2/2008 SP2/2005 SP4, .NET Framework 3.5 SP1, and IE 7.0 (8.0 recommended; Firefox supported for proxy setting only)
Hardware	1.5GHz single-core (2.5GHz+ dual-core recommended), 2GB RAM (4GB recommended), 10GB disk (100+GB recommended), 1024x768 res. monitor (1280x1024 recommended); Internet connection (for updates)
License	Commercial
SCAP Validated	
Standards	
Supplier	HP/Fortify®
Information	*https://www.fortify.com/products/web_inspect.html*

IBM/Rational® AppScan® Standard, Enterprise, and Express Editions

Abstract

IBM/Rational AppScan Standard Edition automates vulnerability testing *via* dynamic Web application analysis and static JavaScript analysis. The tool enables vulnerability testing of Web applications, Web Services, and Web 2.0 and rich Internet applications (JavaScript, AJAX, Adobe Flash®). The built-in JavaScript Security Analyzer performs static (white box) analysis to detect client-side security issues, such as Document Object Model (DOM)-based XSS and code injection. AppScan also scans Web sites for embedded malware and links to malicious or undesirable sites. Its functionality can be customized and extended *via* the AppScan eXtension Framework. The reporting capability includes regulatory compliance reporting templates with 40 out-of-the box compliance reports including PCI DSS, Payment Applications Data Security, ISO 27001/27002, and Basel II. Express Edition provides the same capabilities as Standard edition, but is intended to be installed on a single desktop, for scanning by small businesses and individual users. Standard and Express Editions allow only one-target-at-a-time scanning, while Enterprise Edition allows for simultaneous scanning of multiple targets. However, Enterprise Edition does not support static analysis of Java Script. AppScan Reporting Console can be purchased for aggregating, correlating, and reporting scan results collected by multiple instances of AppScan Standard or Express Edition (Reporting Console comes standard with Enterprise Edition). AppScan can be integrated with IBM/Rational ClearQuest 7.0/7.1.1 or HP Quality Center 9.2/10 for defect tracking. Rational AppScan is also available in Source, Build, and Tester Editions for use by developers and testers during the application development life cycle (pre-production). Source edition supports static source code analysis; Build and Tester editions integrate Web application security testing into the build management and quality assurance workflows, respectively.

IBM/Rational AppScan Standard, Enterprise, and Express Editions

Type	Web Application Scanner
Target(s)	
Format	Software
OS	Windows XP Professional SP2/SP3, 2003 Standard/Enterprise SP1/SP2, Vista Business/Ultimate/Enterprise SP1/SP2, Server 2008 Standard/Enterprise SP1/SP2, 2008 R2 Standard/Enterprise, 7 Professional/Enterprise/Ultimate (all must run in 32-bit mode), running IE 6+, .NET Framework 2.0+ (3.0 required for some options).
Hardware	2.4Ghz Pentium IV, 2GB RAM, 30GB disk, 100baseT NIC with TCP/IP configured
License	Commercial
SCAP Validated	
Standards	CVE, CWE
Supplier	IBM
Information	*http://www-01.ibm.com/software/awdtools/appscan/*

Mavutina Netsparker®

Abstract

Mavutina Netsparker is a Web application security scanner that integrates detection, exploitation, and confirmation logic in a single integrated engine that can find, verify, and report security issues such as SQL injection and cross-site scripting (XSS) in Web applications on any platform, implemented by any technology. Netsparker uses a combination of detection and exploitation techniques to increase the accuracy of its findings. Instead of only reporting detected security issues, the tool shows what an attacker might accomplish by exploiting those issues. Netsparker can crawl and comprehend Web sites that use a variety of AJAX frameworks, frameworks such as JQuery, and custom code. It uses JavaScripts to simulate attacker actions, and provides a command line interface for the user to automate scans and integrate Netsparker into larger vulnerability scanning, reporting, or development systems. When Netsparker identifies a vulnerability, it automatically extracts the version information of the vulnerable target application, executes an exploit to target the vulnerability, and observes the execution of the exploit script to confirm that result, thus confirming that the detected vulnerability is not a false-positive. Netsparker can also carry out post-SQL injection exploit analyses (the tool is being expanded to provide additional post-exploit analyses). Netsparker logs all of its tests and findings, and generates reports in multiple formats, including XML, Word/RTF, and PDF. The tool can be purchased under multiple licenses designed for different enterprise sizes. Mavutina also offers an open source Netsparker Community Edition that gets updated less frequently than the commercial edition, and lacks many capabilities and security checks, but which entitles the user to updates and support *via* the Community Edition Forum.

Mavutina Netsparker

Type	Web Application Scanner (with automated pen testing)
Target(s)	
Format	Software
OS	Windows XP, 7, Vista, 2003/2008
Hardware	
License	Commercial (one Open Source version)
SCAP Validated	
Standards	
Supplier	Mavuntina Security (UK)
Information	*http://www.mavitunasecurity.com/netsparker/*

MAYFLOWER Chorizo! Intranet Edition

Abstract

MAYFLOWER Chorizo! Intranet Edition can be used to scan an unlimited number of internal and Internet-facing Web applications. The appliance records all requests made to the server-side application and scans for security issues such as XSS, cross site request forgery (CSRF), code inclusion, remote code execution, PHP vulnerabilities, session injection, *etc.* The tool generates detailed reports with explanations of problems found, and advice—including code examples—on how to remediate those problems. MAYFLOWER also offers Chorizo! Free (one host IP address) and Standard (five IP addresses) versions to their Web hosting customers as a combination SaaS and client-side browser plug-in.

MAYFLOWER Chorizo! Intranet Edition

Type	Web Application Scanner
Target(s)	
Format	Appliance
OS	Included
Hardware	Included
License	Commercial (reduced-capability freeware available)
SCAP Validated	
Standards	
Supplier	MAYFLOWER GmbH (Germany)
Information	*https://chorizo-scanner.com/*

MileSCAN ParosPro Desktop Edition 1.9.12

Abstract

MileSCAN ParosPro Desktop Edition features a built-in man-in-the-middle proxy that captures all traffic between a client and a server. Information such as request and response headers, parameters, HTML form data, *etc.*, is extracted from each captured request. The interceptor traps all HTTP/HTTPS messages passing through the proxy, so the user can modify the GET or POST data in HTTP messages on-the-fly for manual testing in which the parameters are controlled directly for more effective tests. The tool's vulnerability scanner simulates hacker attacks and identifies security risks on the target Web site. The scanner can be fine-tuned to avoid false positives when scanning for common Web attacks and security flaws from the OWASP Top 10, including SQL injection, XSS, and content management system (CMS) fingerprinting. The tool also includes a network spider that crawls a specified URL to collect information about the site hierarchy, and to analyze each page crawled to discover all links within that page. The network spider crawls the Web site iteratively, level by level, until its maximum link limit is reached. The spider's JavaScript Engine enables the spider to crawl links triggered by JavaScript. The spider reports the list of links and site hierarchy it has collected, enabling further manual inspection; manual inspection is assisted by HTML encoding and conversion tools that include URL encoding/decoding, Base64 encoding/decoding, and Secure Hash Algorithm (SHA) 1/Message Digest (MD) 5 hash calculation. Reports generated by ParosPro Desktop Edition (in PDF format) include detailed information about the tool's risk findings, including risk level and location in the Web site hierarchy. The reports also suggest solutions and references to information that will enable the user to figure out the root causes and fixes for all detected security problems. The tool also includes an Update Manager that automatically checks for new ParosPro plug-ins for new vulnerabilities. MileSCAN offers the proxy portion of ParosPro Desktop Edition (ParosProxy) as freeware; ParosProxy supports only a small subset of the capabilities provided in ParosProxy Desktop Edition.

MileSCAN ParosPro Desktop Edition 1.9.12

Type	Web Application Scanner (with limited automated pen testing)
Target(s)	Web server applications
Format	Software
OS	Windows XP (32-bit), Vista, or 2000/SP2+
Hardware	Intel Pentium III+ CPU, 1GB RAM (2GB+ recommended), 100MB+ disk
License	Commercial (reduced-capability freeware available)
SCAP Validated	
Standards	
Supplier	MileSCAN Technologies Ltd. (Hong Kong)
Information	*http://www.milescan.com/hk/index.php?option=com_content&view=article&id=98&Itemid=103*

MileSCAN ParosPro Server Edition 1.5.0

Abstract

MileSCAN ParosPro Server Edition (formerly Web Security Auditor) provides a multi-user Web security auditing platform that enables the user to schedule periodic automated scans, and can be configured to send email notifications to administrators/users, enabling them to monitor the scan progress offline. Audit logs are captured that enable administrators to record the usage of the scanning server and track any scan configuration changes. The tool's network spider crawls a specified URL to collect information about the site hierarchy, with the contents of each crawled page analyzed to discover its links to other pages; the tool will continue crawling the site's Web page hierarchy until its page crawl limit is reached. The network spider can be tuned manually according to the scan scope and available bandwidth of the network. If the Web site requires user authentication, the user can input authentication credentials in the scan setting for the spider to use. A JavaScript Engine can be enabled in network spider to also crawl links triggered by JavaScript. The tool reports the list of links and site hierarchy to support manual inspection. The tool's vulnerability scanner is powered by plug-ins that target common Web vulnerabilities, including SQL injection and XSS, and vulnerabilities in popular content management systems. The scanner also performs server fingerprinting and information gathering, and simulates hacker attacks against Web sites. After vulnerability scanning, all alerts and vulnerabilities are included in a scan report (in HTML or PDF format), along with a detailed description of each vulnerability and the list of links to Web pages that are vulnerable. The report also identifies solutions and references information on how to fix each vulnerability. The Scan Scheduler enables the user to configure scans at pre-defined dates and times, while the built-in dashboard provides a quick overview of the scan in progress along with alerts for issues detected during scanning. Email notifications can be configured to alert authorized users when a scan has finished; these notifications include finding summaries on scan results.

MileSCAN ParosPro Server Edition 1.5.0

Type	Web Application Scanner (with limited automated pen testing)
Target(s)	Web server applications
Format	Software
OS	Windows XP/Vista/Server 2003 (32-bit)
Hardware	Pentium IV+ CPU, 2GB RAM (3GB+ recommended), 2GB disk
License	Commercial
SCAP Validated	
Standards	
Supplier	MileSCAN Technologies Ltd. (Hong Kong)
Information	*http://www.milescan.com/hk/index.php?option=com_content&view=article&id=99&Itemid=180*

nCircle WebApp360

Abstract

nCircle WebApp360 provides an agentless Web application security testing system that is designed for use in production (rather than development) environments. It provides continuous, real time assessment of vulnerabilities and risks in Web applications and underlying infrastructure of Web servers, operating systems, and adjacent applications. Some of the vulnerabilities checked for by WebApp360 include (but are not limited to) basic authentication, persistent cookies, XSS vulnerabilities (including basic, persistent, numeric, quoteless, and close TextArea XSS), invalid input, plaintext password, basic SQL injection, URL insertion, password field AutoComplete, HTML tag insertion, persistent input validation, and CSRF. WebApp360 ranks and prioritizes its findings using nCircle's unified risk metric and CVSS version 2. Granular role-based access controls enable WebApp360 to reuse existing roles defined for IP360 (in environments that use both nCircle scanners), as well as creation of new roles specific to management of Web properties. The tool's support for HTTP virtual hosts enables assessment of multiple Web sites hosted on a single server. nCircle can be purchased stand-alone or as part of nCircle's Suite360 risk and compliance assessment and management toolset.

nCircle IP360

Type	Web Application Scanner
Target(s)	
Format	Appliance
OS	
Hardware	
License	Commercial
SCAP Validated	
Standards	
Supplier	nCircle Network Security, Inc.
Information	*http://www.ncircle.com/index.php?s=products_webapp360*

NGSSecure Domino Scan II

Abstract

NGSSecure Domino Scan II is a vulnerability scanner for Lotus Domino Web servers. Domino Scan II can perform scans with and without credentials. Domino Scan II interrogates every view, form, and agent within a database, even if access control list-based protection has been invoked. It then performs a range of tests on each document, auditing over 100 sensitive and default databases, and subjecting all documents to a set of vulnerability assessment checks. By using its intelligent spidering technology, Domino Scan II performs deep-level database enumeration, script, and link scanning, and discovers vulnerabilities on servers that may otherwise have remained hidden to conventional vulnerability scanning software. Domino Scan II attempts to gain access to sensitive/default databases, and performs directory traversals and database browsing to discover vulnerabilities to those types of attacks. It also evaluates database design, checking every document for write/edit access, attempting forced searches and ReadEntries/ReadViewEntries access. Domino Scan II can generate reports in plaintext, RTF, HTML, XML, and external database formats.

NGSSecure Domino Scan II

Type	Web Application Scanner
Target(s)	Domino versions R6 to R8 inclusive
Format	Software
OS	Windows
Hardware	
License	Commercial
SCAP Validated	
Standards	
Supplier	NGSSecure (UK)
Information	*http://www.ngssecure.com/ngssecure/services/information-security-software/ngs-domino-scan-II.aspx*

NGSSecure OraScan

Abstract

NGSSecure's OraScan performs security vulnerability audits of Oracle Web applications hosted on Oracle's and other vendors' Web servers. OraScan can detect SQL injection, XSS, poor Web server configurations, and other vulnerabilities, and can audit the configuration of Internet Application Server (IAS) Web servers, ensuring that the Web application portion of the database application architecture is free of security weaknesses. Web server auditing is fully automated, and includes checks on Procedural Language/SQL (PL/SQL), Java Server Pages (JSP), SQL JSP, and XSQL (combination of XML and SQL). The tool uses spidering for vulnerability discovery, deriving the structure of the Oracle Web application and testing each functional component, as well as all site links and referenced scripts. OraScan can generate reports in plaintext, RTF, HTML, XML, and external database formats.

NGSSecure OraScan

Type	Web Application Scanner
Target(s)	Oracle Web applications
Format	Software
OS	Windows
Hardware	
License	Commercial
SCAP Validated	
Standards	
Supplier	NGSSecure (UK)
Information	*http://www.ngssecure.com/ngssecure/services/information-security-software/ngs-orascan.aspx*

Nikto2 2.1.4

Abstract

Nikto2 is an open source Web server application scanner that tests for more than 6,400 potentially dangerous files/programs and CGI scripts, default files, and programs, outdated versions of more than 1,000 servers, version-specific problems of more than 270 servers, server and software misconfigurations, as well as script injection, HTML injection, XSS, file upload, remote file retrieval, remote shell, SQL injection, authentication bypass, remote source inclusion, denial of service, and reverse tuning vulnerabilities. While most checks are for known security issues, Nikto2 does perform some "information only" checks for non-security issues that it would be of benefit to remediate. Nikto2 will also check and report on unknown issues it finds in the target's log files. The tool does not check for command injection vulnerabilities. Nikto is not designed to be stealthy, but rather to test a Web server in the shortest time possible; its activities will show up in system log files. However, as it is built on LibWhisker2, Nikto2 does support LibWhisker's anti-IDS methods; these enable Nikto2 to be configured to elude IDS detection. Nikto2 generates a list of unique file extensions from its test database at runtime and tests each of those extensions against the target. For every file type, the tool then determines the most efficient method for finding errors (*e.g.,* standard Request for Comments response, content/string match, or MD4 hash). Nikto2 attempts to identify installed Web servers and software. Nikto2 supports SSL, proxies, host authentication, attack encoding, output to Metasploit, and other security features. Scan items and plug-ins are automatically updated frequently, and can also be updated on demand *via* the tool's command line. Reports from Nikto2 scans can be output in multiple formats, including HTML and XML; output can also be sent to Metasploit. Nikto2 should operate on any platform with a Perl environment; the table below lists those platforms on which it has been validated. Note that some Nikto2 POSIX features (*e.g.,* interactive commands) may not work when the tool is run on Windows.

Nikto2 2.1.4

Type	Web Application Scanner
Target(s)	HTTP/HTTPS-based Web server applications
Format	Software
OS	Windows (running ActiveState or Strawberry Perl); Mac OS X; Linux (Red Hat, Debian, Knoppix); Solaris. All with LibWhisker installed.
Hardware	
License	Open source
SCAP Validated	
Standards	
Supplier	CIRT.net (Chris Sullo and David Lodge)
Information	*http://www.cirt.net/nikto2/*

NOSEC JSky 3.5.1

Abstract

NOSEC JSky is a Web vulnerability scanner and Web application vulnerability assessment tool. It can scan for SQL injection, XSS, non-secure indexing, local path disclosure, server misconfigurations, and other vulnerabilities to Web application threats. The scanner's Web spider can perform multi-threaded crawls of hundreds of thousands of Web pages, and can extract additional links from JavaScript and Flash. Rather than using pattern-matching and a dictionary of vulnerability signatures to detect vulnerabilities, JSky uses the Pangolin SQL injection tester, which enables detection of advanced SQL injections. JSky's modular design enables it to be extended with new modules, and its XML-based vulnerability file and integrated execution parser enables new vulnerability exploits to be added to the scans by editing the XML file, without the need for software coding. The XML file and parser are used by the JSky artificial intelligence hacking engine to automate pen testing of Web sites, effectively simulating what a human hacker would see and do in a real-world attack. JSky is designed for penetration testers and by Web administrators with very little testing expertise. NOSEC also offers an SaaS version called iiScan.

NOSEC JSky 3.5.1

Type	Web Application Scanner (with limited pen testing)
Target(s)	Web applications with backend SQL databases, including Oracle, SQL Server, MySQL, Informix, DB2, Access, SQLite®, Sybase, PostgreSQL
Format	Software
OS	Windows 2000/XP/2003/Vista/7
Hardware	1.5GHz+ Intel CPU, 1GB RAM, 2GB disk
License	Commercial
SCAP Validated	
Standards	
Supplier	NOSEC (Hong Kong)
Information	*http://www.nosec-inc.com/en/products/jsky*

N-Stalker Web Application Security Scanner 2009

Abstract

N-Stalker Web Application Security Scanner 2009 uses a Web attack signature database of 39,000 signatures to drive its component-oriented Web application security assessment of off-the-shelf Web applications, but is also able to crawl and evaluate custom-developed Web Applications without reference to out-of-box signatures. The signature database includes common Web application vulnerabilities (*e.g.,* OWASP Top 10, CWE Top 25) plus a wide range of other security issues. The tool can scan both the Web server infrastructure and application layers. N-Stalker Web Application Security Scanner allows for assessment of Web applications at different times in the application life cycle, including the development phase, the deployment phase, and the production and maintenance phase. N-Stalker Security Scanner allows the user to create custom assessment policies and requirements, including control of information exposure, development flaws, infrastructure issues, and security vulnerabilities that can be explored by external agents. N-Stalker Security Scanner comprises three distinct components: (1) Web crawling engine: instead of relying on "AJAX patterns" and DOM reconstruction, the tool includes a full JavaScript engine that allows for native script execution, DOM integration, and scanning AJAX-based Web applications with no prior knowledge of their location; (2) Web attack engine: this is the tool's scan engine that looks for Web application problems such as general parameter tampering, forceful browsing, and information exposure, as well as the common vulnerabilities captured by the Security Scanner database of 39,000 Web attack signatures; (3) User interface: used to control scan settings and to access a set of tools that augment and complement the capabilities of the scanner, including a Web proxy, Web server discovery, password brute force tool, HTTP load tester, and Google Hacking Database tool (a real-time Google-like search engine used to inspect the Web site directory tree). N-Stalker also offers Web Application Security Scanner 2009 Free Edition for individual/home business use.

N-Stalker Web Application Security Scanner

Type	Web Application Scanner
Target(s)	
Format	Software
OS	Windows 2000+
Hardware	1GB RAM, 500MB disk
License	Commercial (Freeware version also offered)
SCAP Validated	
Standards	CWE
Supplier	N-Stalker
Information	*http://nstalker.com/products*

NT OBJECTives NTOSpider

Abstract

NT OBJECTives' NTOSpider scans and analyzes large, complex Web sites and applications to identify application vulnerabilities and site exposure risk. The tool ranks each threat according to mitigation priority, and presents its findings in a graphical HTML report that also indicates site security posture according to vulnerabilities detected and threat exposure determined. Specific vulnerabilities detected by NTOSpider include SQL injection (including blind SQL injection), XSS (reflected, persistent, and DOM), parameter analysis, OS commanding, HTTP response splitting, CSRF, remote file includes, file uploads, session strength, forced browsing, directory browsing/traversal, basic Flash/Java analysis, and malicious script and malicious frame analyses. The tool's built-in Data Sleuth intelligence engine analyzes the content, structure, and nature of each vulnerability. Data Sleuth can analyze files/resources, source code and scripts, comments, and directory contents. In addition to assessing application vulnerabilities, NTOSpider analyzes the Web site structure, content, and configuration to identify inherent exposures to future or emerging threats. This exposure is communicated in the form of a security posture rating, which is included in the tool's report, along with a qualitative analysis of findings, and complete catalog of all site resources and their attributes (*e.g.,* forms, cookies, scripts, SQL strings and ODBC connectors, authentication, applets/objects, hidden fields, *etc.*).

NT OBJECTives NTOSpider

Type	Web Application Scanner
Target(s)	
Format	Software
OS	
Hardware	
License	Commercial
SCAP Validated	
Standards	OVAL, CWE
Supplier	NT OBJECTives, Inc.
Information	*http://www.ntobjectives.com/ntospider*

PortSwigger Burp Suite Professional Edition Burp Scanner Component

Abstract

The Burp Scanner within PortSwigger's Burp Suite Professional Edition Web security toolset is a vulnerability scanner for Web applications. It is designed to integrate closely with existing techniques and methodologies for manual and automated testing of Web applications. Burp Scanner provides fine-grained control over which items get scanned, and provides immediate feedback and results for each scanned item. Burp Scanner can perform: (1) passive scanning of all requests and responses made through PortSwigger's Burp Proxy, to identify flaws such as information disclosure, insecure use of SSL, and cross-domain exposure, finding bugs without sending additional requests to the application; (2) active scanning of all in-scope requests passing through Burp Proxy, using the tester's browser to walk Burp Scanner through the parts of the application's functionality to be actively scanned. Burp Scanner will then send numerous additional requests to the target application, to identify vulnerabilities such as SQL injection, cross-site scripting, and file path traversal; (3) user-directed active or passive scanning of specific user-selected requests within any of the Burp Suite tools, useful for manually testing individual parts of an application's functionality that require human intelligence to perform effectively, to augment Burp Scanner's automatically testing for a wide range of vulnerabilities. Burp Scanner does not rely on a database of checks. Rather, it was designed to reproduce the actions of skilled, methodical human testers.

PortSwigger Burp Suite Professional Edition Burp Scanner Component

Type	Web Application Scanner (with limited pen testing)
Target(s)	
Format	Software
OS	Windows, Linux, Mac OS X; Java Virtual Machine (JVM/JRE)
Hardware	
License	Commercial
SCAP Validated	
Standards	
Supplier	PortSwigger Ltd. (UK)
Information	*http://portswigger.net/burp/scanner.html*

Subgraph Vega

Abstract

Subgraph Vega is an open source, multi-platform Web application vulnerability scanner written in Java. Vega will allow users to run a series of security checks against Web applications to identify possible vulnerabilities. Vega includes both automated scanning and interactive modes, the latter for focused penetration testing. The automated scanner features include application crawling, platform and application fingerprinting, identification of injection points and vulnerabilities, parameter fuzzing, alerting of discovered vulnerabilities, and response (remediation) process modules. The penetration testing features are supported by an interactive proxy that enables interception and editing of requests, setting of breakpoints, SSL man-in-the-middle attacks, encoding/decoding, and script processing. Vega is designed to support user or community-created custom functionality implemented in JavaScript. Vega includes a built-in JavaScript interpreter and well documented API to support the development of such customizations. As of 27 April 2011 Vega was completing its final testing and was scheduled for public release on 1 May 2011.

Subgraph Vega

Type	Web Application Scanner (with manual pen testing)
Target(s)	
Format	Software
OS	
Hardware	
License	Open source
SCAP Validated	
Standards	
Supplier	Subgraph (Canada)
Information	*http://subgraph.com/product.html*

Syhunt Sandcat and Sandcat Pro

Abstract

Syhunt Sandcat combines multi-process scanning technology with the Lua language to perform over 260 Web application security checks targeting local or remote Web servers. The scanner crawls Web sites searching for more than 38 types of Web attacks, including XSS, directory transversal problems, attempts to execute commands, and all CWE, SANS Top 25, OWASP Top 10 Web and Top 5 PHP vulnerabilities. Sandcat Pro adds the ability to scan SSL-enabled Web servers, ability to run multiple Sandcat instances in multiple windows, a full version of the Sandcat Console application with two graphical user interfaces, support for interrupting and resuming scan sessions (checkpoint restart), more extensive vulnerability information and references (CVE, NVD, CWE, Bugtraq, Open Source Vulnerability Data Base [OSVDB]) in the tool's reports, which can be generated and exported in multiple formats (HTML, PDF, XML, plaintext, CSV, RTF, XLS, Word) with ability to configure automatic email alerts (emailing reports as soon as the scan is completed), automatic updates (*via* the Internet), 24/7 technical support, and license terms that allow use of Sandcat in professional vulnerability assessment/penetration testing service offerings.

Syhunt Sandcat and Sandcat Pro

Type	Web Application Scanner
Target(s)	Web applications running on UNIX, Linux, or Windows
Format	Software
OS	Windows XP, 2003, 2008, Vista, 7
Hardware	128 MB RAM, 100 MB disk space
License	Commercial
SCAP Validated	
Standards	CVE, CWE
Supplier	Syhunt Cyber-Security Co. (Brazil)
Information	*http://www.syhunt.com/?n=Sandcat.Sandcat*

WATOBO 0.9.5

Abstract

WATOBO (Web Application Tool Box) is intended to enable security professionals to perform (semi-automated) Web application security audits. WATOBO has no attack capabilities and is provided for legal vulnerability audit purposes only. WATOBO works like a local proxy, similar to WebScarab, ParosProxy, or Burp Suite, but also supports passive and active checks. The passive checks act like filter functions to collect useful information, *e.g.,* email or IP addresses, during normal browsing activities. No additional requests are sent to the (Web) application. Active checks produce a large number of requests. It is the active checks that do the automated part of vulnerability identification during a scan. WATOBO also provides Session Management capabilities that enable the user to define login scripts and logout signatures. The tool is configured to perform vulnerability scans "out of the box". Also, because it is written in FXRuby, it enables the user to define custom checks.

WATOBO 0.9.5

Type	Web Application Scanner (with manual pen testing)
Target(s)	
Format	Software
OS	Windows (XP, Server 2003/2008, Vista, 7); Linux (BackTrack 4, Ubuntu, OpenSuSE), Mac OS X
Hardware	
License	Open Source
SCAP Validated	
Standards	
Supplier	Andreas Schmidt/Siberas IT-Sicherheitsberatung Schmidt & Apelt (Germany)
Information	*http://sourceforge.net/apps/mediawiki/watobo/index.php*

MULTILEVEL SCANNERS

Belarc® BelManage: BelSecure Module

Abstract

The BelSecure Module within Belarc's BelManage enterprise system management solution performs automatic vulnerability assessments of IT systems, and checks their security policies, configuration settings, and discovers other information about the targets such as anti-virus status, application versions, security patches, user accounts, *etc.* All policy settings are automatically compared with consensus benchmarks from the Center for Internet Security, enabling IT managers to automatically determine the security status of their IT assets in advance of an attack. The vulnerability and configuration data is collected daily in BelSecure's central repository. BelSecure Module features include: (1) automated, daily vulnerability assessments, including assessments of Microsoft OSs and applications and Web applications; (2) Automatic configuration comparisons against Center for Internet Security and FDCC checklists; (3) Collection of all configuration and vulnerability data into a central repository; (4) Automation of security compliance checking (*e.g.,* for FISMA). BelSecure can only be purchased with BelManage, which can be purchased in agentless and agented versions.

Belarc BelManage: BelSecure Module

Type	Multilevel Scanner
Target(s)	Windows Server 2008 R2, 2008, 7, Vista, 2003, XP, 2000, NT 4, Me, 98, 95; Linux; Microsoft Office Suite applications, Web applications
Format	Software
OS	Agents: see targets Server: Windows Server 2008/2008 R2(64- or 32-bit), Windows Server 2003 (32-bit), Windows 2000 Server, all running SQL Server (2005 Express [included], or 2008/2008 R2, 2005, 2000, 7) or Oracle 10g
Hardware	Disk Space: 300MB disk + 1MB additional disk per target
License	Commercial
SCAP Validated	
Standards	
Supplier	Belarc, Inc.
Information	*http://www.belarc.com/belsecure.html*

Critical Watch FusionVM® Enterprise and FusionVM MSSP

Abstract

FusionVM from Critical Watch is a patented security risk management solution that automates Vulnerability Management and Configuration Auditing that scans network devices, Web applications, and databases. FusionVM discovers networked assets, determines their vulnerabilities and risks, manages risk remediation, tracks exceptions, and displays risk metrics. It also detects, mitigates, and tracks security vulnerabilities in Web applications. It can be purchased as an appliance, or as SaaS (for scanning Internet-facing assets). For internal scanning, a VM Server (including the FusionVM scanning engine) can be deployed on the internal network and remotely managed by Critical Watch. If purchased as an appliance, FusionVM comprises (1) the All-In-One Manager that contains FusionVM Vulnerability Assessment and Management Software; Vulnerability, Asset, and Reporting databases; Policy Compliance Library, and Scanning Engine; and (2) the VM Server that hosts the scanning engine, and can be managed by the All-In-One Manager to enabled distributed scanning. FusionVM MSSP provides the FusionVM Software as a Service infrastructure installed on a set of appliances for purchase by managed security service providers, network operation centers, *etc.*, enabling them to provide FusionVM SaaS to their customers. FusionVM MSSP essentially creates a “SOC [security operation center]-in-a-box” through which organizations can perform vulnerability management and configuration auditing for multiple distinct clients from a centralized console. While it is primarily designed for managed security service providers and service organizations, FusionVM MSSP may also prove useful to very large enterprises with multiple lines of business, divisions, or subsidiaries that are managed as distinct financial units.

Critical Watch FusionVM Enterprise and FusionVM MSSP

Type	Multilevel Scanner
Target(s)	
Format	Appliance
OS	
Hardware	
License	Commercial
SCAP Validated	
Standards	
Supplier	Critical Watch
Information	*http://www.criticalwatch.com/vulnerability-management.aspx* *http://www.criticalwatch.com/products/mssp.aspx*

Imperva® SecureSphere® Discovery and Assessment Server

Abstract

Imperva SecureSphere Discovery and Assessment Server (DAS) provides more than 1,000 vulnerability scanning tests and assessments of platforms, software, and configurations. The vulnerability assessment process can be fully customized. Test results are captured in a set of detailed reports that document both vulnerabilities and configurations that deviate from defined standards. SecureSphere DAS's discovery capability locates databases on the network and reveals undocumented "rogue" databases. SecureSphere DAS then scans the databases for sensitive data of interest for security and compliance (PCI DSS, Defense Information Systems Agency [DISA] Security Technical Implementation Guides [STIGs], *etc.*), with the scan results highlighting well-known and custom sensitive data types and their locations (down to the database object, row, and column). SecureSphere DAS also enables automatic aggregation and review of user rights through the optional User Rights Management for Databases add-on module, which enables the focused analysis of rights for accessing sensitive data, and identifies excessive rights and dormant accounts based on organizational context, object sensitivity, and actual usage. SecureSphere DAS can also be extended to include database activity auditing/monitoring to enable administrators to define and deploy granular, focused auditing policies. Combined with Imperva's SecureSphere Database Firewall, SecureSphere DAS can support realtime creation of firewall security policies for discovered vulnerabilities before patches are available to remediate them. Management and operation of the DAS are provided *via* browser or console interface to the DAS. DAS can also be configured to provide realtime alerts *via* SNMP, Syslog, email, incident management/ticketing system integration, or a realtime dashboard interface. SecureSphere DAS, like all SecureSphere products, is designed to run on one of the Imperva SecureSphere range of appliances that range in size to support small businesses up to very large enterprises. SecureSphere DAS can also be implemented in a SecureSphere V2500 or V4500 Virtual Appliance; specs for the latter are provided in the table below.

Imperva SecureSphere Discovery and Assessment Server

Type	Multilevel Scanner
Target(s)	Oracle, SQL Server, Sybase, DB2, Informix, MySQL; SAP, Oracle e-Business Suite, PeopleSoft®
Format	Appliance or Software (virtual appliance)
OS	Virtual Appliance: VMware ESX/ESXi 3.5/4.0
Hardware	V2500: two dual-core server Intel VTx or AMD-V, 4GB RAM; V4500: four dual-core server Intel VTx or AMD-V; 8MB RAM; Both: 250GB disk, hypervisor-supported NIC
License	Commercial
SCAP Validated	
Standards	
Supplier	Imperva Inc. (U.S./Israel)
Information	*http://www.imperva.com/products/dsc_database-discovery-and-assessment-server.html*

Integrigy AppSentry

Abstract

Integrigy AppSentry learns the technology and data model of the application to be tested based on policy, configuration, and session definitions defined by the database administrator, security officer, and/or internal auditor. This knowledge enables security audits and checks (implemented in XML and Java) to be tailored specifically for that application. Just as hackers and malicious insiders exploit security issues at different layers of the technology stack, AppSentry can perform a complete security audit of the multi-tiered environment in which the application operates by integrating operating system, Web server, database, and application analyses capabilities in a single tool. The tool enables penetration testing along with automatic scanning of open network ports for well-known and application-specific vulnerabilities, validations of application and technology stack configurations (through analysis of configuration files, logs, file versions), analysis of users and roles to identify separation-of-duty issues, and auditing of transactions to reveal possible fraud activity. Over 300 audits and checks of Oracle products are possible, with additional checks for supported non-Oracle targets. These checks include: OS-level checks for standard Oracle accounts, UNIX and Windows security patches; Web server checks for Apache® configuration (http.conf), logging (http.log), virtual directories, Apache and JServ security patches, SSL configuration, Oracle support cgi-bin scripts, PL/SQL Cartridge exploits; Application server checks for forms and reports security patches, SSL configuration; Database checks for database accounts, listener exploits, database auditing, database security patches, application permissions, database links, Oracle E-Business Suite checks for application accounts, users with system administrator responsibility, application security patches, application auditing, password related profile options, *etc*. The tool also performs audits for compliance (*e.g.*, PCI DSS, FISMA/NIST 800-53, DISA STIGs). AppSentry also provides interfaces for integration with security management systems or SNMP-based network management systems, and supports Syslog, SNMP Trap, and ArcSight® Common Event Format.

Integrigy AppSentry

Type	Multilevel Scanner
Target(s)	Oracle products (on Solaris, HP-UX, AIX, Linux, Windows Server), including Oracle database, E-Business Suite (on Solaris, HP-UX, AIX, Linux, Windows Server), Application Server, WebLogic, PeopleSoft; Microsoft SQL Server (on Windows Server 2000/2003/2008). By July 2011, support for the following additional targets is expected: Oracle Collaboration Suite/Clinical/Retail/Siebel; SAP; DB2; Sybase; Apache; MySQL (AppSentry Open Source Edition only)
Format	Software
OS	Windows 2000 SP4, XP SP1, Vista, 7; console must run Adobe Acrobat 4.0+ and IE 5.0+
Hardware	Pentium+ or AMD CPU, 512MB RAM, 120MB free disk space
License	Commercial
SCAP Validated	
Standards	
Supplier	Integrigy Corporation
Information	*http://www.integrigy.com/products/appsentry*

Jump Network Jabil® Network Vulnerability Assessment System

Abstract

Jump Network's Jabil Network Vulnerability Assessment System (NVAS) targets network-based assets to perform in-depth, detailed vulnerability testing, analysis, and diagnosis, and to provide advice on mitigations and preventive protection measures. In preparation for vulnerability scanning, NVAS uses a combination of test techniques (host survival of probing, intelligent port detection, operating system fingerprint identification, *etc.*), to discover the specific attributes of the targeted network host, including host name, device type, port status, operating system version, and open services. NVAS's scanning methodology enables the tool to detect vulnerabilities and weaknesses in different components of the host, including the operating system and application software. Currently, NVAS can detect more than 2,500 types of vulnerabilities derived from CVE, Bugtraq, and other sources across a variety of popular Web servers, operating systems, applications, and database management systems. Integrated into NVAS is a Web application scanner that can detect vulnerabilities in Web applications and services, and their underlying infrastructure systems. The tool can also characterize host and network risk using CVSS Version 2 scores, asset value, and Chinese national standard risk assessment algorithms (quantitative and qualitative). NVAS prioritizes vulnerabilities (again by CVSS score) to help guide mitigation strategies to ensure that the most dangerous vulnerabilities are mitigated first. The tool can also be configured to automatically invoke a patch manager to patch a vulnerability as soon as it is detected. Scans can be scheduled for periodic execution, and can focus on a single network segment or multiple segments (hierarchical scheduling is also possible). NVAS also includes automated and manual vulnerability validation tools, *e.g.,* pen testing tools, password bruteforcer.

Jump Network Jabil Network Vulnerability Assessment System

Type	Multilevel Scanner (with limited pen testing)
Target(s)	Network services, host OSs, databases (SQL Server, MySQL, PostgreSQL, *etc.*), Web applications/services
Format	
OS	
Hardware	
License	Commercial
SCAP Validated	
Standards	CVE, CVSS
Supplier	Xi'an Jiaotong University/Jump Network Technology Co., Ltd. (China)
Information	*http://www.jump.net.cn/cp/cplx.aspx?code=19 (in Chinese only)*

NSFOCUS Remote Security Assessment System

Abstract

NSFOCUS Remote Security Assessment System automatically detects security vulnerabilities in network and cyber assets, measures their associated risks, and suggests remediations. The system can measure risks by adopting the risk assessment model and provides professional solutions. "One-click" intelligent task mode, one-click scanning, fast reporting, and Intelligent profile technologies are all used. The system leverages the Open Vulnerability Management (OpenVM) platform for controlling vulnerability management workflow, and to provide interfaces and interoperability with third-party products. The tool derives its base of more than 2,400 vulnerabilities from NFOCUS's vulnerability database of more than 11,000 vulnerability signatures. The scanner can also perform deep content analysis of Web applications, to detect SQL injection, credential disclosure, and other Web application vulnerabilities.

NSFOCUS Remote Security Assessment System

Type	Multilevel Scanner
Target(s)	OS (Windows, UNIX, AIX, BSD, HP-UX, Silicon Graphics® Irix®, Linux, Mac OS X, NetWare, Solaris, others); network devices (Cisco, Huawei, 3COM®, Nortel®, Motorola® Vanguard router, Checkpoint firewall, ZyXEL® Prestige Asymmetric Digital Subscriber Line [ADSL] router, Alcatel® ADSL Modem, Alcatel-Lucent Ascend router, Shiva Integrator router, Nortel/Bay Networks Nautica Marlin router, others); HP JetDirect® printer; databases (SQL Server, Oracle, DB2, Informix, Sybase, MySQL, PostgreSQL, others); Web applications
Format	Appliance
OS	
Hardware	
License	Commercial
SCAP Validated	
Standards	CVE
Supplier	NSFOCUS (China)
Information	*http://www.nsfocus.com/en/1_solution/1_2_3.html*

Open Vulnerability Assessment System 4

Abstract

The Open Vulnerability Assessment System (OpenVAS) is a framework of several custom-built and third-party services and tools that collectively implement a vulnerability scanning and vulnerability management solution. The included security scanner is updated daily through a feed of Network Vulnerability Tests; as of January 2011, the scanner supported 20,000 different vulnerability tests. OpenVAS Scanner can scan many target hosts concurrently, and can perform tests *via* an SSL session connection if necessary. OpenVAS Manager can manage multiple OpenVAS Scanners concurrently. It also provides management of scan results, including false positive verification and reduction, and scan operation (start, pause, stop, resume, scheduling). It also provides reporting capabilities, *via* plug-ins, in multiple formats, including (but not limited to) XML, HTML, and LaTeX. The OpenVAS Administrator enables configuration of the OpenVAS user accounts, and synchronization of its data feeds. All OpenVAS tools are accessible *via* Greenbone clients—either a remote client (that can be run from a thin/lean client with only a browser), a full desktop client (implemented in the Qt framework), or a command-line interface client (console). All clients run on Windows, Linux, and other OSs. The third-party tools integrated into the OpenVAS framework are Nikto, Nmap, ike-scan, snmpwalk, amap, ldapsearch, Security Local Auditing Daemon, Ovaldi OVAL interpreter, pnscan, portbunny, strobe, and w3af.

Open Vulnerability Assessment System 4

Type	Multilevel Scanner
Target(s)	Networks, Web applications
Format	Software, Appliance, or SaaS
OS	Linux (CentOS/Fedora/Red Hat/Debian/OpenSuSE/Ubuntu/Scientific Linux/Mandriva/Gentoo®/Slackware/SuSE Linux Enterprise/ArchLinux/BackTrack); FreeBSD; Windows
Hardware	
License	Open source
SCAP Validated	
Standards	
Supplier	Atomic Corporation's OpenVAS Project (Germany)
Information	*http://www0.atomicorp.com/index.html*

SAINT® Professional and SAINT® Enterprise

Abstract

SAINT (originally Security Administrator's Integrated Network Tool) is a suite of integrated products that perform vulnerability scanning, assessment, and validation on network devices, operating systems, databases, desktop applications, Web applications, and other targets. The tool suite includes SAINTscanner, an agentless (*i.e.,* does not require agent software to be loaded on assessed endpoints) vulnerability assessment tool that can perform both authenticated and unauthenticated vulnerability scans that uncover areas of weakness on the target, and recommend remediations. SAINTscanner also performs content scanning to detect data that should not be stored on desktops/servers. SAINTscanner not only detects weaknesses but also identifies remediations that can be applied to them before those weaknesses can be exploited by intruders. It provides information on how to implement those remediations, including pinpointing the most exploitable vulnerabilities for which remediations should be applied first. Captured vulnerability data can be stored locally or remotely (so vulnerability data does not need to be sent over the Internet). SAINTscanner's database of vulnerability checks and exploits is automatically updated each day with new checks/exploits, enabling it to anticipate many common system vulnerabilities. SAINTscanner also enables the user to add custom checks and vulnerability signatures. SAINTscanner can also be used to demonstrate compliance with government and industry regulations, and to perform configuration audits for conformance to policies defined in the FDCC and the U.S. Government Configuration Baseline (USGCB). SAINTscanner reports the presence of exploits, the detected vulnerabilities' CVSS score, the identification of the vendor whose product is found to harbor the vulnerability, and other useful information. SAINT's integrated penetration testing tool, SAINTexploit®, enables the user to exploit and verify vulnerabilities found by the scanner. SAINTmanager® is a remote management console with a centralized GUI for communicating with multiple scanner instances. It provides granular access controls, a dashboard view of the managed scanners, trouble ticket generation, and analyses such as security trending. SAINTmanager is designed for use in larger enterprises in which multiple scans need to be scheduled and managed. SAINTwriter® enables the user to custom design and generate vulnerability assessment, with reports able to present findings of even the largest network scans in a format that uses color charts. SAINT Professional includes SAINTscanner, SAINTexploit, and SAINTwriter. SAINT Enterprise adds SAINTmanager. SAINT can be purchased as a licensed software download, or as one of two types of appliances: SAINTbox® or SAINTstick, both of which come preconfigured with SAINTscanner and SAINTexploit (SAINTmanager and SAINTwriter run on separate desktop systems). SAINTbox comes in three configurations: a 1U rack mount, a desktop box, or a slightly smaller portable box. All three devices host SAINT on a hardened version of Ubuntu Linux. SAINTstick is a bootable, ruggedized USB thumbdrive containing a full deployment of hardened Ubuntu Linux, SAINTscanner, and SAINTexploit, enabling SAINT to be run on any system with a USB port. SAINT is also offered in two on-demand SaaS packages, WebSAINT® and WebSAINT PRO®.

SAINT Professional and SAINT Enterprise

Type	Multilevel Scanner
Target(s)	Network devices; OSs, databases, desktop applications, and Web applications on any host that can be identified by an IP Version 4 (v4) or v6 address or by a URL
Format	Software, Appliance, or SaaS
OS	Linux (CentOS 5.5, Debian, Fedora 14, Mandriva 2010, Red Hat Enterprise 5/6, SuSE, Ubuntu 9.04/10.04), UNIX (Free BSD, SPARC Solaris), or Mac OS X 10.6.5+, with Perl 5.004+ and Firefox 3.6+, IE 8+, Safari® 5+, or Opera®
Hardware	Professional: Minimum -1.6GHz+ CPU; 1GB RAM; 100MB free disk space (1GB recommended); Recommended: Small networks - 2.3GHz+ CPU, 2GB RAM, 1GB disk; Large networks - 2.6GHz+ CPU; 8GB RAM; 1GB disk; Enterprise: 3.0GHz dual CPU; 8GB RAM; 160GB disk
License	Commercial
SCAP Validated	*http://nvd.nist.gov/validation_saint.cfm*
Standards	SCAP, CVE, OVAL, CVSS
Supplier	SAINT Corp.
Information	*http://www.saintcorporation.com/products/productsOverview.html*

SecPoint The Penetrator

Abstract

SecPoint's The Penetrator is a "Vulnerability Scanning Appliance with Penetration Testing Capabilities" that performs automated vulnerability scans based on 43,000+ signatures, enabling it to detect XSS, SQL injection, and other Web errors; The Penetrator includes its own automatic Web crawling engine that can identify both known and unknown files on Web servers. The Penetrator also automates penetration tests such as denial of service attacks, brute force attacks, and other exploits. The Penetrator also detects malware. Multiple Penetrator appliances can be deployed on a network, and centrally managed from the same browser-based console. Automatic auditing can be prescheduled, with automatic alerts when new vulnerabilities are found. The Penetrator can also compare new vulnerabilities against previous audit records to support trends analysis of the target's security posture over time. The appliances come in small form factor desktop and 1U rack mount configurations. The Penetrator software can also be deployed in a VMware virtual machine environment. SecPoint also offers a SaaS version called The Cloud Penetrator.

SecPoint The Penetrator

Type	Multilevel Scanner (with limited pen testing)
Target(s)	Hosts running Windows (98, XP, 2000, Vista, Server 2003), OS/2®, UNIX (AIX, Solaris, NetBSD, OpenBSD, FreeBSD), Linux (Fedora, Gentoo, Slackware, Ubuntu, Mandriva), Mac OS/Mac OS X; networking devices (routers, firewalls, voice over IP [VoIP] servers, other networking devices); Web applications
Format	Appliance (preconfigured Dell® desktop or 1U rackmount running customized Slackware 2.6)
OS	
Hardware	
License	Commercial
SCAP Validated	
Standards	
Supplier	SecPoint ApS [Anpartsselskab] (Denmark)
Information	*http://www.secpoint.com/penetrator.html*

SecPoint The Portable Penetrator

Abstract

SecPoint's The Portable Penetrator is an automated penetration testing system for testing hosts, Web applications, and network devices running on Wi-Fi® networks. In addition to providing all of the same host and Web server vulnerability scans found in The Penetrator, The Portable Penetrator performs security audits for wireless networks encrypted by Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA), or WPA2, and can identify hidden networks. Like The Penetrator, The Portable Penetrator is sold as a preconfigured "appliance", in this case hosted on a preconfigured portable computer (laptop or netbook). The Portable Penetrator software can also be deployed in a VMware virtual machine environment.

SecPoint The Portable Penetrator

Type	Multilevel Scanner (with limited pen testing)
Target(s)	Hosts running Windows (98, XP, 2000, Vista, Server 2003), OS/2, UNIX (AIX, Solaris, NetBSD, OpenBSD, FreeBSD), Linux (Fedora, Gentoo, Slackware, Ubuntu, Mandriva), Mac OS/Mac OS X; networking devices (routers, firewalls, VoIP servers, Wi-Fi hotspot devices, other networking devices); Web applications
Format	Appliance (preconfigured Dell laptop or netbook running customized Slackware 2.6)
OS	
Hardware	
License	Commercial
SCAP Validated	
Standards	
Supplier	SecPoint ApS (Denmark)
Information	*http://www.secpoint.com/portable-penetrator.html*

Symantec® Control Compliance Suite: Vulnerability Manager

Abstract

Symantec Control Compliance Suite is an integrated, automated IT risk and compliance assessment and management system. It comprises four interoperable components that can be purchased separately or as part of a complete Control Compliance Suite. The four components are: (1) Policy Manager (for defining, publishing, and reporting compliance to security control configuration policies); (2) Standards Manager (for performing scans for technical security control standards compliance); (3) Response Assessment Manager (for collecting, creating, and distributing attestation evidence for regulatory and internal compliance reporting); (4) Vulnerability Manager (for end-to-end vulnerability assessments of Web applications, databases, hosts, and network devices, including Supervisory Control And Data Acquisition [SCADA] systems and network devices). It is Vulnerability Manager that is of interest for purposes of this Tools Report. Vulnerability Manager performs 54,000 regularly-updated vulnerability checks representing 14,000+ vulnerabilities. These vulnerabilities include all of the OWASP Top 10 Web application vulnerabilities (*e.g.,* SQL injections, XSS, CRSF, unrestricted URL access, unvalidated redirects). The tool also provides a North American Electric Reliability Corporation (NERC)-compliant "safe scan" mode for SCADA network devices. Moreover, Vulnerability Manager's vulnerability chaining mechanism enables the tool to identify cumulative risks and attack vectors, and the risk scoring algorithm provides insight into whether or not each detected vulnerability is exploitable. Based on feedback from the scanner, displayed in Control Compliance Suite's detailed dynamic Web-based dashboards and reports, the user can identify, remediate, and communicate security risks. Symantec Control Compliance Suite can also be integrated with trouble ticketing systems.

Symantec Control Compliance Suite: Vulnerability Manager

Type	Multilevel Scanner
Target(s)	Host operating systems (*e.g.,* Windows, VMware ESX/ESXi); databases (*e.g.,* MySQL, Sybase, Informix, Oracle, PostgreSQL); Web applications
Format	Software
OS	Server: Windows Server 2003 SP2 or 2008 running Microsoft SQL Server 2005 SP2 Client: Windows XP/2008/Vista/7 running Microsoft Office® 2003 or later
Hardware	Server: Dual 3GHz CPU (64-bit); 4GB RAM; 130GB disk Client: 2.8GHz Intel CPU; 1GB RAM; 1024x768 (or better) res. monitor
License	Commercial
SCAP Validated	*http://nvd.nist.gov/validation_symantec.cfm* (Control Compliance Suite Federal Toolkit 10.5)
Standards	SCAP, OVAL, CVE, CVSS
Supplier	Symantec
Information	*http://www.symantec.com/business/control-compliance-suite*

Symantec Risk Automation Suite

Abstract

Symantec Risk Automation Suite helps organizations continuously discover and visualize all IT networks and assets, prioritize risk accordingly, and measure remediation efforts. Risk Automation Suite includes four critical modules: (1) Asset Discovery—discovers and inventories all networks and assets, including managed and unmanaged devices, and enables network leak detection; (2) Vulnerability Management—conducts ongoing vulnerability detection and reporting for operating systems, infrastructure, network applications and databases; (3) Configuration Management—maintains an accurate inventory of system configurations, including installed software, user accounts and system changes; (4) Policy Management—continuously evaluates system configuration and compliance with standards and policies. All four modules continuously provide information into a centralized Risk Automation Suite portal, enabling an end-to-end measurement process—from asset discovery to analytics, reporting, and workflow. With SCAP-validated vulnerability and configuration scanning options included for agent-less, dissolving-agents, and persistent-agent operation, Risk Automation Suite helps public sector agencies measure and verify compliance with FISMA, FDCC, SCAP, NIST SP 800-53, *etc*. Users also have an option for scanning off-network devices, with results imported into the portal if required. The portal provides an overall IT risk management framework for collecting, reporting and managing compliance and security information; and it is the central point of integration and automation between modules and other IT systems, providing a holistic view of the entire IT environment, as well as the workflow and reporting functions necessary to support compliance programs. The Vulnerability Management module controls the scans for thousands of known vulnerabilities in operating systems, infrastructure, network applications and databases. The module offers management and workflow capabilities to speed and automate the entire vulnerability management lifecycle, and provides options for authenticated SCAP vulnerability scans that reduce the known issues of false-positive and false-negatives, and can leverage existing commercial or open-source unauthenticated vulnerability scanners. The portal collects all vulnerability data, automatically prioritizes findings, and provides detailed reporting by agency unit, platform, network, asset class and vulnerability type.

Symantec Risk Automation Suite

Type	Multilevel Scanner
Target(s)	Network devices, host OSs, databases, network applications
Format	Software
OS	Portal Server: Windows Server 2003/2008 running IIS and SQL Server Scanning Server: Windows Server 2003/2008 running IIS
Hardware	Server: Dual 3GHz CPU (64-bit); 4GB RAM; 130GB disk Client: 2.8GHz CPU; 1GB RAM; 1024x768 (or better) res. monitor
License	Commercial
SCAP Validated	*http://nvd.nist.gov/validation_symantec.cfm*
Standards	SCAP, OVAL, CVE, CVSS
Supplier	Symantec
Information	*http://www.symantec.com/business/risk-automation-suite*

Tenable® Nessus® 4.4

Abstract

Tenable's Nessus is an agentless, active vulnerability scanner that performs vulnerability scanning and analysis (including Web application scanning, *via* a plug-in), as well as compliance checking, asset discovery and profiling, configuration auditing, and sensitive data discovery. Nessus can perform both credentialed scanning (authenticated) and non-credentialed (unauthenticated) scanning. In authenticated scanning, login credentials are provided by Nessus to authenticate itself to the remote host. Nessus includes its own TCP port scanner, but can also be configured to use Nmap. Every audit/test in Nessus is coded as a plug-in—a simple program that checks for a particular flaw. Nessus currently uses more than 40,000 different plug-ins for local and remote flaws. Plug-ins are also available for patch auditing, service auditing, password policy auditing, and Netstat/Windows Management Instrumentation port scanning, and SCADA vulnerability checks for Industrial Control Systems/devices. Nessus vulnerability scanners can be distributed throughout an entire enterprise, inside demilitarized zones (DMZs) and across physically separate networks. Nessus is available as freeware for a wide variety of platforms. While the software is free, commercial organizations that use Nessus must purchase a ProfessionalFeed subscription that allows them to use Nessus to scan their network, and to obtain support and updates to the Nessus database of vulnerability checks and compliance audits. ProfessionalFeed subscribers are also entitled to obtain a hardened, Web-based VMware virtual appliance to host Nessus. Tenable also offers Nessus pre-installed on one of two rack-mountable hardware appliances. Home users must subscribe to Nessus HomeFeed, which licenses the subscriber to scan up to 16 IP addresses on a non-business network, and to get the same support/updates as ProfessionalFeed subscribers. Nessus App for iPhone & iPod touch enables remote login to start/pause/stop a remote Nessus scanner(s). Nessus Perimeter Service provides Nessus 4.4 scans as an on-demand SaaS.

Tenable Nessus 4.4

Type	Multilevel Scanner
Target(s)	TCP/UDP/IP networks; Cisco IOS devices; operating systems including Windows (NT/2000/Server 2003/XP/Vista/7/2008), UNIX/Linux; Windows file content types; SQL databases (Oracle, Microsoft SQL Server, MySQL, DB2, Informix/Distributed Relational Database Architecture, PostgreSQL); Web servers, CGI scripts
Format	Software
OS	Linux (Debian 5, Fedora Core 12/13/14, Red Hat ES 4/5/6, SuSE 9.3/10.0/11, Ubuntu 8.04/9.10/10.04/10.10; FreeBSD 8; Mac OS X 10.4/10.5/10.6; SPARC Solaris 10; Windows XP (pre SP2)/Server 2003/Server 2008/2008 R2/Vista/7; VMware if simulated machine does not use Network Address Translation (NAT)
Hardware	When running on Windows: 2GHz Pentium III+ or dual core Intel CPU for Apple Computers; 1GB RAM (2GB recommended for moderate scans; 4GB for large scans)
License	Freeware/Commercial (software is free, but subscription must be purchased to operate and get support/updates)
SCAP Validated	*http://nvd.nist.gov/validation_tenable.cfm* (part of Tenable SecurityCenter validation)
Standards	SCAP, OVAL, CVE, CVSS
Supplier	Tenable Network Security®
Information	*http://www.nessus.org/products/nessus*

Tenable Passive Vulnerability Scanner

Abstract

Tenable's Passive Vulnerability Scanner (PVS) monitors network traffic in real time. It determines server and client side vulnerabilities and sends these to Tenable SecurityCenter in real time. It also uses advanced protocol analysis to log all file sharing, SQL, HTTP and other types of protocols for analysis to the Tenable Log Correlation Engine. As with Nessus, PVS's tests are coded as plug-ins, with nearly two dozen plug-ins currently available, and protocol analysis for nearly two dozen networking and host protocols. PVS continuously looks for new networks, hosts, applications, and vulnerabilities. Used in tandem with an unauthenticated active scanner, PVS can passively detect client side vulnerabilities in Web browsers, email clients, and other clients. PVS can also perform Web application auditing, including Web server discovery, detection of expired SSL certificates, identification of active Web sites on each Web server, sampling of hosted Web content, identification of hostile ActiveX controls, passive discovery of Web forms and variables, and harvesting of links and email addresses. Tenable's research team updates plug-ins for the PVS as they do for Nessus. And like Nessus, PVS' vulnerability reports include CVE, Bugtraq, and CPE references, OS enumeration, severity ratings, and CVSS scores. Multiple deployments of PVS can be centrally managed by Tenable's SecurityCenter to support distributed passive monitoring of large networks. If both Nessus and PVS are deployed, they can be configured to work in tandem to passively discover new hosts, actively scan those hosts, and display both active and passive scan progress and findings in the same report or dashboard. PVS can also produce realtime logs that can be sent to its Log Correlation Engine for analysis, search, and storage. PVS licenses are available either per sensor (with unlimited IP address targeting) or as Class B or Class C network enterprise licenses (with unlimited deployments of PVS sensors, but limited to a specific IP address range). As with Nessus, PVS can be purchased as software, a virtual appliance, or a hardware appliance.

Tenable Passive Vulnerability Scanner

Type	Multilevel Scanner
Target(s)	TCP/User Datagram Protocol [UDP]/IP networks and associated servers (*e.g.,* DNS servers); OS, email clients and servers (SMTP, IMAP, POP3), Web clients and servers, FTP servers, Web applications (CGI, Java, PHP, ActiveX), P2P servers, Internet Relay Chat/Instant Messaging clients
Format	Software
OS	Linux (Red Hat 4/5, CentOS 4/5 [32/64-bit]), Windows (2003/2008); VMware ESX/Server/Workstation/ Fusion®
Hardware	3GHz CPU; 8GB RAM; 100/1000baseT NIC
License	Commercial
SCAP Validated	
Standards	CVE, CVSS
Supplier	Tenable Network Security®
Information	*http://www.nessus.org/products/ tenable-passive-vulnerability-scanner*

Venusense Vulnerability Scanning and Management System

Abstract

Venusense Vulnerability Scanning and Management System's scan and analysis methodology combines operating system fingerprinting, intelligent port service identification, and other technologies to identify the attributes of scanning targets—including operating system version, network name, users, services opened on abnormal ports, *etc*. Venusense Vulnerability Scanning and Management System can scan for more than 2,300 kinds of vulnerabilities—including nearly 300 database vulnerabilities—across 32 categories. The tool can combine different scan methods for the same vulnerability, to correlate and validate its findings. The system also includes Windows domain scan technology, which makes it possible for the tool to assume administrator privileges to perform authenticated scans. The system uses CVSS scoring of all detected vulnerabilities, and provides prioritized guidelines for vulnerability remediation. CVSS scoring also enables the system to qualitatively and quantitatively assess overall asset risk, by correlating vulnerability risk scores with required asset protection level and value; the risk assessment algorithm the tool uses was developed by the Standardization Administration of China. Vulnerability Scanning and Management System updates its patching information and remediation suggestions through real time tracking and analysis of published information on vulnerabilities. The system's vulnerability database receives bi-weekly updates, as well as immediate *ad hoc* updates whenever a new, significant vulnerability emerges. The system can generate customized reports for various user roles, in various formats (*e.g.,* chart, table, text description), and can export them as PDF, XML, HTML, Excel, or Word files.

Venusense Vulnerability Scanning and Management System

Type	Multilevel Scanner
Target(s)	Network devices (*e.g.,* Cisco, 3Com, Checkpoint, others), network printers, servers and desktops running Microsoft Windows 9X/NT/2000/XP/2003, Sun Solaris, HP UNIX, IBM AIX, IRIX, Linux, BSD, *etc.*, databases (SQL Server, Oracle, Sybase, DB2, MySQL, *etc.*) and applications (Web, *FTP,* Email, *etc.*)
Format	Appliance
OS	
Hardware	
License	Commercial
SCAP Validated	
Standards	CVE, CVSS
Supplier	Beijing Venustech Security Inc. (China)
Information	*http://english.venustech.com.cn/Products/ProductInfo_97.html*

AUTOMATED PENETRATION TEST TOOLS

Arachni

Abstract

Arachni is a modular Ruby pen testing framework for evaluating the security of Web applications. Arachni uses various real-world attack techniques including taint-analysis, fuzzing, differential analysis, timing/delay attacks, as well as novel technologies such as rDiff analysis and modular meta-analysis, developed specifically for the framework. This allows the Arachni to make informed decisions about the nature of a target's response to a variety of different inputs, diminishing false positives and providing human-like insights into the inner workings of Web applications.

Arachni

Type	Automated Pen Testing Framework
Target(s)	Web applications
Format	Software
OS	Linux, UNIX, POSIX-compliant; Window/ Cygwin
Hardware	
License	Open source
SCAP Validated	
Standards	
Supplier	Tasos "Zapotek" Laskos, Matías Aereal Aeón
Information	*http://arachni.segfault.gr/*

CORE IMPACT® Pro

Abstract

CORE IMPACT Pro automates previously manual penetration testing processes, enabling the tester to determine whether attackers can actually exploit network, endpoint, or Web application vulnerabilities. CORE IMPACT Pro provides a series of automated penetration tests "out of the box", including network (including wireless network and network device), client-side (endpoint and end-user), and Web application penetration tests. Unlike scanners and fuzzing tools that provide some vulnerability exploitation capabilities, CORE IMPACT Pro enables the tester to (1) profile systems in a stealthy way by mimicking the evasive techniques of an actual attack; (2) attempt to gain root (administrator) access on the compromised system; (3) "pivot" attacks to other targets on the network; (4) replicate attacker's attempts to access/steal or manipulate data on compromised systems. CORE IMPACT Pro provides attacks of varying complexity in its One-Step Test modules and automated Rapid Penetration Test modules, and also supports tester-development of manual tests and customization of test targets and sequences. Written in Python, CORE IMPACT Pro is extensible with these custom-developed tests and test modules, and its test-control macros can be augmented with tester-developed macros to define custom test scenarios. CORE IMPACT Pro can also be integrated with the Metasploit Framework to combine CORE's library of professionally-developed exploits with the additional network exploits provided by Metasploit. Test results can be captured in HTML and XML formats. The tool can also generate PCI DSS and FISMA compliance reports.

CORE IMPACT Pro

Type	Automated Pen Testing Suite
Target(s)	Web applications, databases, client/server host operating systems, email users
Format	Software
OS	Windows 7 (Ultimate/Pro/Enterprise 32/64-bit); Vista (Ultimate/Enterprise/Business) SP2; Server 2008/2003 R2/2003 SP2; XP Pro SP3; all running IE 7.0
Hardware	3GHz+ Pentium IV, 1GB RAM (2GB recommended), 4GB disk, Ethernet NIC, 1024x768 res. monitor (1280x1024 recommended)
License	Commercial
SCAP Validated	*http://nvd.nist.gov/validation_coresecurity.cfm*
Standards	SCAP, CVE, CVSS
Supplier	CORE Security Technologies
Information	*http://www.coresecurity.com/content/CORE-INSIGHT-Enterprise*

CORE INSIGHT Enterprise

Abstract

CORE INSIGHT Enterprise is an automated security testing and measurement solution that can be used to continuously assess the security of an organization's Web applications, networks, and client-side weaknesses. CORE INSIGHT Enterprise does not scan for potential vulnerabilities, monitor for incidents, or model threats. Instead it replicates real-world attacks against systems and data, using the same offensive techniques that hackers employ to find and exploit weaknesses and expose critical data. In this way the tool reveals paths of exposure to vulnerabilities in specific assets in enterprise networks of 10,000 systems, Web applications, and users. CORE INSIGHT Enterprise employs a seven step testing methodology: (1) Target Environment Profiling to discover all potential targets; (2) Test Campaign Definition of what tests will be used; (3) Attack Path Calculation to determine in what sequence to run tests, against which targets first; (4) Attack Replication (actual execution of attacks); (5) Adaptive Path Adjustment, to calculate new attacks and paths based on results from prior attacks; (6) Adaptation to Infrastructure Changes, to add new infrastructure components as targets for future testing; (7) Dashboarding and Reporting of test results. CORE INSIGHT Enterprise includes a variety of connectors to popular network and Web vulnerability scanners, enabling the tool to import scanner results and validate their detected vulnerabilities for exploitability. Connectors are also provided to popular network management systems, so that CORE INSIGHT Enterprise can import network topographies as the basis for defining its assessment surfaces. CORE INSIGHT's CSO Dashboard provides centralized control and viewing of security testing activities and results, including at-a-glance view with full drill-down capabilities to enable the tester to focus in on specific operational areas and test campaigns.

CORE INSIGHT Enterprise

Type	Automated Pen Testing Suite
Target(s)	Network devices (routers, hubs, switches, firewalls, IDS/IPS, *etc.*), Web applications, databases (Microsoft SQL Server, Oracle, IBM DB2, *etc.*), server client/server host operating systems (Windows, Linux, Mac OSs, *etc.*), endpoint applications (*e.g.,* antivirus/antiphishing/antimalware systems, host IDS/IPS, browsers, email clients, instant messengers, media players, business applications, productivity tools, *etc.*) and end users.
Format	Software
OS	Windows 7 (Ultimate/Pro/Enterprise 32/64-bit); Vista (Ultimate/Enterprise/Business) SP2; Server 2008/2003 R2/2003 SP2; XP Pro SP3; all running IE 7.0
Hardware	3GHz+ Pentium IV, 1GB RAM (2GB recommended), 4GB free disk space, Ethernet NIC, 1024x768 res. monitor (1280x1024 recommended)
License	Commercial
SCAP Validated	
Standards	
Supplier	CORE Security Technologies
Information	*http://www.coresecurity.com/content/CORE-INSIGHT-Enterprise*

Google® Skipfish

Abstract

Google Skipfish is an active Web application penetration testing and security reconnaissance tool suite. It prepares an interactive sitemap for the targeted site by carrying out a recursive crawl and dictionary-based probes that produce customized dictionaries through an auto-learning capability that builds an adaptive, target-specific dictionary based on the tool's site content analysis. The resulting map is then annotated with the output from a number of active (but hopefully non-disruptive) security checks. The final report generated by the tool is meant to serve as a foundation for professional Web application security assessments. Unlike Web vulnerability scanners, Skipfish uses probes and tests to trigger and observe behavioral patterns rather than relying on pattern-matching with vulnerability signatures. Skipfish includes tests for vulnerabilities to server-side SQL, PHP, shell command, XML, and XPath injections, format string vulnerabilities, integer overflow vulnerabilities, XSS, directory traversal/file inclusion, untrusted embedded content, HTTP credentials in URLs, self-signed SSL certificates, Multipurpose Internet Mail Extensions (MIME) type and character set mismatches, as well as other exploitable security issues. Skipfish can also recognize obscure HTTP 404 error-related behaviors, unusual parameter passing conventions, redirection patterns, content duplication, *etc.* At this point, Skipfish is still considered experimental, and does not satisfy most of the requirements outlined in the Web Application Security Consortium (WASC) Web Application Security Scanner Evaluation Criteria. Skipfish requires relatively little configuration, but is intended for expert users; it is not intended to be a point-and-click tool.

Google Skipfish

Type	Automated Pen Testing Suite
Target(s)	Web applications
Format	Software
OS	Linux, FreeBSD, Mac OS X, and Windows/Cygwin
Hardware	
License	Open Source
SCAP Validated	
Standards	
Supplier	Google Skipfish
Information	*http://code.google.com/p/skipfish/wiki/SkipfishDoc*

Immunity® CANVAS® Professional

Abstract

CANVAS is an automated exploitation system plus exploit development framework. The tool currently provides more than 370 exploits, with four new exploits released each month (on average) targeting high-value vulnerabilities, such as remote, pre-authentication, and new vulnerabilities in common software.

Immunity CANVAS Professional

Type	Automated Pen Testing Framework
Target(s)	All common platforms and applications
Format	Software
OS	Windows, Linux (validated on Ubuntu and Fedora), Mac OS X, UNIX, other OSs (*e.g.,* mobile phone OSs) with Python25/26, GTK2, pycairo, pygobject, and pygtk installed
Hardware	1.2GHz CPU, 1GB RAM, 250MB disk, wired or wireless NIC
License	Commercial
SCAP Validated	
Standards	
Supplier	Immunity, Inc.
Information	*http://www.immunitysec.com/products-canvas.shtml*

Immunity SILICA®

Abstract

SILICA is an automated, Wi-Fi-specific, vulnerability assessment and penetration testing tool suite. SILICA determines the risk of a particular access point by non-intrusive exploitation of vulnerabilities to determine what assets the vulnerable access point exposes to compromise. SILICA reports whether a given vulnerability can be successfully exploited. Attacks automated by SILICA include (1) Recovery of WEP, WPA (1 and 2 and Lightweight Extensible Authentication Protocol (LEAP) keys; (2) Passive hijacking of Web application sessions for email, social networking, and Intranet sites; (3) Mapping a wireless network and identifying its relationships with associated clients and other access points; (4) Passive identification of vendors, hidden Service Set Identifiers (SSIDs), and equipment; (5) Scanning and penetrating hosts on the network using integrated Immunity CANVAS exploit modules and commands to recover screenshots, password hashes, and other sensitive information; (6) Man-in-the-middle attacks to find valuable information exchanged between hosts; (7) Capturing and reporting wireless and network data. SILICA's specific features include: access point recon and analysis and exploits; automated client discovery; automated exploit execution; automated SSID discovery; WEP, WPA 1/2, and LEAP credential recovery; man-in-the-middle capability. SILICA can scan up to 256 Wi-Fi-based hosts/devices simultaneously.

Immunity SILICA

Type	Automated Pen Testing Suite
Target(s)	802.11 a/b/g/n Wi-Fi-based hosts and devices
Format	Appliance or Software
OS	*Software:* Ubuntu Linux (native or on VMware)
Hardware	Intel CPU, Personal Computer Memory Card International Association PC Card or ExpressCard
License	Commercial
SCAP Validated	
Standards	
Supplier	Immunity, Inc.
Information	*http://www.immunitysec.com/products-silica.shtml*

Parasoft® SOAtest with Parasoft Load Test

Abstract

The Security Testing component of Parasoft's Load Test detects security vulnerabilities in Web service-based service oriented architectures (SOAs) through penetration testing and execution of complex authentication, encryption, and access control test scenarios. The Parasoft Functional & Load Testing Solution automatically generates tests to perform security penetration testing at the message layer. By testing the SOA with penetration attacks and analyzing the responses, security vulnerabilities can be discovered and fixed earlier in the software development cycle. The following penetration tests are currently supported: Parameter fuzzing, SQL injections, XPath injections, XML bombs, external entities, malformed XML, invalid XML, username harvesting, large XML. Parasoft's solution includes security support for testing Web services with security layers. At the transport level, it supports SSL (both server and client authentication), basic, Digest and Kerberos authentication. At the message level, it supports WS-Security including X.509, Security Association Markup Language (SAML), Username security tokens, XML Encryption and XML Digital Signature. The solution allows for security token validation as well as negative tests that ensure proper enforcement of message integrity and authentication. Parasoft's solution automatically generates tests to perform security penetration testing of Web interfaces. By simulating a hacker and "attacking" a Web site with malformed input data, it can uncover OWASP Top 10 issues such as SQL injection, XSS, buffer overflow, command injection, unvalidated input, and more. The solution also uses a database of over 4,000 checks to find vulnerabilities related to outdated server applications, default installations, and so on. This helps secure and standardize HTML to enforce best practices related to login forms, comments, hidden fields, and other security-relevant HTML issues. Parasoft's pattern-based code analysis verifies that your organization's security policy is implemented in your application code (JavaScript, VBScript/ASP, HTML, JSP, Java, .NET, and so on). It also identifies common security vulnerabilities. Parasoft's static analysis rule set is constantly being extended. In addition, Parasoft's data flow static analysis detects injection vulnerabilities, XSS, exposure of sensitive data, and other vulnerabilities without test cases or application execution. Moreover, Parasoft's peer code review process automation facilitates the high-level code review that is often required for regulatory compliance (PCI DSS, *etc.*). SOAtest comes in several editions; however, only Server Edition currently has a Load Test license included.

Parasoft SOAtest with Parasoft Load Test

Type	Automated Pen Testing Suite
Target(s)	*Representative (not complete list):* IBM WebSphere, Oracle (including BEA WebLogic and *AquaLogic), .NET* (with Windows Communication Foundation), Software AG/webMethods, Progress® Sonic® (SonicMQ®, SOAP/XML, Java Message Service [JMS])
Format	Software
OS	Windows 2000/2003/XP/Vista/7; Linux; Solaris. If running plug-in version of SOAtest with Load Testing Solution plug-in, must also run Eclipse 3.2.1+
Hardware	
License	Commercial
SCAP Validated	
Standards	
Supplier	Parasoft Corp.
Information	*http://www.parasoft.com/jsp/solutions/soa_solution.jsp?itemId=319#security_testing*

Rapid7® Metasploit® Express

Abstract

Rapid7 Metasploit Express is a single-user penetration testing tool that enhances the features of the open source Metasploit Framework, with which it is tightly integrated, by adding a graphical user interface that guides the user through the penetration workflow steps of discovery, gaining access, taking control, and collecting evidence. Express also automates many common penetration testing tasks, and provides the ability to launch advanced attacks without the need to develop custom scripts. It provides live, HTML, PDF, and Word reporting options, and like Metasploit Pro, can be integrated with Nmap and NeXpose®. Because it draws its exploits from the Metasploit Framework, Metasploit Express provides the same tests and supports the same targets as Metasploit Pro. Express also lacks the following features available only in Metasploit Pro: VPN tunnel support, standard and custom Web application discovery, client-side social engineering attacks, team collaboration for concert attack simulations, PCI DSS compliance reporting, customizable report templates, team-wide audit logging, command-line interface, advanced Metasploit Pro console, access control at the sub-project level, asset tagging.

Rapid7 Metasploit Express

Type	Automated Pen Testing Framework
Target(s)	Web applications, network devices, database servers, endpoint systems, and email users on the following platforms: Linux (Ubuntu, BackTrack, Red Hat), Mac OS X, Windows, UNIX, Apple iPhone®, Google Android®, Nokia® N900
Format	Software
OS	Windows (XP, 2003, Vista, 2008 Server, 7); Linux (Red Hat Enterprise 5.x, Ubuntu 8.04+ [32-bit/64-bit]; may run on other Linux distributions, but not validated on them by Rapid7)
Hardware	2GHz+ processor, 2GB RAM (increase as needed if running virtual machine targets on the same device), 500MB disk, 10/100Mbps NIC
License	Commercial
SCAP Validated	
Standards	CVE
Supplier	Rapid7
Information	*http://www.metasploit.com/*

Rapid7 Metasploit Pro

Abstract

Rapid7 Metasploit Pro Advanced provides automated multi-layered penetration testing capabilities for Web, network, and endpoint targets; the tests also employ stealth features that enable the tests to run despite the presence of IDS, IPS, anti-virus, and endpoint protections. The Metasploit Pro Workflow Manager automates penetration testing steps that security professionals would otherwise conduct manually. Rapid7 researchers apply strict quality assurance and reliability ratings for all exploits to ensure they are safe to use and don't install any software on the target system. Metasploit Pro can be integrated with Nmap and Rapid7 NeXpose (optional), enabling those tools to be run from within Metasploit Pro. This enables the user to narrow Metasploit tests to targeting the most vulnerable systems on the network first. Metasploit Pro delivers the following core capabilities: (1) It leverages the Metasploit Database, an integrated public database of exploits and payloads to conduct its tests; (2) It can target both standard and custom Web applications, network devices, database servers, endpoint systems, and email users; (3) Its graphical user interface and step-by-step test execution model simplifies usability and enhances penetration tester efficiency; (4) It can tunnel any traffic through the target, for example to route vulnerability scans through a compromised machine; (5) It uses phishing and endpoint security testing to create exploit campaigns, track click-throughs, and capture passwords; It can identify Web services across the entire enterprise, audit those services for vulnerabilities, and exploit those vulnerabilities to validate the results; (6) It can support team-coordinated concerted attacks; (7) its online and offline reporting capabilities provide detailed vulnerability descriptions and remediation information, and support customization of reporting templates.

Rapid7 Metasploit Pro

Type	Automated Pen Testing Framework
Target(s)	Web applications, network devices, database servers, endpoint systems, and email users on the following platforms: Linux (Ubuntu, BackTrack, Red Hat), Mac OS X, Windows, UNIX-like platforms, Apple iPhone, Google Android, Nokia N900
Format	Software
OS	Windows (XP, 2003, Vista, 2008 Server, 7); Linux (Red Hat Enterprise 5.x, Ubuntu 8.04+ [32-bit/64-bit]; may run on other Linux distributions, but not validated on them by Rapid7)
Hardware	2GHz+ processor, 2GB RAM (increase as needed if running virtual machine targets on the same device), 500MB disk, 10/100Mbps NIC
License	Commercial
SCAP Validated	
Standards	CVE
Supplier	Rapid7
Information	*http://www.metasploit.com/*

Rapid7 NeXpose

Abstract

Rapid7 NeXpose identifies exploitable vulnerabilities by mimicking more than 54,500 attacks that find more than 14,000 types of vulnerabilities. The tool also provides detailed remediation guidance that includes time estimates, exploit risk score, and asset criticality. In addition to vulnerability checking, NeXpose performs compliance and policy checks, including PCI DSS, FISMA, *etc.* It provides an option for operating over FIPS-140-compliant encrypted network connections. NeXpose can be integrated, out-of-the-box, with the Metasploit® penetration testing framework, and with any third-party security, compliance, or risk management solutions for which NeXpose provides a pre-built integration *via* the NeXpose XML-based open API. NeXpose is offered in four versions: (1) NeXpose Enterprise®, intended for organizations with large, complex networks of more than 1,024 IP addresses; NeXpose Enterprise is intended to be installed on dedicated servers that host no other security software (*e.g.,* no IPS, IDS, virus scanner, *etc.*); (2) NeXpose Consultant, intended for use by independent security consultants and auditors, and designed to run on a laptop; it also provides configuration features that tune the tool for one-time integrated scans/tests; (3) NeXpose Express, intended for small-to-medium sized businesses (Class C networks with 256 IP addresses or fewer), and also intended to be deployed on a laptop; (4) NeXpose Community, a free, single-user edition intended for single user or home business use on networks of 32 or fewer IP addresses; the Community version lacks custom scan and report configuration, email alert, Web application scanning, compliance/configuration scanning, and provides only limited reporting (XML format only).

Rapid7 NeXpose

Type	Automated Pen Testing Suite
Target(s)	Networks, operating systems, databases, Web applications
Format	Software
OS	Windows Server 2003 SP2/R2, Red Hat Enterprise Linux 5, Ubuntu 8.04 Long Term Support; VMware ESXi 4,
Hardware	2GHz+ Intel CPU, 4GB RAM (32-bit) or 8GB RAM (64bit), 90GB+ disk, 100Mbps NIC
License	Commercial (Community edition is Freeware)
SCAP Validated	*http://nvd.nist.gov/validation_rapid7.cfm*
Standards	SCAP, OVAL, CVE, CVSS
Supplier	Rapid7
Information	*http://www.rapid7.com/products/nexpose-enterprise-edition.jsp* *http://www.rapid7.com/products/nexpose/features/overview.jsp*

Spirent® Avalanche Vulnerability Assessment

Abstract

Avalanche Vulnerability Assessment provides integrated ThreatEx capabilities for attack and vulnerability generation for use in exposing devices and networks to actual threats in a controlled test lab environment. Avalanche Vulnerability Assessment comprises: (1) Avalanche Attack Designer, which enables threats to be created without programming; (2) Threat Knowledge Base of more than 3,500 named attacks (including networking protocol attacks, distributed denial of service, worms, email attacks, viruses/Trojans, VoIP attacks, application penetrations, evasive attacks, *etc.*) and hundreds of thousands of variants, to which detected threats are posted, thereby continuously updating the tool's library of threat definitions; (3) Avalanche API for automating test cases and the testing process *via* Tcl scripts. The Avalanche Vulnerability Assessment runs on all of Spirent's Avalanche hardware appliances.

Spirent Avalanche Vulnerability Assessment

Type	Automated Pen Testing Suite
Target(s)	Networks
Format	Appliance
OS	
Hardware	
License	*Tool:* Open source; *Appliance:* Commercial
SCAP Validated	
Standards	
Supplier	Spirent Communications (UK)
Information	*http://www.spirent.com/Solutions-Directory/Avalanche/Avalanche_Vulnerability_Assessment.aspx*

w3af

Abstract

w3af is a Web Application Attack and Audit Framework for use in locating and exploiting Web application vulnerabilities. The framework comprises three types of plug-ins: discovery, audit, and attack. Discovery plug-ins implement Web spidering and other discovery techniques to find new URLs, forms, and other "injection points" (exposures) in Web applications. The plug-in takes a URL as input and returns one or more injection points. If multiple Discovery plug-ins are executed, they will recursively chain their results, so that new URLs found by one plug-in will be forwarded to the next plug-in when it comes online, with new plug-ins activated until all possible information about the targeted Web server has been discovered. Audit plug-ins target the injection points found by Discovery plug-ins by sending specially-crafted data to them that will reveal their vulnerabilities, *e.g.,* SQL injection vulnerabilities. The third type of plug-ins, the Attack plug-ins, attempt to exploit the vulnerabilities found by the Audit plug-ins. Success of an Attack plug-in results in their return of a shell on the targeted remote server or, in the case of SQL injection exploits, a dump of remote tables from the targeted database. The tool provides two user interfaces, one command line, the other graphical.

w3af

Type	Automated Pen Testing Framework
Target(s)	Web applications
Format	Software
OS	Windows XP/Vista (validated), OpenBSD (validated), any other platform that supports Python (not validated); all must have Python 2.5 and related files installed
Hardware	
License	Open source
SCAP Validated	
Standards	
Supplier	Rapid7 (Andrés Riancho)
Information	*http://w3af.sourceforge.net/*

Wapiti 2.2.1

Abstract

Wapiti audits the security of Web applications by performing "black box" scans. Wapiti's penetration tests do not rely on a vulnerability database, although it does use a vulnerability database as the basis for crafting its attacks. Wapiti's objective is to discover unknown vulnerabilities in Web applications. Specifically, Wapiti scans the Web pages of a deployed Web application, looking for scripts and forms into which it can inject data. Once it has compiled a list of all forms in the Web application, Wapiti acts as a fuzzer, injecting payloads to discover whether each script is vulnerable. Wapiti can detect the following vulnerabilities: file handling errors (local and remote *include/require, fopen, readfile, etc.*); database injections (PHP/JSP/ASP SQL injections and XPath injections); XSS; LDAP injection; command executions (*eval(), system(), passtru(), etc.*); carriage return/line feed (CR/LF) attacks (HTTP response splitting, session fixation, *etc.*). Wapiti is able to differentiate between temporal and permanent XSS vulnerabilities. Each time a script is found that allows an HTTP upload or that returns an HTTP 50*x* error code (used frequently in ASP/IIS applications), Wapiti issues a warning. Wapiti can also generate complete reports that include all discovered vulnerabilities, together with information that suggests ways to fix them.

Wapiti 2.2.1

Type	Automated Pen Testing Suite
Target(s)	Web applications
Format	Software
OS	Any OS in which a Python interpreter and runtime are installed (including Windows, Mac OS X, Linux)
Hardware	
License	Open source
SCAP Validated	
Standards	
Supplier	Nicolas Surribas (Spain)
Information	*http://www.ict-romulus.eu/Web/wapiti/home*

Websecurify

Abstract

Websecurify is an integrated Web security testing environment, which can be used to identify Web vulnerabilities by using advanced browser automation, discovery, and fuzzing technologies. The platform is designed to perform automated as well as manual vulnerability tests. At the core of the platform sits a Web browser through which Websecurify gains fine-grained control over the targeted Web application and detects vulnerabilities. All of Websecurify's tools and platform features are integrated into a single cohesive test system with a graphical user interface that supports smooth transitioning from one type of test, and eases management of the complex flow of data gathered during penetration testing. Websecurify includes a built-in vulnerability scanner and analysis engine that can automatically detect many types of Web application vulnerabilities as penetration testing proceeds. These vulnerabilities include: SQL injection, local and remote file Includes, XSS, CSRF, information disclosure problems, session security problems, and many others, including all categories in the OWASP TOP 10. The toolset is designed to be extensible: virtually all platform components can be extended through add-ons and plug-ins (implemented in JavaScript, Python, C, C++, Java, and other Web application languages) to support new tests and business specific customizations. The Websecurify security testing engine is also available for the Google Chrome Web browser.

Websecurify

Type	Automated Pen Testing Framework
Target(s)	Web applications, including those that use newer Web technologies (*e.g.,* HTML 5)
Format	Software
OS	Windows, Mac OS X, Linux
Hardware	
License	Open source
SCAP Validated	
Standards	
Supplier	GNUCITIZEN Information Security Think Tank
Information	*http://www.websecurify.com/overview*

VULNERABILITY SCAN CONSOLIDATORS

Note that this section focuses on tools the main purpose of which is to consolidate outputs from across multiple vulnerability and compliance scanners. This section does not include Enterprise Security Management systems that consolidate data from across a larger range of security tools, which may include vulnerability scanners.

Atlantic Systems Group Information Assurance Application 3.0

Abstract

Atlantic Systems Group's (ASG's) Information Assurance Application (IA²) 3.0 is a fully integrated workflow management system that supports full lifecycle management and assessment of SCAP assessments (including OVAL/CVE-compliant vulnerability assessments) and FISMA C&A efforts, from system creation, control definition, control assessments, Plans of Action and Milestones, risk management, and reporting, to continuous monitoring. The system can be used in two ways: with listening agents deployed on all target computers, or in an agentless configuration in which host-based firewalls must be configured to allow inbound TCP port 445 traffic and the scanners must be able to authenticate using Microsoft Active Directory. IA² can synchronize its local database with the output from third party vulnerability scanners (*e.g.,* Nessus, eEye Retina, nCircle WebApp360, *etc.*), combining and cross-referencing the data from each to provide a single picture of the vulnerability status of the assessed environment. IA² also incorporates a reporting solution that enables tracking, trending, and *ad hoc* reporting, with reports output in PDF, RTF, Word, Excel, HTML, XML, and plaintext formats.

ASG Information Assurance Application 3.0

Type	Vulnerability Scan Consolidator
Target(s)	
Format	Software
OS	Windows XP Professional SP2 or Vista
Hardware	
License	Commercial
SCAP Validated	*http://nvd.nist.gov/validation_asg.cfm* (IA² SCAP Module 2.3.8)
Standards	SCAP, OVAL, CVE, CVSS
Developer	Atlantic Systems Group, Inc.
Availability	*http://www.asg.cc/IA2/*

Epok® CAULDRON

Abstract

Epok CAULDRON [7] implements Topological Vulnerability Analysis, invented by researchers at George Mason University Center for Secure Information Systems under sponsorship by the DHS Homeland Security Advanced Research Projects Agency, the Army Research Office, the Federal Aviation Administration, and the National Science Foundation. CAULDRON imports and analyzes vulnerability data collected by network scanners and rulesets from firewalls, then models the interdependencies between detected vulnerabilities *via* attack graphs in which all known attack paths from an attacker to a target are depicted for each vulnerability. This attack path mapping provides the analyst with a concrete depiction of how individual and combined vulnerabilities impact overall network security. CAULDRON also correlates and prioritizes vulnerabilities according to criticality. CAULDRON can consume data output in XML format from Nessus, Foundstone®, and Symantec scanners and rules from McAfee Sidewinder® firewalls.

Epok CAULDRON

Type	Vulnerability Scan Consolidator
Target(s)	
Format	Software
OS	Windows Server 2003 (x32 and x64)
Hardware	
License	Commercial
SCAP Validated	
Standards	
Supplier	Epok, Inc.
Information	*http://www.epok.net/products_cauldron.html*

[7] Formerly "Combinatorial Analysis Utilizing Logical Dependencies Residing on Networks"

Prolific Solutions proVM Auditor

Abstract

Prolific Solutions' proVM Auditor provides views of vulnerability data from various vulnerability assessment tool outputs. proVM Auditor was originally designed to accept the native outputs of the tools most common by the DOD. It presents vulnerability data in a Vulnerability Matrix (rendered as a Microsoft Excel spreadsheet) that simplifies vulnerability management, tracking, and resolution. Users can filter data views to eliminate data that is not of interest. The Matrix also maps vulnerabilities to the DOD Instruction 8500.2 controls that should be used to remediate them. The tool can also generate individual registry key fixes for DISA Gold Disk. proVM Auditor currently accepts the native outputs of eEye Retina, Application Security AppDetective, Tenable Nessus, and Nmap, as well as inputs from DISA Security Readiness Reviews and DISA Gold Disks, plus data in XCCDF format. Prolific Solutions can also customize proVM Auditor to accept native outputs from other tools upon request. Prolific Solutions is also developing proVM Enterprise, which will extend proVM Auditor's capabilities into an enterprise vulnerability management system.

Prolific Solutions proVM Auditor

Type	Vulnerability Scan Consolidator
Target(s)	
Format	Software
OS	Windows running JRE 6 Update 17+
Hardware	1.8GHz+ CPU, 2GB RAM, 250MB disk
License	Commercial
SCAP Validated	
Standards	
Supplier	Prolific Solutions, LLC
Information	*http://www.proso.com/catalog/provm-auditor/*

RedSeal® Vulnerability Advisor 4.2

Abstract

RedSeal Vulnerability Advisor gathers the configurations of all network devices—firewalls, routers, load balancers, wireless access points, *etc.*—and combines this information with the findings of third-party network vulnerability scanner(s). Vulnerability Advisor uses the combined information to identify where vulnerabilities are exposed to untrusted networks, and to generate a prioritized list of the vulnerabilities that cause the greatest business risk. RedSeal Vulnerability Advisor also identifies gaps where network scanning coverage needs to be extended. Types of information highlighted by RedSeal Vulnerability Advisor include: every subnet that can be attacked from the Internet or extranet; risk posed by change requests before the changes are made, highlighting both potential direct vulnerability exposure and downstream risk; the exact devices and rules that expose a vulnerability; exposed, un-scanned subnets. RedSeal Vulnerability Advisor provides detailed reports appropriate for presentation to auditors and management. RedSeal Vulnerability Advisor can accept input from eEye Retina 3.7.9, McAfee Vulnerability Manager 7.0, nCircle IP360 6.8.6, Qualys® QualysGuard® 6.8, Rapid7 NeXpose 4.10, and Tenable Nessus v4.2. It can also interoperate with BMC Remedy Action Request System 7.5 and Service Desk Problem Management 7.0.3 trouble ticket systems, HP Network Automation 7.6, Solarwinds® Orion Network Configuration Manager 6.0, and Tripwire® Enterprise 8.0 configuration management systems, and McAfee ePolicy Orchestrator 4.6 security management system.

RedSeal Vulnerability Advisor

Type	Vulnerability Scan Consolidator
Target(s)	Brocade (BigIron®/FastIron® 8, ServerIron® XL 7.5); Check Point (Provider-1 R65/R70/R71, VPN-1 Power, VPN-1 Unified Threat Management [UTM] R65/R70, VPN-1 Power VSX R65/R70); Cisco (Adaptive Security Appliance [ASA] 8.3.1, Firewall Services Module [FWSM] 2/3/4, IOS 11.0-15.0, NX-OS 5.1, PIX 6.3/7/8, VPN3000 4, Aironet® 12.3/2.4T(5)); Citrix® NetScaler® 9.2 F5; BigIP 10.2; Fortinet FortiOS 4.0; Juniper® (Netscreen® ScreenOS® 6; JUNOS® 8.5/9.3/10.0/10.1/10.4); McAfee Enterprise Firewall 8 (Sidewinder))
Format	Appliance or Software
OS	Server: Windows 2003/2008 Enterprise Server (64-bit) running JRE 6 Client: Windows 7 or XP SP3 running JRE 6 update 17
Hardware	Server: Multicore CPU (2-16 cores), 8-128GB RAM; 250GB+ disk (sizing depends on size and complexity of network to be scanned) Client: 2GB RAM
License	Commercial
SCAP Validated	
Standards	
Supplier	RedSeal Systems Inc.
Information	*http://www.redseal.net/products/redseal-vulnerability-advisor*

Relational Security Rsam® Enterprise Governance, Risk, and Compliance: Threat & Vulnerability Management

Abstract

Relational Security's Rsam is an enterprise governance, risk and compliance platform that integrates business risk assessment data, regulatory assessment data, and vulnerability findings. The Threat & Vulnerability Management component supports vulnerability tracking, enabling users to filter and record appropriate vulnerability data gleaned from existing scanning devices, and automate the vulnerability remediation management process. Using Rsam for vulnerability tracking, organizations can import data from any vulnerability scanning tools that can output their data in XML, Excel, delimited, or ODBC-compliant database format. Rsam enables users to automate the vulnerability management process/workflow by setting up custom workflows based on current processes, configuring alerts and escalation levels and appropriate areas. Rsam supports comprehensive remediation, including remediation selection and prioritization. Rsam records action plans and sets target dates for applying remediations, and will send out reminders and reports on remediation activities. Rsam further supports prioritized remediation by prioritizing and fixing discovered vulnerabilities. Vulnerabilities are prioritized based on other relevant risk data (asset criticality, compliance requirements, known threats, *etc.*), and appropriate action plans are generated and prioritized. Finally, Rsam can assign individual tasks to staff members, and track their progress throughout the assessment and remediation processes. Rsam is offered as client-side software or as SaaS.

Relational Security Rsam Enterprise Governance, Risk, and Compliance: Threat & Vulnerability Management

Type	Vulnerability Scan Consolidator
Target(s)	
Format	Software
OS	Windows running backend SQL Server
Hardware	
License	Commercial
SCAP Validated	
Standards	
Supplier	Relational Security Corp.
Information	*http://www.rsam.com/products_vulnerability.htm*

Skybox® Risk Control

Abstract

Skybox Risk Control automatically collects data from threat feeds, vulnerability scanners, and patch management systems as well as network device configurations for firewalls, routers, load balancers, and more. Risk Control incorporates information about assets and the relative value of systems and services – necessary to rank potential risks. The Risk Control analytical engine normalizes the information into a configuration management database, creates a model of the network, and incorporates Skybox vulnerability content with intelligence about the likelihood and severity of potential attacks. A Skybox IT risk assessment is done from the attacker's point of view – identifying possible access paths and the security gaps that can be used to reach critical assets. Risk Control provides security managers with information on the most critical risks and remediation alternatives. Connected to a ticketing system, Risk Control can also notify the IT security team of system problems.

Skybox Risk Control

Type	Vulnerability Scan Consolidator
Target(s)	Systems/devices from AlterPoint®, BigFix®, Check Point, Cisco, eEye, HP, IBM Internet Security Systems, Juniper Networks, McAfee, nCircle, Nessus, Nortel, Opsware, Qualys, Symantec
Format	Appliance (Skybox 4000) or Software
OS	View Server and Collector: Windows Server 2003/2008/XP/7; CentOS 4 (64-bit), Red Hat Enterprise Linux 5 (64-bit) View Manager: Windows Server 2003/2008/XP/Vista/7; Red Hat Enterprise Linux 5
Hardware	View Server: <500 node network: 2GHz Pentium IV (2.8GHz Xeon dual server recommended), 4GB RAM, 10GB disk (20GB recommended); 501-10,000 nodes: 2GHz Pentium IV (Xeon EM64T or AMD 64-bit Opteron® recommended), 4GB RAM (8GB recommended), 10GB disk (40GB recommended); 10,001+ nodes: Xeon EM64T or AMD 64-bit Opteron, 8GB RAM (16GB recommended), 40GB disk (80GB recommended) Collector: 2GHz Pentium IV, 1GB RAM (2GB recommended), 10GB disk (20GB recommended) View Manager: 2GHz Pentium IV, 500MB RAM (2GB recommended), 500MB disk (2GB recommended)
License	Commercial
SCAP Validated	
Standards	CVE
Supplier	Skybox Security, Inc.
Information	*http://www.skyboxsecurity.com/products/risk-control*

SECTION 4 ▸ Vulnerability Analysis SaaS

An increasing number of vulnerability tool vendors are making their vulnerability scanning and analysis products accessible *via* on-demand or recurring SaaS; in some cases, vendors who used to sell vulnerability scanning tools have moved entirely to providing their technology *via* SaaS offerings. All SaaS vulnerability scans target Internet-facing systems outside the customer organization's firewall. In some cases, the SaaS supplier also offers appliances or agents that can be installed on the customer's private network "behind the firewall", thereby extending the reach of the vulnerability scanning service to the customer's internal networks/nodes. Access from the SaaS vendor's scanning system to the internal appliance(s)/agent(s) is usually provided by an authenticated, SSL-encrypted connection. The services here are expressly offered as on-demand SaaS. Traditional contracted managed services or consulting services for vulnerability assessment or scanning are not included.

The following table lists all vulnerability scanning SaaS offerings discovered by the authors during their research of vulnerability analysis tools. This listing is not intended to be exhaustive, but can be considered representative.

Service	Type of Scanning	Tool(s) used	Vendor	Information
Cenzic ClickToSecure Managed	Web application	Cenzic Hailstorm	Cenzic, Inc.	*http://www.cenzic.com/products/saas/ctsmanaged/*
Comodo HackerGuardian (Free, Standard, and Enterprise editions)	Network	unknown	Comodo Certificate Authority (CA) Ltd. (UK)	*https://www.hackerguardian.com*
Critical Watch FusionVM SaaS	Multilevel	FusionVM MSSP	Critical Watch	*http://www.criticalwatch.com/products/saas.aspx*
Digital Defense Automated Vulnerability Scan (AVS), Vulnerability Lifecycle management (VLM), VLM Pro	Network	Operationally Critical Threat, Asset and Vulnerability Evaluation (OCTAVE) Risk Assessment Utility	Digital Defense, Inc.	*http://www.ddifrontline.com/solutions/vulnerability-scanning-solutions.php* *http://nvd.nist.gov/validation_ddi.cfm*
eEye Retina Community	Network	Retina Network	eEye Digital Security	*http://www.eeye.com/Products/Retina/Community*
HackerTarget.com	Network , Web application	Nmap, sqlx, sqlmap, OpenVAS, Nikto, FierceHackerTarget.com, LLC	unknown	*http://hackertarget.com/*
GamaSec GamaScan	Web application (with limited pen testing)	unknown	GamaSec, ltd. (Israel)	*http://www.gamasec.com/Gamascan.aspx*
German Web Security Web Scan Service	Web application	unknown	German Web Security [Unternehmergesellschaft] (UG) (Germany)	*http://www.german-websecurity.com/*
IBM/Rational AppScan OnDemand and OnDemand Production Site Monitoring	Web application	AppScan Build Server and Standard	IBM/Rational	*http://www.ibm.com/software/awdtools/appscan/ondemand/* *http://www.ibm.com/software/awdtools/appscan/ondemandmonitor/*

Service	Type of Scanning	Tool(s) used	Vendor	Information
MAYFLOWER Chorizo! Free and Standard	Network	Chorizo!	MAYFLOWER GmbH (Germany)	*https://chorizo-scanner.com/*
McAfee Vulnerability Assessment SaaS	Network	Vulnerability Manager	McAfee	*http://www.mcafee.com/us/products/vulnerability-assessment-saas.aspx*
nCircle HITRUST Security and Configuration Audit Service	Network	IP360; Configuration Compliance Manager	nCircle	*http://www.ncircle.com/index.php?s=products_HITRUST*
NETpeas COREvidence	Multilevel	unknown	NETpeas, SA (Morocco)	*http://www.netpeas.org/saas-based-security/*
netVigilance SecureScout (Cloud Edition)	Network	SecureScout (Windows Edition)	netVigilance, Inc.	*http://www.netvigilance.com/cloudedition*
NopSec Vulnerability Risk Management (VRM)	Multilevel	unknown	NopSec	*http://www.nopsec.com/index.php/vrm*
NOSEC iiScan	Web application (with limited pen testing)	Jsky, Pangolin	NOSEC (Hong Kong, China)	*http://www.nosec-inc.com/en/products/iiscan/*
Protecht SaaS Network Vulnerability Scans	Network	Vulnerability Scanning Appliance	Protecht.ca Corporation (Canada)	*http://www.protecht.ca/vulnerability-scan*
Protecht SaaS Website Vulnerability Scans	Web application	Vulnerability Scanning Appliance	Protecht.ca Corporation (Canada)	*http://www.protecht.ca/vulnerability-scan*
Qualys QualysGuard IT Security and Compliance Suite (Vulnerability Management; Web Application Scanning)	Network, Web application	unknown	Qualys	*http://www.qualys.com/products/qg_suite/*
Relational Security Rsam Enterprise Governance, Risk, and Compliance: Threat & Vulnerability Management	Vulnerability scan consolidation	Rsam	Relational Security Corp.	*http://www.rsam.com/products_vulnerability.htm*
SecPoint The Cloud Penetrator	Network, Host, Web application (with limited pen testing)	The Penetrator	SecPoint ApS (Denmark)	*http://www.secpoint.com/cloud-penetrator-web-vulnerability-scanner.html*
Tenable Nessus Perimeter Service	Network	Nessus	Tenable Network Security	*http://www.tenable.com/services/nessus-perimeter-service*
Trustwave® Managed Internal Vulnerability Scanning (IVS)	Network	TrustKeeper®	Trustwave	*https://www.trustwave.com/internal-vulnerability-scanning.php*
Trustwave TrustKeeper	Host	TrustKeeper (optional TrustKeeper Agent extends scans to internal network)	Trustwave	*https://www.trustwave.com/external-vulnerability-scanning.php* *https://www.trustkeeper.net*
Veracode® Application Security and Analysis for Developers	Application code analysis	unknown	Veracode	*http://www.veracode.com/solutions/application-security-for-developers.html*
VUPEN Web Application Security Scanner	Web application	VUPEN Web Application Security Scanner	VUPEN Security S.A. (France)	*http://www.vupen.com/english/services/wass-features.php*

Service	Type of Scanning	Tool(s) used	Vendor	Information
Webroot® Web Security Service Vulnerability Scanning and Spyware Detection	Web application	unknown	Webroot Software, Inc.	*http://www.webroot.com/En_US/business-web-security-saas.html*
WebSAINT	Multilevel	SAINTscanner	SAINT Corporation	*http://www.saintcorporation.com/products/saas/webSaint.html*
WebSAINT PRO®	Multilevel with pen testing	SAINT Professional	SAINT Corporation	*http://www.saintcorporation.com/products/saas/webSaintPro.html*
WhiteHat Security Sentinel Service (Premium, Standard, Baseline, and PreLaunch editions)	Network	unknown (optional Satellite Appliance extends scans to internal network)	WhiteHat Security	*https://www.whitehatsec.com/services/services.html*
ZeroDayScan	Web application	unknown	ZeroDayScan team	*http://www.zerodayscan.com/*

SECTION 5 ▶ Information Resources

The following sections list English-language print and online resources that provide more extensive, in-depth information about vulnerability assessment tools. Excluded are information sources that predate 2001 or that focus on a specific tool or supplier.

5.1 Books

The following are books in print that should be of interest to those wishing to obtain further information on the technical aspects of vulnerability assessment and vulnerability assessment tools, or guidance on acquisition or use of such tools.

- Ali, Firkhan Ali Hamid. *Vulnerability Analysis on the Computer Network Security: Implementation and Practices* (Lambert Academic Publishing, 2010).
- Anton, Philip S., Robert H. Anderson, and Richard Mesic. *Finding and Fixing Vulnerabilities in Information Systems: The Vulnerability Assessment and Mitigation Methodology* (Rand Publishing, 2004)
- Bidgoli, Hossein. *Handbook of Information Security, Volume 3: Threats, Vulnerabilities, Prevention, Detection, and Management* (Wiley, 2006).
- Cross, Michael, Steven Kapinos, Haroon Meer, Igor Muttik, Steven Palmer, and Petko D. Petkov. *Web Application Vulnerabilities: Detect, Exploit, Prevent* (Syngress, 2007).
- EC-Council. *Network Defense: Security and Vulnerability Assessment* (Course Technology, 2010).
- Gregg, Michael and David Kim. *Inside Network Security Assessment: Guarding Your IT Infrastructure* (Sams, 2005).
- Hope, Paco and Ben Walther. *Web Security Testing Cookbook: Systematic Techniques to Find Problems Fast* (O'Reilly Media, 2008).
- Jackson, Chris. *Network Security Auditing* (Cisco Press, 2010).
- Kröger, Wolfgang and Enrico Zio. *Vulnerable Systems* (Springer, 2011).
- Manzuik, Steve, Andre Gold, and Chris Gatford. *Network Security Assessment: from Vulnerability to Patch* (Syngress, 2006).
- McCarthy, Elisabeth and Lisa J. Sotto. *Network Security Assessment* (Lorman Education Services, 2006).
- McNab, Chris. *Network Security Assessment: Know Your Network,* 2nd Edition (O'Reilly Media, 2007).
- Peltier, Thomas R., Justin Peltier, and John A. Blackley. *Managing A Network Vulnerability Assessment* (Auerbach Publications, 2003).
- Renub Research. *Worldwide Vulnerability Assessment Market and 13 Companies Analysis* (MarketResearch.com, 2011).
- Singh, Abhishek, editor. *Vulnerability Analysis and Defense for the Internet* (Springer, 2008).
- Surhone, Lambert M., Mariam T. Tennoe, Susan F. Henssonow, editors. *Vulnerability Scanner* (Betascript Publishing).
- Surhone, Lambert M., Mariam T. Tennoe, Susan F. Henssonow, editors. *Web Application Security Scanner* (Betascript Publishing).
- Surhone, Lambert M., Mariam T. Tennoe, Susan F. Henssonow, editors. *Common Vulnerabilities and Exposures* (Betascript Publishing).
- Vladimirov, Andrew, Konstantin Gavrilenko, and Andriej Michajlowski. *Assessing Information Security: Strategies, Tactics, Logic and Framework* (IT Governance Publishing, 2010).

5.2 Online Publications and Other Web-Based Resources

The following are downloadable technical papers and articles, Web sites, and Web pages pertaining to general vulnerability analysis tool information, specific vulnerability assessment tool technical topics and issues, and guidance and best practices for tool selection, configuration, and administration. The reader is also encouraged to search YouTube for the instructional videos focusing on vulnerability assessment tools.

5.2.1 Resources on Vulnerability Assessment Methods and Technology

- Perry, James. "Lessons Learned in the Establishment of a Vulnerability Assessment Program". Presented at EDUCAUSE Southeast Regional Conferences, Atlanta, GA, 8 June 2005. *http://www.educause.edu/Resources/LessonsLearnedintheEstablishme/160897* (accessed 28 April 2011).
- German Informatics Society Special Interest Group on Security Intrusion Detection and Response Annual Conference on Detection of Intrusions and Malware, and Vulnerability Assessment. *http://www1.gi-ev.de/fachbereiche/sicherheit/fg/sidar/dimva/* (accessed 28 April 2011).
- Dai, Huning, Michael Glass, and Gail Kaiser. "Baseline: Metrics for setting a baseline for Web vulnerability scanners". VULCANA (VULnerability sCANner Assessment benchmark) Project Technical Report, September 2010. *http://www.cs.columbia.edu/~dai/papers/baseline_submission.pdf* and *http://mice.cs.columbia.edu/getTechreport.php?techreportID=1438&format=pdf&* (accessed 28 April 2011).
- Doupé, Adam, Marco Cova, and Giovanni Vigna. "Why Johnny Can't Pentest: An Analysis of Black-box Web Vulnerability Scanners". In *Proceedings of the Seventh Conference on Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA) 2010,* Bonn, Germany, 8-9 July 2010. *http://www.cs.ucsb.edu/~adoupe/static/black-box-scanners-dimva2010.pdf* (accessed 28 April 2011).
- Shelly, David A. *Using a Web Server Test Bed to Analyze the Limitations of Web Application Vulnerability Scanners.* Virginia Polytechnic Institute and State University Master of Science Thesis, 20 July 2010. *http://scholar.lib.vt.edu/theses/available/etd-08102010-184408/unrestricted/Shelly_DA_T_2010.pdf* (accessed 28 April 2011).
- Vigna, Giovanni. "Web Vulnerability Analysis". University of California Santa Barbara CS279 Lecture Notes, 2010. *http://www.cs.ucsb.edu/~vigna/courses/cs279/Slides/WebSecurity.pdf* (accessed 28 April 2011).

5.2.2 Source Selection and Acquisition Resources

- SCAP Validated Products. *http://nvd.nist.gov/scapproducts.cfm* (accessed 28 April 2011).
- OVAL Adoption by Product List. *http://oval.mitre.org/adoption/productlist.html* (accessed 28 April 2011).
- CVE-Compatible Products and Services. *http://cve.mitre.org/compatible/compatible.html* (accessed 28 April 2011).
- WASC: Web Application Security Consortium: Web Application Security Scanner Evaluation Criteria, Version 1.0, 2009. *http://projects.webappsec.org/w/page/13246986/Web-Application-Security-Scanner-Evaluation-Criteria* (accessed 28 March 2011).
- Google wavsep Web Application Vulnerability Scanner Evaluation Project. *http://code.google.com/p/wavsep/* (accessed 28 March 2011).

APPENDIX A ▶ Acronyms, Abbreviations, Glossary

The table in section A.1 lists and amplifies all acronyms and abbreviations used in this document. The table in section A.2 provides a glossary of vulnerability analysis tool-related terms used in this document. As noted in Section 1.3, this glossary provides definitions for vulnerability assessment tool-specific terms only. For broader information and communications technology or information assurance and cybersecurity terminology, the reader is encouraged to consult the following resources:

- International Foundation for Information Technology. *Glossary of Information Technology (IT) Terms and Phrases. http://if4it.org/glossary.html* (accessed 20 March 2011).
- Navy/Marine Corps Intranet. *NMCI Dictionary. http://www.cnic.navy.mil/navycni/groups/public/@pub/@hq/documents/document/cnicd_a064707.pdf* (accessed 20 March 2011).
- World Wide Web Consortium. *Web Services Glossary. http://www.w3.org/TR/ws-gloss* (accessed 20 March 2011).

For general information assurance and cybersecurity terms, the reader is encouraged to consult the following resources:

- NIST. *Glossary of Key Information Security Terms,* NIST Internal Report (NISTIR) 7298 Revision 1, February 2011. *http://csrc.nist.gov/publications/nistir/ir7298-rev1/nistir-7298-revision1.pdf* (accessed 20 March 2011).
- CNSS. National Information Assurance (IA) Glossary. *http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf* (accessed 20 March 2011).
- US-CERT. *IT Security Essential Body of Knowledge (EBK) Glossary of Terms. http://www.us-cert.gov/ITSecurityEBK/EBKGlossary08.pdf* (accessed 20 March 2011).
- Internet Engineering Task Force. *Internet Security Glossary,* Version 2 (RFC [request for comments] 4949). *http://www.ietf.org/rfc/rfc4949.txt* (accessed 20 March 2011).

A.1 Acronyms and Abbreviations

Acronym/Abbreviation	Amplification
®	registered trademark symbol
ACF2	Advanced Communications Function Version 2
AG	Aktiengesellschaft
AIX	Advanced Interactive eXecutive
AJAX	JavaScript And XML
AMD	Advanced Micro Devices
API	application programmatic interface
ApS	Anpartsselskab
ARC	Application Risk Controller
AS/400	Application System 400
ASDL	Asymmetric Digital Subscriber Line

Acronym/Abbreviation	Amplification
ASE	Adaptive Server Enterprise
ASG	Atlantic Systems Group
ASP	Active Server Pages
ASVS	Application Security Verification Standard
AVAST	Automated Vulnerablity Analysis Support Tool
AVDL	Application Vulnerability Description Language
AVDS	Automated Vulnerability Detection System
AVS	Automated Vulnerability Scan
BMC	Boulett Moores Cloer
BRITE	Behavioral Runtime Intelligent Testing Engine
BSD	Berkeley Software Distribution
CA	Computer Associates (formerly)
C&A	Certification and Accreditation
CAESARS	Continuous Asset Evaluation, Situational Awareness, and Risk Scoring
CCE	Common Configuration Enumeration
CD/DVD-ROM	Compact Disc/Digital Video Disk-Read Only Memory
CD&R	Capability Development and Research
CERIAS	Center for Education and Research in Information Assurance and Security
CERT/CC	Computer Emergency Response Team/Coordination Center
CGI	Common Gateway Interface
CHM	Compiled HTML
CME	Common Malware Enumeration
CMS	content management system
CNSS	Committee for National Security Systems
Co.	Company
COPS	Computer Oracle and Password System
CPE	Common Platform Enumeration
CPU	central processing unit
CR/LF	carriage return/line feed
CSRF	cross site request forgery
CSV	comma-separated values
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
CWE	Common Weakness Enumeration
DB2	DataBase 2

Acronym/Abbreviation	Amplification
DAS	Discovery and Assessment Server
DHCP	Dynamic Host Configuration Protocol
DIACAP	DOD IA C&A Process
DISA	Defense Information Systems Agency
DMZ	demilitarized zone
DNS	Domain Name System
DOD	Department of Defense
DOM	Document Object Model
DTIC	Defense Technical Information Center
DVM	DragonSoft Vulnerability Management
EAL	Evaluation Assurance Level
email	electronic mail
ES	Enterprise Server
ESX	Elastic Sky X
ESXi	Elastic Sky Server 3i
FAV	Falcon Vulnerability Analysis
FBI	Federal Bureau of Investigation
FDDC	Federal Desktop Core Configuration
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Management Act
FTP	File Transfer Protocol
GB	Gigabyte(s)
GmbH	Gesellschaft mit beschränkter Haftung
HARM	Hailstorm Application Risk Metric
HIPAA	Health Insurance Portability and Accountability Act
HP	Hewlett-Packard
HP-UX	Hewlett-Packard UniX
HTML	Hyper Text Markup Language
HTTP	Hyper Text Transfer Protocol
HTTPS	HTTP Secure
IA	information assurance
IA^2	Information Assurance Application
IAC	Information Analysis Center
IAS	Internet Application Server
IATAC	Information Assurance Technology Analysis Center

Acronym/Abbreviation	Amplification
IAVA	IA Vulnerability Alert
IBM	International Business Machines
ICMP	Internet Control Message Protocol
ICT	information and communications technology
ID	identifier
IDS	intrusion detection system
IE	Internet Explorer
IEC	International Electrotechnical Commission
IIS	Internet Information Server
Inc.	Incorporated
IO	information operations
IOS	Internetwork Operating System
IP	Internet Protocol
IPS	Intrusion Prevention System
ISO	International Organization for Standardization
ISS	Internet Security Systems
IT	information technology
IVS	Internal Vulnerability Scanning
JRE	Java Runtime Environment
JSP	Java Server Pages
JVM	Java Virtual Machine
Kbps	thousand bits per second
LAN	local area network
LDAP	Lightweight Directory Access Protocol
LEAP	Lightweight Extensible Authentication Protocol
LLC	Limited Liability Corporation
Ltd.	Limited (partnership)
MAC	media access control
Mac OS X	Macintosh Operating System 10
MAEC	Malware Attribute Enumeration and Characterization
MB	Megabyte(s)
Mbps	million bits per second
MD 5	Message Digest 5
MIME	Multipurpose Internet Mail Extensions
NAT	Network Address Translation

Acronym/Abbreviation	Amplification
NERC	North American Electric Reliability Corporation
NetBIOS	Networked Basic Input/Output System
NFS	Network File System
NGS	Next Generation Security
NIC	network interface controller
NISCC	National Infrastructure Security Co-ordination Centre
NIST	National Institute of Standards and Technology
NISTIR	NIST Internal Report
NVAS	Network Vulnerability Assessment System
NVD	National Vulnerability Database
OASIS	Organization for the Advancement of Structured Information Standards
OCTAVE	Operationally Critical Threat, Asset, and Vulnerability Evaluation
ODBC	Open Database Connectivity
OpenVAS	Open Vulnerability Assessment System
OpenVM	Open Vulnerability Management
OS	operating system
OSVDB	Open Source Vulnerability Data Base
OVAL	Open Vulnerability Assessment Language
OWASP	Open Web Application Security Project
P2P	peer-to-peer
PCI DSS	Payment Card Industry Digital Security Standards
PDF	Portable Document Format
pen	penetration
PHP	PHP Hypertext Preprocessor
PIX	Private Internet eXchange
PL/SQL	Procedural Language/SQL
POP3	Post Office Protocol 3
POSIX	Portable Operating System Interface for unIX
PTO	Patent and Trademark Office
PVS	Passive Vulnerability Scanner
R&D	research and development
R2	Release 2
RAM	random access memory
res.	resolution
RFC	request for comments

Acronym/Abbreviation	Amplification
RMF	Risk Management Framework
RPC	remote procedure call
RISC	reduced instruction set computer
RTF	Rich Text Format
SA	Société Anonyme
SaaS	software as a service
SAINT	Security Administrator's Integrated Network Tool (formerly)
SAML	Security Association Markup Language
SANS	System Administration, Networking, and Security
SAP	Systeme, Anwendungen, Produkte
SCADA	Supervisory Control And Data Acquisition
SCAP	Security Content Automation Protocol
SCO	Santa Cruz Operation
SDK	software developer's kit
SEDEF	Susceptibility and Flaw Definition
SHA	Secure Hash Algorithm
SIEM	security information and event management
SMTP	Simple Message Transfer Protocol
SNMP	Simple Network Management Protocol
SNSI	Software Network Security Inspector
SOA	service oriented architecture
SOAP	Simple Object Access Protocol
SOC	security operation center
SP	Special Publication; Service Pack
SPARC	Scalable Performance ARChitecture
SQL	Standard Query Language
S.r.l.	Società Responsabilità Limitata
SSA	Security System Anayzer
SSH	Secure Shell
SSID	Service Set Identifier
SSL	Secure Socket Layer
STIG	Security Technical Implementation Guide
SuSE	Software- und System-Entwicklung
TCP	Transmission Control Protocol
TESS	Trademark Electronic Search System

Acronym/Abbreviation	Amplification
UDP	User Datagram Protocol
UG	Unternehmergesellschaft
UK	United Kingdom
URL	Uniform Resource Locator
U.S.	United States
USB	Universal Serial Bus
USGCB	U.S. Government Configuration Baseline
UTM	Unified Threat Management
v	version (*e.g.,* IP v6)
VBScript	Virtual Basic Script
VEDEF	Vulnerability and Exploit Description and Exchange Format
VLM	Vulnerability Lifecycle Management
VoIP	Voice over IP
VPN	virtual private network
VRM	Vulnerability Risk Management
w3af	Web Application Attack and Audit Framework
WAN	wide area network
WASC	Web Application Security Consortium
WATOBO	Web Application TOol BOx
WEP	Wired Equivalent Privacy
WMI	Windows Management Instrumentation
WPA	Wi-Fi Protected Access
WSDL	Web Services Definition Language
XCCDF	eXtensible Configuration Checklist Description Format
XML	eXtensible Markup Language
XSS	cross site scripting

A.2 Glossary

The following definitions were derived or adapted from definitions of the same terms in the following documents:

- CNSS Instruction Number 4009, *National Information Assurance Glossary,* 26 April 2010. *http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf* (accessed 8 May 2011).
- NIST Internal Report 7298, *Glossary of Key Information Security Terms,* Revision 1, February 2011. *http://csrc.nist.gov/publications/nistir/ir7298-rev1/nistir-7298-revision1.pdf* (accessed 8 May 2011).
- NIST Internal Report 7511, *Security Content Automation Protocol (SCAP) Version 1.0 Validation Program Test Requirements,* Revision 2 DRAFT, 10 February 2011. *http://csrc.nist.gov/publications/drafts/nistir-7511/Draft-NISTIR-7511r2_update2.pdf* (accessed 8 May 2011).
- NIST Special Publication 800-40, *Creating a Patch and Vulnerability Management Program,* Version 2.0, November 2005. *http://csrc.nist.gov/publications/nistpubs/800-40-Ver2/SP800-40v2.pdf* (accessed 8 May 2011).
- UK Centre for the Protection of National Infrastructure. *Introduction to Vulnerability Assessment Tools,* Technical Note 08/04, 1 October 2004. *http://www.cpni.gov.uk/Documents/Publications/2004/2004010-TN0804_Vulnerability_assessment_tools.pdf* (accessed 8 May 2011).

Term	Definition
Agent	A component of a scanner that must reside on the target being scanned. The agent performs the actual scanning, at the direction of a central management system, to which it returns the scan results. The central management system then aggregates, correlates, and reports results from multiple agents.
Appliance	Hardware device specifically designed and/or configured to host a particular application or class of applications, such as a firewall
Authenticated Scanner	A scanner that includes the mechanism necessary to authenticate itself to and run with privileges on the target system, in order to perform its assessment of that system
Common Vulnerabilities and Exposures (CVE)	A dictionary of common names for publicly known information system vulnerabilities.
Common Vulnerabilities and Exposures (CVE)	A format to describe publicly known information security vulnerabilities and exposures. The CVE ID is the actual CVE-conformant identifier of a specific flaw defined within the official CVE Dictionary.
Common Vulnerability Scoring System (CVSS)	A metrical/measurement or scoring system that provides an open framework for determining the relative severity of software flaw vulnerabilities and a standardized format for communicating vulnerability characteristics.
Continuous Monitoring	The process implemented to maintain a current security status for one or more information systems or for the entire suite of information systems on which the operational mission of the enterprise depends. The process includes: (1) The development of a strategy to regularly evaluate selected IA controls/metrics, 2) Recording and evaluating IA relevant events and the effectiveness of the enterprise in dealing with those events, 3) Recording changes to IA controls, or changes that affect IA risks, and 4) Publishing the current security status to enable information-sharing decisions involving the enterprise.

Term	Definition
Database scanner	An automated program or utility that analyzes a particular instance of a database management system installed on the same platform as the scanner, in order to find indications of vulnerabilities in the configuration or implementation of the database management system, as well as in the databases, stored procedures, and database application code on the same platform that make up the database applications associated with that database management system.
False Positive	An alert that incorrectly indicates that a vulnerability (or the indicator of a vulnerability) is present when it is not.
Fingerprinting	Analyzing characteristics of packets sent by a target, such as packet headers or listening ports, to identify the operating system, application software, network protocols, *etc.*, in use on the target.
Host scanner	An automated program or utility that analyzes the particular instance of the operating system installed on the same platform as the scanner, in order to find indications of vulnerabilities in that operating system.
Information Assurance Vulnerability Alert (IAVA)	Notification that is generated when an IA vulnerability may result in an immediate and potentially severe threat to DOD systems and information; this alert requires corrective action because of the severity of the vulnerability risk.
Misconfiguration	A setting within a computer program that violates a configuration policy or that permits or causes unintended behavior that impacts the security posture of a system
National Vulnerability Database (NVD)	The U.S. government repository of standards-based vulnerability management data. This data enables automation of vulnerability management, security measurement, and compliance (*e.g.,* FISMA).
Network scanner	An automated program or utility that analyzes one or more systems or devices on a network in order to find indications of vulnerabilities in those systems/devices.
Network sniffing	A passive technique that monitors network communication, decodes protocols, and examines headers and payloads for information of interest. It is both a review technique and a target identification and analysis technique.
Open Vulnerability and Assessment Language (OVAL)	An XML-based language used for communicating the details of vulnerabilities, patches, security configuration settings, and other machine states in a machine-readable form. An OVAL ID is assigned to identify a specific OVAL format-compliant definition.
Passive Scanning	Scanning that does not involve any direct interaction with a target, such as sending packets to the target.
Patch Scanning	The systematic identification of corrective operating system and application software code revisions. Such corrective revisions are known as patches, hot fixes, or service packs.
Penetration Testing	Security testing in which evaluators mimic real-world attacks in an attempt to identify ways to circumvent the security features of an application, system, or network. Penetration testing often involves issuing real attacks on real systems and data, using the same tools and techniques used by actual attackers. Most penetration tests involve looking for combinations of vulnerabilities on a single system or multiple systems that can be used to gain more access than could be achieved through a single vulnerability.
Port Scanning	Using a program to remotely determine which ports on a system are open (*e.g.,* whether systems allow connections through those ports).

Term	Definition
Remediation	The act of correcting a vulnerability or eliminating a threat. Three examples of remediation are (1) Installing a patch, (2) Adjusting configuration settings, (3) Uninstalling a software program. A remediation that mitigates the threat posed by a particular vulnerability but that does not fix the underlying problem is referred to as a workaround. A workaround often limits functionality of the system or network element containing the remediated vulnerability.
Risk Assessment	The process of identifying, prioritizing, and estimating risks. This includes determining the extent to which adverse circumstances or events could impact an enterprise. Uses the results of threat and vulnerability assessments to identify risk to organizational operations and evaluates those risks in terms of likelihood of occurrence and impacts if they occur. The product of a risk assessment is a list of estimated potential impacts and unmitigated vulnerabilities. Risk assessment is part of risk management and is conducted throughout the Risk Management Framework (RMF).
Scanning	Sending packets or requests to another system to gain information that can be used in a subsequent attack.
Security Content Automation Protocol (SCAP)	A specification for expressing and manipulating security data in standardized ways. SCAP uses several individual specifications in concert to automate ongoing security monitoring, vulnerability management, and security policy compliance evaluation reporting. The purpose of SCAP is to define a method for using specific standardized testing methods to enable automated vulnerability management, measurement, and policy compliance evaluation against a standardized set of security requirements.
Target	The object a scanner analyzes to discover the presence of vulnerabilities. A target may be a collective set of assets on a network (the target of a network scanner), or the operating system, database, or Web application running on a single host.
Threat Analysis	The examination of threat sources against system vulnerabilities to determine the threats for a particular system in a particular operational environment.
Threat Assessment	Process of formally evaluating the degree of threat to an information system or enterprise and describing the nature of the threat.
Unauthenticated Scanner	A scanner that conducts its assessment of a target system without first authenticating itself to and obtaining privileges on that target. Unauthenticated scans are most often network data and port scans.
Vulnerability	An error, flaw, or mistake in the design, code, or configuration of software (or firmware or hardware) that permits or causes an unintended behavior with security implications to occur.
Vulnerability	Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.
Vulnerability Assessment	Systematic examination of an information system or product to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation.
Vulnerability assessment tool (or scanner)	An automated program or utility that can be used to test the capability of a system's or network's security and discover points of weakness. These tools do not provide direct protection or security for a system or network but instead they gather and report information, such that some other mechanism, policy or tool can be put in place to provide protection against any vulnerability found.

Term	Definition
Vulnerability Scan Consolidator	A tool that aggregates, correlates, and reports results from multiple vulnerability scanners.
Web application scanner	An automated program or utility that analyzes a particular instance of a Web server installed on the same platform as the scanner, in order to find indications of vulnerabilities in that Web server's configuration or implementation, as well as software vulnerabilities in the Web pages, scripts, and other logic elements that make up the Web application hosted by that Web server. Some Web application scanners also target Web clients (browsers) and their plug-ins.

APPENDIX B ▸ Obsolete Open Source and Freeware Tools

The following open source and free vulnerability analysis tools have been "frozen" at a release that has not been updated by the tool's developer(s) since December 2008 or earlier. For several of these tools, ongoing support by the developer is uncertain. However, these tools are still cited by some users as being helpful.

Supplier	Tool	Target	Last Update	Information
Johns Hopkins University Advanced Physics Laboratory	Automated Vulnerablity Analysis Support Tool (AVAST)	Network	2005	*http://www.jhuapl.edu/ott/technologies/technology/articles/P02124.asp*
	Grendel-Scan	Web application	2008	*http://grendel-scan.com*
Chinotech Technologies	ParosProxy	Web application	2004	*http://www.parosproxy.org*
LanTricks	LanSpy	Network	2007	*http://lantricks.com/download*
Purdue University Center for Education and Research in Information Assurance and Security (CERIAS) Computer Operations, Audit, and Security Technology Program	Computer Oracle and Password System (COPS)	Database	2000	*ftp://coast.cs.purdue.edu/pub/tools/unix/scanners/cops*
SensePost	Wikto v2.1.0	Web application	2008	*http://www.sensepost.com/labs/tools/pentest/wikto*
Security-Database	Security System Analyzer (SSA)	Host	2008	*http://www.security-database.com/ssa.php*
Virginia Tech	SafetyNet	Network	unknown	*http://opensource.w2k.vt.edu/safetynet.php*
International Secure Systems Lab	SecuBat	Web application	2006	*http://www.iseclab.org/projects/secubat*