IV. Vulnerability Tools

The main goal and objective of vulnerability scanning is to identify the potential threats before the hackers try to access the information. Network’s security can be maintained by conducting regular scans to have an up-to-date assessment and taking steady approach to enhance the cybersecurity. Moreover, vulnerability scanning helps you meet data protection standards and ensures data processing security. The scan generates a comprehensive report that outlines all system scans conducted and the vulnerabilities detected, each with a corresponding severity rating. Additionally, the report offers recommended measures to address the identified vulnerabilities.

Among the widely recognized network vulnerability scanners, Nessus stands out as a prominent option. It efficiently checks for software misconfigurations on a PC, identifies open ports, and determines the software versions running on the device. Nessus also looks for TCP/IP stack denial-of-service attacks, vulnerabilities that may allow unauthorized access or control of sensitive data by remote hackers, and facilitates PCI DSS assessments. Furthermore, it includes web application scanning, effectively detecting issues like SQL injection and cross-site scripting.

Another valuable tool for web application security evaluation is Acunetix. This automated solution scans web applications for exploitable vulnerabilities, such as SQL Injection and Cross-Site Scripting. Acunetix covers websites and web applications accessible via web browsers using the HTTP/HTTPS protocol. It excels in assessing both pre-made and custom web applications, including those implementing JavaScript, AJAX, and Web 2.0 web apps. Acunetix employs a smart crawler capable of discovering a wide range of files, ensuring comprehensive scanning and assessment of potential vulnerabilities.

|  |  |  |
| --- | --- | --- |
| Aspect | Nessus | Acunetix |
| Performance Speed | Well-known for its efficient performance in conducting network-wide vulnerability scans.  Scanning speed is slower. | Offers fast and effective scanning capabilities, specifically tailored for web application security evaluation.  Scanning speed is faster. |
| Execution | It employs an agent-based approach, allowing users to install agents on target systems for scanning. It also supports remote scanning of network hosts. | Follows an agentless approach, eliminating the need for installing agents on target systems. It offers remote scanning capabilities for web applications, simplifying the assessment process. |
| Coverage | Provides comprehensive scanning capabilities, enabling organizations to assess vulnerabilities across their entire network infrastructure, including hosts, servers, and network devices. | Focuses primarily on web application scanning. It excels in identifying vulnerabilities in web applications accessible through web browsers using the HTTP/HTTPS protocols. |
| Ideal for | Best suited for organizations seeking a robust solution for network-wide vulnerability assessment, making it ideal for evaluating security risks across a large-scale infrastructure. | Is the go-to tool for businesses and developers primarily concerned with securing their web applications against potential threats and vulnerabilities. It specializes in web application security evaluation. |
| Pricing | Is affordable where free options are also available. | Is too rigid and expensive. |
| Functionalities | Offers a wide array of functionalities, including vulnerability detection, reporting, and advanced scanning techniques like credentialed scanning for detailed assessment of hosts. It can identify vulnerabilities in various aspects of the network infrastructure. | Specializes in detecting vulnerabilities in web applications, such as SQL Injection, Cross-Site Scripting (XSS), and other security flaws that can be exploited by attackers. It provides a dedicated focus on web application security, ensuring comprehensive coverage in this domain. |
| Functions | Is known for its robust network scanning capabilities that extend to network devices, servers, and endpoints. It detects vulnerabilities, misconfigurations, and potential security risks within the network environment. | Excels in the identification of web application vulnerabilities that could be exploited by cyber attackers to compromise the application's security and sensitive data. It focuses on in-depth analysis of web application code and behavior. |
| Strengths | Offers a comprehensive solution for organizations with diverse network infrastructures, ensuring that security teams can gain insights into potential vulnerabilities across a wide range of devices and hosts. | Primary advantage lies in its specialized expertise in web application security. By focusing on web application vulnerabilities, it can provide in-depth insights and targeted recommendations for securing critical applications. |
| Technologies Used | Utilizes a variety of scanning techniques, including active and passive scanning methods, credentialed scanning for detailed host assessment, and various network vulnerability checks. | Leverages advanced web application scanning tools to thoroughly assess web applications, including JavaScript-heavy and Web 2.0 technologies. It employs a smart crawler to discover and evaluate web application files and parameters effectively. |
| Deployment | Provides the flexibility of deployment options. Users can choose between an on-premises installation or opt for Nessus Cloud, a cloud-based version hosted by Tenable. | Is deployed as a cloud-based solution, offering convenient access from anywhere with an internet connection. Users can efficiently manage and monitor their web application security assessments through the Acunetix cloud platform. |

Table V: Comparison of Vulnerability tools.

References:

1. Jai Narayan Goel, B.M. Mehtre, Vulnerability Assessment & Penetration Testing as a Cyber Defence Technology, Procedia Computer Science, Volume 57, 2015, Pages 710-715, ISSN 1877-0509, <https://doi.org/10.1016/j.procs.2015.07.458>.
2. Bairwa, Sheetal & Mewara, Bhawna & Gajrani, Jyoti. (2014). Vulnerability Scanners-A Proactive Approach To Assess Web Application Security. International Journal on Computational Science & Applications. 4. 10.5121/ijcsa.2014.4111
3. International Journal on Computational Sciences & Applications (IJCSA) Vol.4, No.1, February 2014

DOI:10.5121/ijcsa.2014.4111

1. Alazmi, Suliman & Leon, Daniel. (2022). A Systematic Literature Review on the Characteristics and Effectiveness of Web Application Vulnerability Scanners. IEEE Access. 10. 1-1. 10.1109/ACCESS.2022.3161522.