**VULNERABILITY TOOLS**

The primary objective of vulnerability scanning is to identify threats before a hacker can take advantage of them. Once a scan is performed, you may quickly conduct another one. You could have ongoing, up- to-date assurance about the security of your network in this way. Likewise, vulnerability scanning can help you in improving your cybersecurity in little steps. Furthermore, it can assist you in meeting data protection standards. Additionally, it can support data processing security. A vulnerability scan's report represents the outcome. Every system scan is reported. Additionally, it will report on all vulnerabilities discovered. Each vulnerability detected by vulnerability scanners is usually given a rating. The severity of the incident is indicated by the vulnerability rating. Plus, the scanner will propose ways to fix the vulnerability.

One of the most well-known network vulnerability scanners in the world is Nessus [7]. It enables software that was installed on the PC to be checked for misconfiguration. Additionally, it includes identifying the machine's open ports and the software version that is now running on the device. In addition, it scans for denial-of-service attacks against the TCP/IP stack, vulnerabilities that allow a remote hacker to take control of or access sensitive data on a system, and PCI DSS assessments. Web application scanning is also included in this; for instance, to find SQL injection and cross-site scripting.

Acunetix [8] is an automated tool for evaluating the security of web applications, scanning your web applications for exploitable vulnerabilities like SQL Injection and Cross-Site Scripting. Any website or web application that can be reached through a web browser and makes use of the HTTP/HTTPS protocol is generally scanned by Acunetix. For assessing pre-made and custom web applications, including those implementing JavaScript, AJAX, and Web 2.0 web apps, Acunetix provides a strong and distinct solution. Acunetix has a smart crawler that can discover virtually any file. Since what is not found cannot be checked, this is important.

# Our GitHub link to view the implementation: https://github.com/pooja-polampalli/INSE6610- 2022-Project-Group10/tree/main/vulnerability-tools

## Comparison of the tools [7]:

|  |  |  |
| --- | --- | --- |
| ***Keyword*** | ***Nessus*** | ***Acunetix*** |
| Performance speed | Scanning speed is slower | Scanning speed is faster |
| Working | Does cursory scanning against web applications | AcuSensor crawls all web applications |
| Scanning range | Has a limited range of web applications | Scans any kind of web applications without any  limitations |
| Best for | Serves small and medium  organizations with web security needs (1000+ users) | Ideal for security practitioners, consultants, and pen testers  (1-1000 users) |
| Pricing | Cheaper when compared to Acunetix | Costlier |
| Functionalities | Basic network scan, Malware Scan, Mobile Device Scan, Host Discovery, Policy Auditing, Host Discovery, Policy Auditing, Drown Detection, PCI External Scan | Threat Intelligence, Risk Analysis, Web Inspection, Network Mapping, Continuous Monitoring, Interactive Scanning, Logging and Reporting, Defect Tracking,  Vulnerability Assessment, |

|  |  |  |
| --- | --- | --- |
|  |  | Asset Discovery, Defect Tracking |
| Functions | * Reporting: Customs reports to sort by vulnerability or host. It creates an executive summary and compares scan results to highlight changes. * Monitoring: Targeted Email notifications of scan results , remediation recommendations and scan configuration improvements. * Scanning Capabilities: Vulnerability Scanning (Including IPv4/IPv6/Hybrid Networks)   1. Uncredentialed vulnerability Discovery.   2. Credentialed scanning for system hardening and missing patches. | * Reporting: Various reports like Developer, Executive, Comprehensive etc make it possible to receive outcomes depending on a specific need.   Can also compare two scans for a single target and produce a comparison report.   * Monitoring: checks for vulnerabilities like SQL Injection, Cross site scripting and other exploitable vulnerabilities.   It performs out-of- band checks. It also gives suggestions on how to fix the vulnerability.   * Scanning Capabilities: This network security scanner helps to scan your IP address ranges for open ports and other network device-   specific security flaws. |
| Advantages | * Highly accurate scanning with low false positives. * Comprehensible scanning capabilities and features. * Easy deployment and maintenance. | * Allows multiple scans simultaneously * Gives suggestions for solving the vulnerabilities * Less false positive values |
| Technologies used | Hypervisors, web servers,  databases | AcuSensor and AcuMonitor |
| Deployment | Linux, macOS, Windows operating system. | Linux, macOS, Microsoft Windows operating system. Also, you can deploy it as a cloud service to store your  local resources. |

*Table 8: Comparison of vulnerability tools*