hakin9

Consumers test

Security Scanners

hakin9 magazine, *en@hakin9.org, www.hakin9.org/en*

Security Scanners Chart

Dear Readers – we present a new section in hakin9, consumers test. In this edition we asked users about their opinion on advantages and disadvantages of security scanners. You can find out if the prizes are adequate to the quality, what are the main problems that the users experienced and finally you will see the rating.

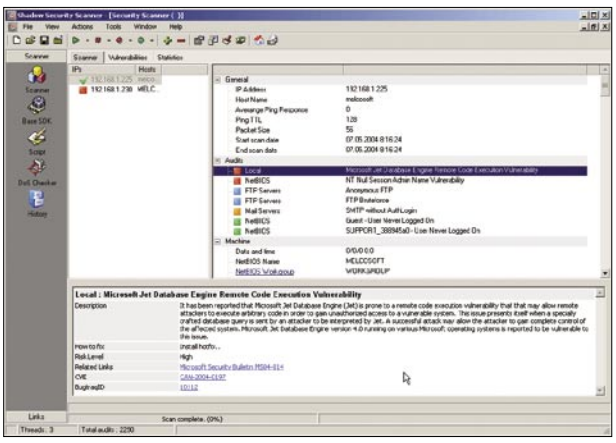
We have decided to compare the most popular security scanners. Here we present users opinions on eight most frequently use products.

Shadow Security Scanner 2005

Shadow Security Scanner is thought to be an excellent vulnerability scanner. The users point out such advantages as a reasonable interface and 5000 of audits that seem to be updated on a daily basis. The most frequent reproach was a too high price. *Excellent product but pricey* the users would say.

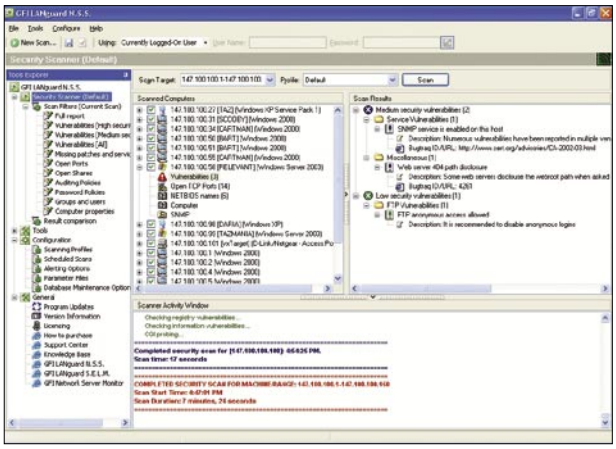
Shadow Security Scanner has been created to provide a secure, reliable and quick detection of a wide range of vulnerabilities. After finishing the system scan, Shadow Security Scanner examins the data collected, finds security system holes and possible errors in server tuning options. Finally it suggests solutions to the problems encountered. Shadow Security Scanner employs a system security analysis algorithm based on a patented *intellectual core*.

Shadow Security Scanner is believed by its authors to work at such a speed and with such a precision so as to be able to compete with the professional IT security services and hackers, attempting to break into your network. Running on its native Windows platform, Shadow Security Scanner also scans servers built on other platforms. It is able to reveal vulnerabilities in Unix, Linux, FreeBSD, OpenBSD, Net BSD, Solaris and, of course, Windows 95/98/ME/NT/2000/XP/.NET. Shadow Security Scanner might be the only security scanner able to detect faults with CISCO, HP, and other network equipment. Because of a fully open (ActiveX-based) architecture any professional with knowledge of VC++, C++ Builder or Delphi may easily expand the capabilities of the Scanner. ActiveX technology also enables the system administrators to integrate Shadow Security Scanner into practically any ActiveX supporting product. As network vulnerability assessment scanner provides a direct access to its core, you may use the API to gain full control of Shadow Security Scanner or to change its properties and functions. The Rules and Settings Editor will be essential for the users willing only to scan the desired ports and services without wasting time and resources on scanning other services. Flexible tuning lets system administrators manage scanning depth and other options and benefit from speed-optimized network scanning without any loss in quality. To improve the overall speed, the authors have added a simultaneous multiple network scanning function (up to 10 hosts per session). Another advantage of the Shadow Security Scanner is the way it saves detailed scan session log not only in traditional HTML format (which is available in 99% other scanners) but also in XML, PDF, RTF and CHM (compiled HTML) formats. The new interface is easy to use and it has been optimized to provide a better access to program's main functions. Managing Shadow Security Scanner options is also simplified: the most important elements of the program interface have bubble help windows with a brief description of how they work. The Update Wizard provides the timely updates of program's executive modules with the most up-to-date security information. *Its value is adequate to its functions. For the purpose for which we use it for internal testing its well worth its value. Its a network security/vulnerability scanner with many testing capabilities. Shadow Security Scanner is easy for staff to understand without much technical knowledge. Fairly robust in its testing ability.*



Retina Network Security Scanner by eEye Digital Security

This scanner is recognized as the industry standard for vulnerability assessment, identifies known network security vulnerabilities and assists in prioritizing threats for remediation. It is believed to work promptly, accurately and scan in a non-intrusive manner. It finds even the most recent discovered holes in security systems. Users can also leverage Retina for security risk assessment, project risk management and enforcing standards-based registry settings through custom policy audits. As the majority of Retina scans can be conducted without administrator rights, Retina is said to be the easiest scanner to use, and the most cost-effective to deploy. Retina leverages the expertise of eEye's Security Research Team, emplying the most comprehensive and up-to-date vulnerabilities database and scanning technology. These are automatically downloaded at the beginning of each Retina session. This enables network security professionals to proactively secure their networks against vulnerabilities. For those organizations looking to enforce the overall security of their remote access deployments, eEye offers



implemented version Retina Scan on Connect auditing systems attempting to access the network via SSL/VPN's. Retina Network Security Scanner identifies known network security vulnerabilities and assists in prioritizing threats for remediation. The users' comments are positive: *It's a very powerfull easy to use vulnerabillty, scanner.My preference is based on the fact that it's vulnerabillty database is updated regularly.Furthermore it's allround,so you don't necessarily have to buy multiple products in order to conduct a pentest. You can select multiple scanning profiles,eg: SANS top 20 UNIX,SANS top 20 windows,upto everything thats in the internal database.Another advantage is the build in report generator.Once the test has been completed you can make an atractive and professional report straight ahead and print it out. Another advantage is the opportunity to let the scanner correct registry issues it has found.The company is all in all very satisfied.* Retina is most frequently described as an excellent but too expensive device. Our readers consider this product as capable of making scripts in it.

GFI LANguard Network Security Scanner (N.S.S.)

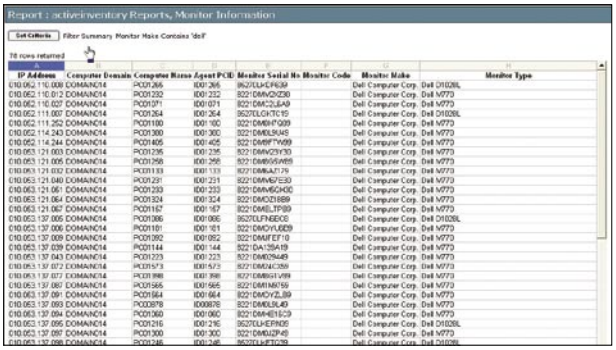
GFI LANguard Network Security Scanner (N.S.S.) is thought to be a leading network security scanning tool on the market. It provides full patch management ensuring most of the latest Microsoft patches and updates are deployed throughout your network. This scanner checks for and deploy missing security patches and service packs in OS and Office. It is said to employ very fast TCP & UDP port scanning and identification. Another advantage of GFI LANguard Network Security Scanner is the fact that it alerts pinpoint security issues and recommends the solutions. It automatically detects even the newest security holes with scheduled scan results comparisons and checks anti-virus and anti-spyware tools to ensure latest definitions are installed on your computer. Very useful addition is a wireless node/link detection and possibility of USB device scanning. The users indicate that its effectiveness lies in the close integration with the patch management process, and in the overall simplicity. In some ratings it received 5 out of 5 points in others – 3/5. People say that it might be called the best Windows security scanner with very complex and prompt updates. GFI is advisable for small-medium size enterprises. A frequently prized aspect of the scanner is the way it provides a wide range of details and information scans open ports. Some users use it to monitor machines, add files to specific units remotely and are satisfied.

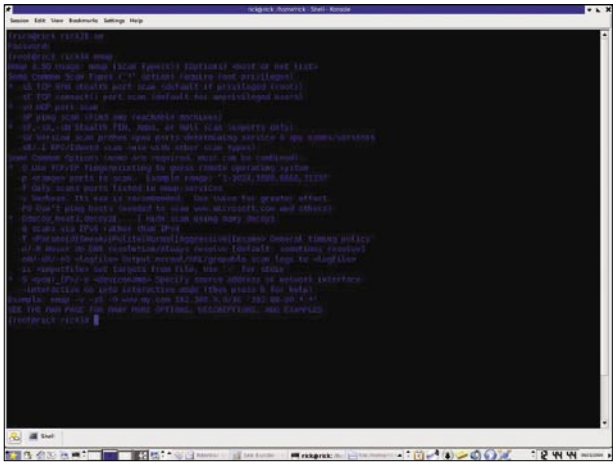
However there were negative opinions as well, claimed that it is good for beginners, and makes a huge amount of mistakes. *There is no possibility to scan a remote host outside your network.The scanning performance is a bit below average.More important Languard doesn't find the majority of deliberate introduced weak spots.I have deliberately left some machines unpatched and altered the firewall settings in order to be sure what the scanner can do in an ideal situation.This way I knew what the scanner should come up with. Approximately 80 % was found.*

Acunetix Web Vulnerability Scanner

Acunetix WVS automatically checks your Web applications for SQL Injection, XSS and other web vulnerabilities. Thanks to WVS you can check password strength on authentication pages (HTTP or HTML forms) Scans Javascript / AJAX applications for security vulnerabilities In users opinion it is a good choice: *So far we had been doing manual scans, and this is saving us so much time. The tool has already proven it's worth to us. We did not expect it to be so complete, it can run several types of security tests, leaving nothing out. And also has an integrated report tool. It's in accordance with my expectations and even more. The most important advantages are: time saving due to automated testing, complete set of tests (types), internal report tool, compare scan results and lots of more. Minus - it can take quite some time (several hours) to run a full scan on a complicated site. You need to take this into account when using a PC. This product is very effective into Web application scanning: information gathering (including email address that can be use for social engineering or for sending specially crafted nasty emails to the target), cross-site scripting, SQL injection, Google Hacking DataBase. It's definitely in accordance with my expectations.*

Advantages: simple to use. Includes an HTTP sniffer/editor to study/replay requests, a HTTP fuzzer, and a vulnerability editor. However there is no possibility to





stop a scan and resume it later. The number of vulnerabilities reported is the number of pages found to be vulnerable to a particuliar problem but there is not aggregation (for example a XSS vulnerability can be reported to be present on 50 pages, thus giving 50 vulnerabilities despite it is only one problem).

Nmap (Network Mapper)

Nmap is an open source utility to explore the network and to audit the security tools. It scans large networks (even those consisting of hundreds of thousands of machines, claims one of the users) quite rapidly, although it works fine against single hosts. The users like the fact that Nmap uses raw IP packets to find out what hosts are available on the network, which application those hosts are offering and what operating systems (and what versions) they are running. It is able, state some of the readers, to indicate what type of packet filters and firewalls are in use. Nmap runs on most types of computers and both console and graphical versions are available. What is very important and what is most frequently prized by the users – Nmap is free!

The scanner can be run to support most operating systems: Linux, Windows, FreeBSD, OpenBSD, Solaris, IRIX, Mac OS X, HP-UX, NetBSD, Sun OS, Amiga. Nmap offers many advanced features for power users. You can start out as simply as *nmap -v- Atargethost*. Both - command line and graphical (GUI) are available to suit user's preference. Those who do not wish to compile Nmap from source can always use the binaries. Although it is not so easy to run, Nmap has good, up-to-date man pages and tutorials in many languages. The disadvantage noticed by the users is the fact that the scanner comes with no warranty.

The swiss army knife of network surveilance.What can i say,it should be in every networking professionals toolbox.Advantage is the prize,its free open source.Yet a very powerfull tool to gain more knowledge about the target.You have two versions,one for the command prompt and NmapFE as GUI interface.Drawback is the lack of an suitable report generator,although mostly one will use Nessus and Nmap together.

Free tool Nmap: the one I will always use and trust, most reliable for discovering and fingerpritng, the fastest one too. The main purpose of the tool to discover, to identify open ports or fingerprint services.

Nmap has won *Information Security Product of the Year* award by Linux Journal, Info World and Codetalker Digest. Ratings show that Nmap is among the top ten (out of 30,000) programs at the *Freshmeat.Net* repository.

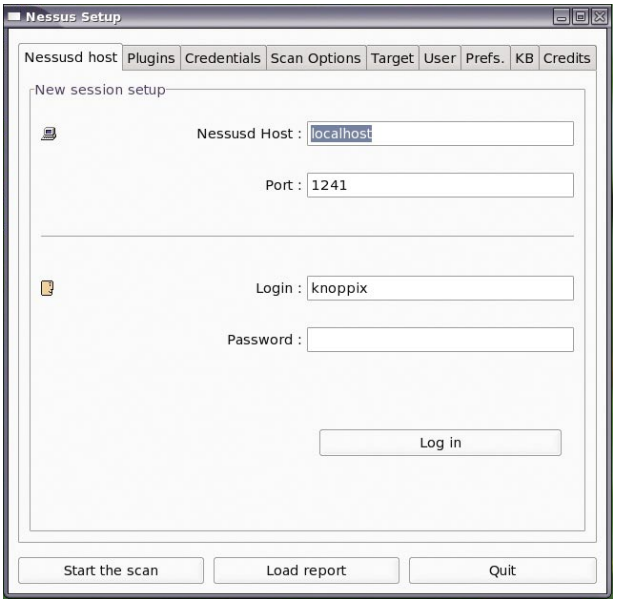
The result of an Nmap run is a list of scanned targets with some more information on each of them (depending on the options used), which is quite useful according to our testers. In addition to the interesting ports table, Nmap can provide further details on targets, including reverse DNS names, operating system guesses, device types, and MAC addresses.

Nessus Vulnerability Scanner

One of the most popular scanners in the world, endorset by professional information security organizations like SANS Institute. It focuses mainly on uptading security database on a daily basis and all the newest checks are available (one required credentials to log in and check a system loccally, the other has the ability to detect the remote flaws of the host on the Network). It's suitable for a single CPU with low memory as well as CUP with exra large gigabytes of RAM.

The Nessus Scanner includes NASL (Network Attack Scripting Language), desinged for writing security test in an easy manner. Other Features are: smart service recognition, multiplies services, full SSL support and non destructive security audit. Most of the time I prefer to use Nessus besides Retina.Great advantage is the cost of ownership,pratically zero.The program is Open Source which means free as in beer. Furthermore another plus is the modules are being updated frequently and you can easily write some custom modules yourself with libnasl.There are numerous of options such as IDS evation techniques,bruteforcing, Nmap works together with Nessus. Disadvantage is maybe the attack database is not as current as the Eeye Retina security scanner. But than again the program is professional enough, and free. Another disadvantage is the somewhat arcane GUI and lack of an prefessional report generator. Like Eeye Retina you can choose to actually attack an host and if you desire bring a host on its knees,given the use of the right modules.I choosed this scanner because it's free and still powerfull just as Retina.

Nessus has very user friendly interface and explanation of any vulnerability he thinks he has found. Has a huge vulnerability DB, but it has a quite big number of false positives, so using this tool we should test every-



thing he claims he has found. I would choose this product for checking services I have found with NMAP.

SecureCentral ScanFi

ScanFi is a web-based vulnerability assessment scanner for detecting and analyzing network holes and threats across various networks. ScanFi finds, scans, reports and supports vulnerability remediation. It features both scheduled and on-demand vulnerability scanning capabilities, based on a vulnerability database composed from multiple sources and vendors that is constantly kept up-to-date. Being a web-based software, just a browser is needed to connect to ScanFi, perform a scan and view the reports. ScanFi can be installed and run on both Windows and Linux operating systems, offering the freedom to allocate machines based on availability in a resource-constrained environment.

The authors emphasize that the scanner is equipped with SecureCentral ScanFi, an automated vulnerability management software. It detects, assesses and remediate network insecurities across the networks comprising servers, workstations, laptops, routers, switches, etc. Those who have used the device point out that the scaner identifies network devices that are open to known vulnerabilities and scans the network in non – intrusive way. It is said that the inventory of the network assets as well as the reports of the scan and remediation solutions(with references to corresponding CVE, Bugtraq and other repositories) are quite detailed and useful.

Another advantages highlighted by the users are advanced scheduling capabilities and comprehensive vulnerability knowledge base. Most of the users liked the fact that ScanFi assets all the software that has been currently installed on a Windows system as well as discovers and lists the inventory of different hardware components present in a system like Computer details - what brand it is, model, bios name, CPU details, Drives associated to this system, Peripherals that are connected to this system like Keyboard, Mouse, Monitor, Video/Sound Cards, USBs, Network information - IP address, MAC address, NIC

name, DNS server etc. and Port details - port type and status. The device described is believed to be practical also because it deploys missing patches and service packs for non-English Windows systems like German, Spanish, Japanese, Chinese, Portuguese, French, Italian and others. Our readers point out that ScanFi can be installed and run on both Windows and Linux (RedHat & Debian) operating systems.

NetworActiv Port Scanner 4.0

NetworkActiv Port Scanner is a network exploration and administration tool that allows you to scan and search internal LANs and external WANs. The user can choose many operating modes. The scanner may be used by experienced network administrators as well as by novices admit the readers. NetworkActiv Port Scanner provides all the basic features that most of the network scanners have, but it is also equipped with some additional features and technologies. This device consists of TCP connect() port scanner (standard TCP port scanner), TCP SYN port scanner (auxiliary TCP port scanner), UDP port scanner with automatic speed control and UDP subnet port scanner along with TCP subnet port scanner, for finding Web servers and other servers.

Its advantage is a high performance trace-route and ability to make, often good guess about the operating system of a remote host. Some people prize the wizard that walks you through step-by-step to perform network scanning, traceroute. Some of you liked the ability to perform whois queries, user may either specify a whois server, or have the program attempt to determine a whois server automatically. Users may configure maximum speed by themselves and chose to have subnet port scanner, port scanner, Windows(c) clipboard, and other programs integrated.

The device can detect trojans on remote and local systems and find computers currently connected on the network. It also lists host responses on open TCP ports,state the users,which may be useful in determining the type of FTP servers running, operating systems, etc. All features are integrated into one interface, which allows for fast action when you find a computer on a network, an open port, etc.

hakin9 editors do not take responsibility of the reviews content

Table 1a. *General security scanners chart*

Manufacturer	Model	Features	Prize US*	Rating
Safety-Lab	Shadow Security Scanner	• employs a unique system security analysis algorithm based on a patented *intellectual core*, • scans servers built practically on any non- Windows platform, • able to detect faults with CISCO, HP, • capable of tracking more than 4,000 audits per system, • the only scanner to audit proxy servers (other scanners just verify ports availability), • any professional with knowledge of VC++, C++ Builder or Delphi may easily expand its capabilities, • provides a direct access to its core • wizard guiding through the process of new audit creation, • the function of simultaneous multiple network scanning (up to 10 hosts per session).	From $499	★★★★☆
eEye	Retina	• nables to create custom audits, including application version control, permissible ports, P2P and enabling regulatory compliance requirements, • comprehensive Vulnerability Database, based on the award-winning Retina Network Security Scanner, • scan on Connect can be configured to ensure devices connecting to the network have the Blink Unified Client Security agent installed, • administrators can ensure vulnerability protection of their networks by employing the REM Security Management Console, adding greater capabilities to identify and quantify risk.	From $945	★★★★★
Nessus	Nessus Vulnerability Scanner	• able to detect the remote flaws of the hosts on the network, • it can scale down to a single CPU computer with low memory to a quad-CPUs monster with gigabytes of RAM, • each security test is written as an external plugin, written in NASL, • It recognizes a FTP server running on a non-standard port, or a web server, • if a host runs the same service twice or more, it will test all of them, • has the ability to test SSLized services such as https, smtps, imaps, • gives the choice between performing a regular non-destructive security audit, or to throw everything at a remote host.	Free	★★★★☆
GFI	LANguard Network Security Scanner	• fast TCP & UDP port scanning & identification, • alerts pinpoint security issues & recommends action, • automatically detect NEW security holes with scheduled scan results comparisons, • checks anti-virus and anti-spyware to ensure latest definitions are installed, • wireless node/link detection and USB device scanning.	From $495	★★★☆☆

** hakin9 editors do not take responsibility of the prize changes*

Table 1b. *General security scanners chart*

Manufacturer	Model	Features	Prize US*	Rating
Nmap	Nmap	• supports many techniques for mapping out networks filled with IP filters, firewalls, routers, and other obstacles, • used to scan huge networks of hundreds of thousands of machines, • supports most operating systems, including Linux, Microsoft Windows, FreeBSD, OpenBSD, Solaris, IRIX, Mac OS X, HP-UX, • easy to start out, • available for free, comes with full source code that you may modify, • comprehensive and up-to-date man pages & tutorials; • has won numerous awards, including *Information Security Product of the Year.*	Free	★★★★★
AdventNet	SecureCentral ScanFi	• web-based vulnerability management, • asset discovery, • vulnerability remediation with international language patching, • intelligent service detection, • hardware & software inventory, • asset & vulnerability groups, • non-intrusive scanning, • advanced scheduling capabilities, • comprehensive vulnerability knowledge base, • template based vulnerability reports generation, • cross-platform product installation.	From $495	★★★☆☆
NetworkActiv	Port Scanner 4.0	• UDP port scanner with automatic speed control, • UDP subnet port scanner, • ping scanning of subnets (UDP or ICMP), • high performance trace-route, • remote OS detection, • wizard Walks you through to perform network scanning, • able to perform whois queries, • graphical user interface, with skin support, • able to notify user if remote computer being scanned is stealth, • user configurable maximum speed, • saves the results of the port scanner, subnet port scanner, and other lists to text files.	Free	★★★☆☆
Acunetix	Web Vulnerability Scanner	• automatically checks for SQL injection & Cross site scripting vulnerabilities, • checks password strength on authentication pages (HTTP or HTML forms), • scans Javascript / AJAX applications for security vulnerabilities, • automatically audits shopping carts, forms, dynamic content and other web applications, • creates professional website security audit reports, • determines if dangerous HTTP methods are enabled on the web server and inspects the HTTP version banners for vulnerable products	From $399	★★★★☆

** hakin9 editors do not take responsibility of the prize changes*