OPEN ACCESS Freely available online

International Journal of Advancements in Technology

Research Article

Examination of Vulnerability Scanning Technologies

A Subhangani*, B Anita Chaudhary

Department of Engineering, Dronacharya College of Engineering, Gurgaon, Haryana, India

ABSTRACT

The commercial value of web applications has significantly increased in recent years. They progressed from simple information-sharing platforms to more sophisticated business applications. Web-based apps, unlike most other technologies, are always accessible from anywhere in the world. This makes them ideal targets for malevolent cyberattacks. Scanners can identify and mitigate an organization's vulnerabilities. However, without a thorough awareness of a system's weaknesses, it would be difficult to undertake effective network defense in order to keep intruders out in the real world. As a result, vulnerability scanning is an important part of a cybersecurity curriculum's success. In this paper, we look at the present state of open-source vulnerability scanning technologies. A literature review of vulnerability assessment and reporting, vulnerability scanning, vulnerability scanning technologies, security vulnerabilities, system and application security, and malicious cyber- attacks reveals that a lot of work is being done in this area. This research provides an in-depth examination of vulnerability scanning technologies. In this paper, we covered two important topics: vulnerability scanning and reporting. Then, after identifying gaps in relevant practices and presenting chosen findings, we emphasize future directions and bring this study to a conclusion. The top open-source network vulnerability scanning tools are described in detail.

Keywords: Vulnerability assessment; Vulnerability; Security; Threat

INTRODUCTION

The advent of information technology, user security has become a more important consideration. Because most software developers are unaware of the various security measures that should be implemented because their primary goal is to make the software application run in the desired state without considering the flaws that the programming language may have introduced into the system, it becomes increasingly important to devise new strategies and methodologies that will protect users from being attacked by any unauthorized access. Not only does software with defects leave the user exposed to attacks, but the network is frequently a crucial role in jeopardizing the users' security [1].

Assessing and removing vulnerabilities necessitates a thorough knowledge and comprehension of these flaws. It becomes necessary to understand the basic concept behind these vulnerabilities, such as what causes them to appear in the system, what flaws need to be fixed to make the system free of these vulnerabilities, and what alternatives can be devised for these vulnerabilities in the future to reduce their risk, and so on. Various methods have been used to identify these flaws, and necessary measures have been adopted. Static analysis, attack graph generation and analysis, and vulnerability scanner use are only a few of them. Vulnerability scanners, on the other hand, are widely used today to find flaws. They are very important in the construction of attack graphs.

METHODOLOGY

Vulnerability scanner

A vulnerability scanner is a computer program that scans computers, networks, and applications for known vulnerabilities. To put it another way, these scanners are utilized to find the flaws in a system. They are used to identify and discover vulnerabilities in network-based assets such as firewalls, routers, web servers, application servers, and so on that arise from misconfigurations or defective programming. They're usually available as SaaS (Software as a Service), which means they're supplied as a web application *via* the internet. In order to generate a more thorough image of the system, most vulnerability scanners will attempt to log in to computers using default or other credentials [2]. Following the creation of an inventory, the vulnerability scanner compares each item in the

Correspondence to: Subhangani A, Department of Engineering, Dronacharya College of Engineering, Gurgaon, Haryana, India, Tel: 91-9891729455; E-mail: subhangani726@ gmail.com

Received: 20-Jun-2022, Manuscript No. IJOAT-22-18514; **Editor assigned:** 24-Jun-2022, Pre QC No. IJOAT-22-18514 (PQ); **Reviewed:** 08-Jul- 2022, QC No. IJOAT-22-18514; **Revised:** 15-Jul-2022, Manuscript No. IJOAT-22-18514 (R); **Published:** 22-Jul-2022. DOI:10.35248/0976-4860-22.13.197.

Citation: Subhangani A, Chaudhary BA (2022) Examination of Vulnerability Scanning Technologies. Int J Adv Technol. 13:197.

Copyright: © 2022 Subhangani A, et al. This is an open-access article distributed under the terms of the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

inventory to one or more databases of known vulnerabilities to see if any of the objects are vulnerable. A systems vulnerability analysis is produced as a result of such a scan, revealing any known vulnerabilities that may require threat and vulnerability management (Figure 1).

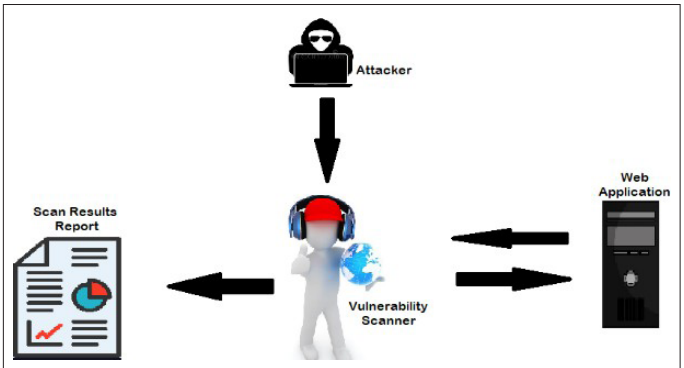

Figure 1: Vulnerability scanning system diagram.

Vulnerability assessment, also known as Vulnerability testing, is vulnerability scanning software used to assess security risks in software systems in order to lessen the likelihood of a security breach (Table 1). It is the process of defining, identifying, classifying, and prioritizing vulnerabilities in computer systems, applications, and network infrastructures. Vulnerability assessments also provide organizations with the information, awareness, and risk backgrounds they need to recognize and respond to threats to their environment [3].

Table 1: Risk level and their cvss range.

Risk level	CVSS range	Examples
Critical	10	SQL injection, remote code execution, and command injections
High	7-9	Memory corruption, distributed/denial of service, directory traversal
Medium	4-6	Cryptographic protocol, command injection
Low	1-3	Internal information disclosure, browsable web directory
Informational	0	Software version disclosure

The goal of a vulnerability assessment is to identify threats and the risks they entail. They usually entail the use of automated testing tools like network security scanners, the results of which are documented in a vulnerability assessment report. Vulnerability assessments can assist organizations of any size, as well as people who are in danger of cyber assaults, but vulnerability analysis will benefit major enterprises and other types of organizations that are vulnerable to continual attacks the most.

Because security flaws can allow hackers to get access to IT systems and apps, it's critical for businesses to identify and fix flaws before they're exploited. Companies can improve the security of their systems by conducting a full vulnerability assessment and implementing a management program. Vulnerability Assessment and Penetration Testing (VAPT) are two approaches that are used in vulnerability analysis, vulnerability evaluations are crucial (Figure 2).

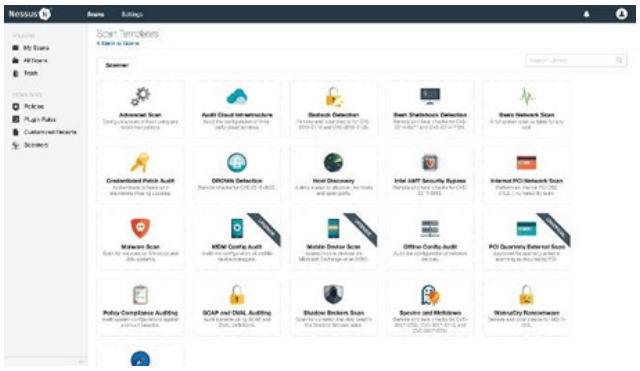

Figure 2: Nessus professional: Vulnerability assessment solution.

A vulnerability assessment gives information on any security flaws in an organization's environment. It also instructs on how to evaluate the hazards connected with certain flaws. This method gives the company a greater awareness of its assets, security issues, and overall risk, lowering the chances of a cybercriminal breaking into its systems and catching the company off guard [4].

Types of a vulnerability scanner

Host-based: Identifies problems with the host or system. The process is completed by using host-based scanners to identify and diagnose vulnerabilities. The host-based tools will install a mediator program on the target machine, which will track the occurrence and alert the security analyst (Table 2).

Table 2: Comparison between nexpose and nessus pricing.

Insight VM	Nessus
$22/Asset	1 Year- $3,390.001 License with one-time purchase
-	$3790 1 Year+Advanced support
-	2 Years- $6,610.501 License
-	$7,030 2 Years+Advanced support
-	3 Years- $9,661.501 License
Free trial	Free trial

Network-based: It will discover open ports and identify any unfamiliar services that are using them. It will then reveal any potential vulnerabilities linked with these services. Network-based scanners are used in this process (Figure 3).

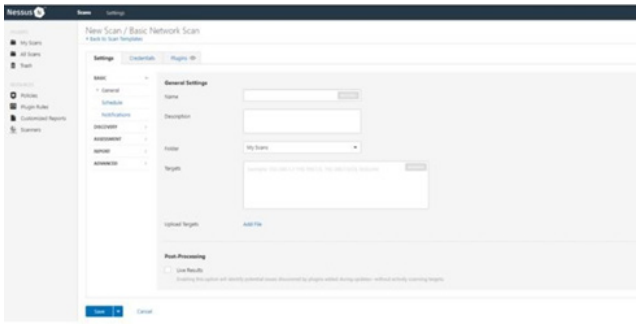

Figure 3: Basic network scan page.

Database-based: It will use tools and techniques to uncover security vulnerabilities in database systems and prevent SQL Injections. (SQL Injections: Malicious users inject SQL statements into a database, allowing them to read sensitive data from the database and edit the data in the database).

Wireless network scans of an organization's Wi-Fi networks frequently concentrate on potential sites of attack in the infrastructure. A wireless network scan can confirm that a company's network is safely configured in addition to discovering rogue access points (Table 3).

Table 3: Owasp top 5 vulnerabilities and preventions.

Vulnerabilities	Vulnerabilities description	Preventive measures
Injection	When an attacker submits untrusted data to an interpreter, injection problems such as SQL injection, CRLF injection, and LDAP injection occur.	Injection issues are easily detected *via* application security testing. When coding, developers should use parameterized queries.
Broken authentication	Attackers could compromise passwords, keys, or session tokens, or take control of users' accounts to assume their identities if user and session authentication is implemented incorrectly.	Multi-factor authentication
Sensitive data exposure	Because applications fail to safeguard sensitive data such as financial information, usernames, and passwords, attackers may be able to gain access to such information and perpetrate fraud.	Data encryption in transit and at rest can assist you in complying with data protection rules.
XML External Entities (XXE)	External entity references in xml documents are evaluated by poorly configured xml processors. External entities can be used by attackers.	By evaluating dependencies and configuration, Static Application Security Testing (SAST) can detect this problem.
Broken access control	Authenticated users with improperly configured or absent restrictions can access unauthorized functionality or data, such as accessing other users' accounts or seeing sensitive documents.	Other testing methods only detect when access controls are lacking; penetration testing is required to detect non-functional access restrictions.

Application scans examine websites for known software flaws and inappropriate network or web application setups. Vulnerability scanners are software that scans a network's design, reports flaws, and gives recommendations on how to fix them. Vulnerability scanners provide information on Common Vulnerabilities and Exposures (CVE), which is a set of standardized names for known vulnerabilities with a risk classification system known as the Common Vulnerability Scoring System (CVSS). The National Vulnerability Database's CVSS scores include factors such as attack vector, complexity, required privileges, user involvement, and the impact of confidentiality, integrity, and availability. Vulnerability scanning is an examination of a computer's or network's potential points of exploit in order to find security weaknesses (Figure 4).

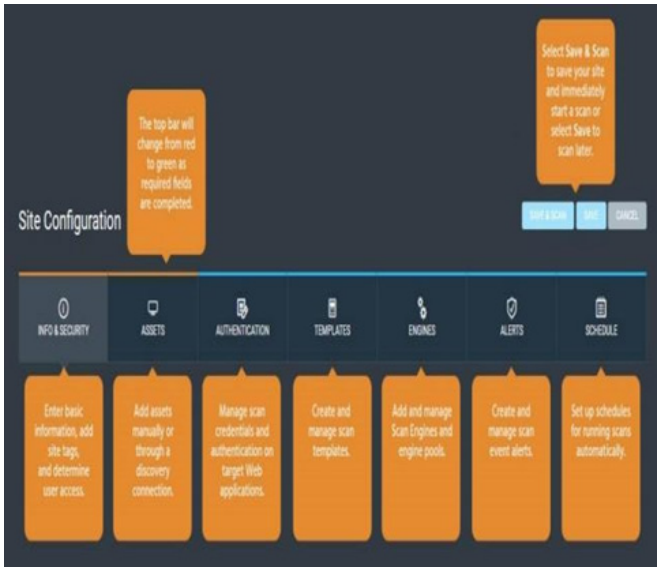

Figure 4: Scanning targeted website.

A security scan identifies and analyses system flaws in computers, networks, and communications equipment, as well as predicts how successful countermeasures will be. An organization's IT department or a security service provider may conduct a scan, maybe as a condition imposed by some authority. Attackers who are looking for points of entry also utilize vulnerability scanning [5].

A vulnerability scanner runs from the person assessing the attack surface in question to the end point of the scanner. Details about the targeted attack surface are compared to a database of known security weaknesses in services and ports, packet building

irregularities, and potential paths to exploitable programs or scripts. Each found vulnerability is attempted to be exploited by the scanner program.

Running a vulnerability scan has its own set of hazards because it is inherently intrusive to the running code on the target system. As a result, the scan may result in errors and reboots, lowering productivity [6].

What factors should consider while selecting a vulnerability scanning tool-

When looking into vulnerability scanners, find out how they rank in terms of accuracy, as well as dependability, scalability, and reporting. If the scanner's accuracy isn't up to par, then have to run two separate scans in the hopes of finding vulnerabilities that the other overlooks. Scanning becomes more expensive and time-consuming as a result of this (Figure 5).

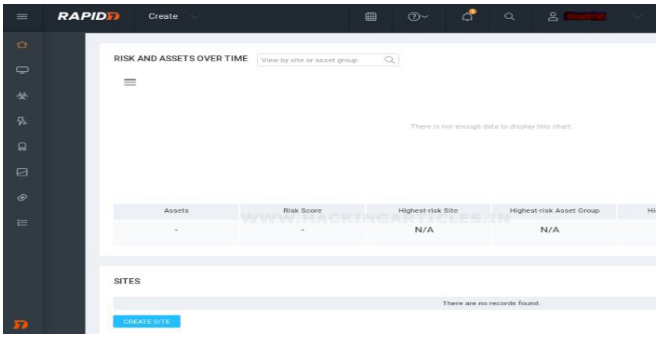

Figure 5: Nexpose console.

RESULTS AND DISCUSSION

Vulnerability scanners that are based on software include configuration auditing, target profiling, penetration testing, and extensive vulnerability analysis are common features of these scanning programs. They operate with Microsoft system center and other Windows products to enable intelligent patch management, and some even work with mobile device managers. They can scan virtual machines, BYOD mobile devices, and databases in addition to traditional network devices, servers, and workstations [7].

Continuous, On-demand monitoring using cloud-based Vulnerability Scanners Software as a Service (SaaS) is a newer sort of vulnerability scanner that is given on-demand (SaaS). On-demand scanners, like software-based scanners, include links for downloading vendor fixes and updates for discovered vulnerabilities, which cuts down on remediation time. Scanning thresholds are also included in these services to prevent devices from becoming overloaded during the scanning process, which might cause them to crash (Figure 6).

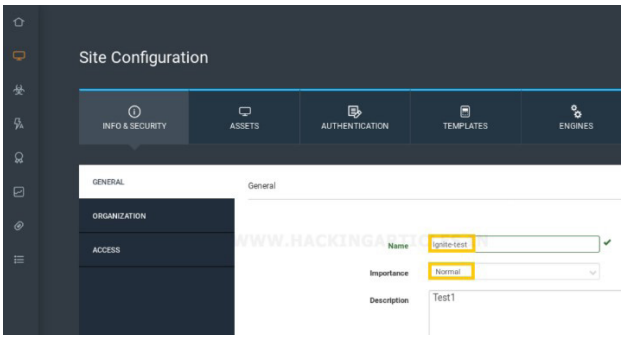

Figure 6: Scanning site configuration.

Top vulnerability scanning tools

Vulnerability scanners employ a continually updated list of databases to find and classify flaws so that their solutions can be prioritized. Some vulnerability scanners even go so far as to automatically patch the flaw, relieving security professionals and developers of the task.

Nessus: Tenable Nessus runs lightning-fast, in-depth scans to find vulnerabilities before they are discovered by an attacker. The solution takes a risk-based approach to identify and assess vulnerabilities. As a result, it gives threat levels to each found vulnerability based on how serious or minor the threat is to the security of your system. With over two million downloads worldwide, Nessus is one of the most popular vulnerability scanners. Nessus also offers thorough coverage, with over 59,000 CVEs scanned [8].

Nexpose: Nexpose by Rapid7 captures data in real-time to provide a continuous view of an organization's changing network. Because the CVSS risk score scale is 1-10, this vulnerability scanner created its own 1-1000 risk score scale to add more detail. It also determines vulnerability age, vulnerability proof, vulnerability solution, and public exploits/malware kits.

Nmap: Nmap is a free, open-source security scanner that is also used by businesses for network discovery, inventory, service upgrade schedule management, and host or service uptime monitoring. Nmap is popular because of its versatility, capacity, portability, and ease of use. Nmap is a versatile tool since it can map a network with packet filters, firewalls, routers, and other barriers. Nmap can be used to scan a network as large as thousands of computer hosts or as tiny as a single host. Nmap is portable since it runs on Linux, Microsoft Windows, and so on. Nmap is included in several operating systems, including BT5 and Kali Linux [9].

OpenVAS: Greenbone networks maintains openVAS, an open-source vulnerability scanner. The scanner also features a community feed with over 50,000 vulnerability testing that is updated on a regular basis. OpenVAS isn't the most user-friendly

scanner, but it's one of the most capable security scanners available for free. It can scan tens of thousands of vulnerabilities and manages false-positive findings.

Stages of vulnerability assessment

Identify the scope of the project-

1. Servers, network devices, printers, IoT, workstations, databases, applications. Get approval, plan for the assessment.

2. Information gathering (ServiceNow, Subnets, etc)

3. Vulnerability scanning-nessus, Nexpose, Qualys, etc.

4. Data analysis/False positive/Exceptions review.

5. Report generation.

Experiment with nessus and nexpose tools-

For this research, I chose nessus and nexpose as my tools. I looked at nessus and nexpose because they are both excellent tools for scanning IT infrastructure.

Nessus: Nessus is a remote security scanning application that examines a computer and alerts you if it finds any vulnerabilities that malevolent hackers could exploit to obtain access to any computer on your network. It accomplishes this by doing over 1200 checks on a specific machine, determining whether any of these assaults could be used to break into or harm the computer. Nessus by tenable network security it is more than a scanner; it is an integrated platform that delivers the most comprehensive coverage for vulnerability management and configuration verification, CVE plugins and updates, SCADA checks with a range of UNIX and linux, and regulations compliance all under the same license [10].

Who would utilize such a device-

If you're the authority of a computer (or a collection of computers) that's linked to the internet, Nessus is an excellent tool to use to keep your domains safe from the common vulnerabilities that hackers and viruses seek.

Exactly what Nessus isn't- Nessus isn't a full-fledged security solution; rather, it's an important component of a well-rounded security approach. Nessus is a tool that scans your systems for weaknesses that hackers could use. It does not actively prevent attacks. The system administrator is responsible for patching these vulnerabilities and creating remediation.

Factors at work- Nessus does not make assumptions about your server setup which can lead to serious vulnerabilities being missed. Nessus is incredibly expandable, with a scripting language that allows you to develop tests that are specific to your system once you've gotten to know the tool. It also has a plug-in interface, and the Nessus plug-in site has a large number of free plug-ins. These plugs are frequently designed to identify a specific infection or vulnerability.

New vulnerabilities and exploits are constantly being discovered. The Nessus team updates the list of vulnerabilities to look for on a regular basis in order to reduce the time between when an exploit is discovered in the wild and when you may detect it with Nessus.

It's free and open-source. Nessus is free and open-source, which means you, can look at and edit the code as you see fit. When Nessus identifies vulnerability, it will almost always be able to propose the best method to mitigate it.

How does it work

Installation: Visit get the latest recent release of Nessus and go to www.nessus.org. On the Unix-based PC, this will install the Nessus server software as well as a client.

Running a scan: To execute a scan, first, start up a Nessus server on some machine, then start up a Nessus client. After you've installed and run nessus, may begin scanning. To begin, go to the top navigation bar and select scan. Then on the My Scans page, click the new scan button.

After that, select the scan template. Scan templates make the process easier by deciding which settings can be changed and how they can be changed. Configure the settings in the Basic Settings section: The name of the scan or policy is specified here. On the Nessus interface, this value is displayed. One or more targets to be scanned are specified. You are not required to provide extra targets if you choose a target group or upload a target file.

Credentials can be configured for a scan as an option. This permits certified scans to run, which can provide far more detailed information and a more thorough assessment of your environment's vulnerabilities. Alternatively, you can save the scan and run it later, or you can run it now.

Viewing scan findings might assist you in gaining a better understanding of your company's security posture and weaknesses. You may customize how you view your scan's results using color-coded indicators and customized viewing choices.

Nexpose: Nexpose security control provides access to manage hosts, scan profiles, reports, licenses, and dashboards implemented in sites. It includes a built-in Postgres SQL database that stores scan templates, policies, and scan results, among other things. The web browser can be used to interface with nexpose. Except for the free nexpose community version, all of the nexpose editions are purchased. Nexpose detects active services on the machine, such as open ports, services, and running applications. Nexpose prioritizes the most serious threats based on threat intelligence that is matched with the company's priorities. Focusing remediation efforts on the most effective activities can help decrease risk with the least amount of effort and keep the IT team on track.

Rapid7's NeXpose is available in four different versions, each with its own set of features and benefits that expand as we obtain more licenses. First, it has the "Community Edition" free edition, which can be used for seven days for free to scan up to

a predetermined number of IPs. The "Express" edition is next, followed by the "Express Pro" edition, and lastly the "Enterprise" edition. All of them propose their proposals at annual fees ranging from USD $ 2,000 to USD $ 25,000.

Factors at work

Nexpose finds assets and scans for vulnerabilities within an organization's mobile, virtual, physical, and cloud contexts then prioritizes risk based on the exploitability of those vulnerabilities. It also prioritizes vulnerability patching and scanning on a regular basis by allowing administrators to set security alarms.

Nexpose includes a unique feature of Live Monitoring that gathers all accessible data and translates it into action plans. The sophisticated exposure analytics function of nexpose finds and prioritizes vulnerabilities that are exploited first. As a result, security managers are spared from being overburdened by security notifications. The Liveaboards feature is used to replace the results of a static dashboard with dynamic visual reporting. Rapid 7 has released a new tool for nexpose called remediation workflow, which is used to track and manage an organization's security employees as well as analyze the progress of fixing vulnerabilities.

How does it work?

Downloading and installing nexpose: Nexpose Community Edition can be downloaded from the Rapid7 website. The Nexpose Security Web Console page will activate once logged in and accomplished all of the required activations, and able to run refer scan.

Running a scan: To begin a new scan, go to the home page, and select Site from the Create dropdown menu. The "Site Configuration" screen will appear in the Security Console.

As shown in the below image, give a name to the site and a description in the General tab. Its importance can be set anywhere between very low and very high.

Include and exclude are the two sections of the Assets configuration page. Provide the target IP address in the Include section, but if want to scan the entire network, provide the entire IP range. The IP address is excluded from scanning using the Exclude section. If scanning an entire IP range and want to exclude some IPs from the scan, it can be done by adding them to the exclude assets section. If need to add any credentials, it can be done in the Authentication section. Set up a specific Scan Template. The default Scan Template, which is a full Audit sans Web Spider. Now choose an engine for the scan i.e. Local Scan Engine. As gathered all of the necessary information to prepare the site for a scan. Click the Save and Scan button in the upper right corner of the Nexpose console panel to begin scanning. When the scan is finished, the result clearly shows the number of vulnerabilities found, the risk score, and the scan duration. Over the Vulnerabilities page, it can refer to the vulnerabilities stated, as well as their Common Vulnerability Scoring System (CVSS) score, which ranges from highest to lowest. The intriguing thing is that at least one of these exploits has been published in the Exploit database and is vulnerable to numerous Metasploit modules. When clicking on a specific vulnerability that is a critical threat, it displays information about the vulnerability, such as its severity, whether it is password protected or not, version, and so on.

Comparison of nessus and nexpose

Please find below the comparison of Nessus and Nexpose Features. Please find below the comparison of Nessus and Nexpose Pricing.

People have given Nexpose and Nessus vulnerability tools positive feedback. Check out this side-by-side comparison of InsightVM (Nexpose) *vs* Nessus based on user preference data. With 62 reviews, InsightVM (Nexpose) has a rating of 4.4/5 stars. Nessus, on the other hand, has 231 reviews and a rating of 4.4/5 stars. The score for each product is computed using real-time data from verified user reviews. Here's a quick rundown of what they said in their reviews.

Owasp top 5 vulnerabilities and preventions

The Open Web Application Security Project (OWASP) is a non-profit global online community that creates articles, documentation, tools, and technology on the subject of web application security. It has tens of thousands of members and hundreds of chapters.

CONCLUSION

Attackers have become bolder in their attempts to enter secure networks, and cyber-attacks are at an all-time high. They will be successful if their scans uncover weaknesses that can be exploited to their benefit. This is why all firms, regardless of size, need vulnerability scanners, preferably ones that run continuously and automatically. Both Nexpose and Nessus Professional are excellent tools for scanning IT infrastructure.

The results reveal that the number of security vulnerabilities detected by different technologies varies significantly. Comparing vulnerability scanners to anti- virus programs may be beneficial. Both are critical to security control and will improve a company's security posture. A vulnerability scanner, like anti-virus software, will not find all of the harmful stuff. Security experts prefer to utilize Nessus to audit IT systems. Nessus is the natural pick of the two for most organizations with the funding for an optimal vulnerability scanning experience. We hope to detail preventive maintenance schedules and well-known approaches to secure website owners in the future study. Each option has the potential to improve an organization's ability to fix discovered vulnerabilities and, as a result, contribute to a safer, more secure society.

REFERENCES

1. Harrell CR, Patton M, Chen H, Samtani S. Vulnerability assessment, remediation, and automated reporting: Case studies of higher education institutions. In 2018 IEEE International Conference on Intelligence and Security Informatics (ICSI). 2018;148-153.

2. Wang Y, Yang J. Ethical hacking and network defense: Choose your best network vulnerability scanning tool. In 2017 31st International Conference on Advanced Information Networking and Applications Workshops (WAINA). 2017;110-113.
3. Holm H, Sommestad T. Sved: Scanning, vulnerabilities, exploits and detection. In MILCOM 2016-2016 IEEE Military Communications Conference. 2016; 976-981.
4. Appiah V, Asante M, Nti IK, Nyarko-Boateng O. Survey of websites and web application security threats using vulnerability assessment. J Comput Sci. 2018.
5. Aarya PS, Rajan A, Sachin KP, Gopi R, Sreenu G. Web scanning: Existing techniques and future. In 2018 Second International Conference on Intelligent Computing and Control Systems (ICICCS). 2018;123-128.
6. Gorbenko A, Romanovsky A, Tarasyuk O, Biloborodov O. Experience report: Study of vulnerabilities of enterprise operating systems. In 2017 IEEE 28th International Symposium on Software Reliability Engineering (ISSRE). 2017;205-215.
7. Yadav, Ravinder, Goyal A. Web application security. Int J Comput Sci Mob Appl.2014:349-355.
8. Kushe R. Comparative study of vulnerability scanning tools: Nessus V.s retina. Security and Future. 2017;1(2):69-71.
9. Im SY, Shin SH, Ryu KY, Roh BH. Performance evaluation of network scanning tools with operation of firewall. In 2016 Eighth International Conference on Ubiquitous and Future Networks (ICUFN). 2016;876-881.
10. Stephenson P. Tenable network security nessus.2015.