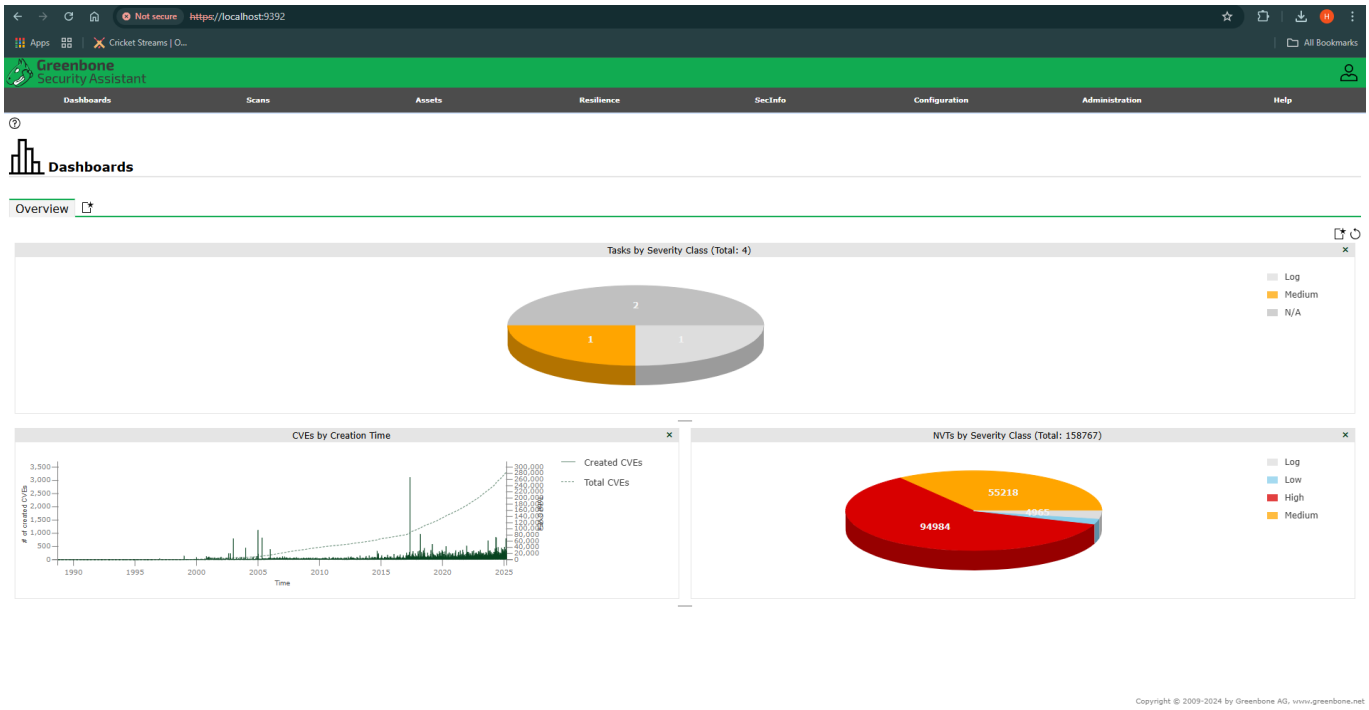
Vulnerability Assessment Using OpenVAS

Cybersecurity Internship

Reported by: Thumma Kiranmai

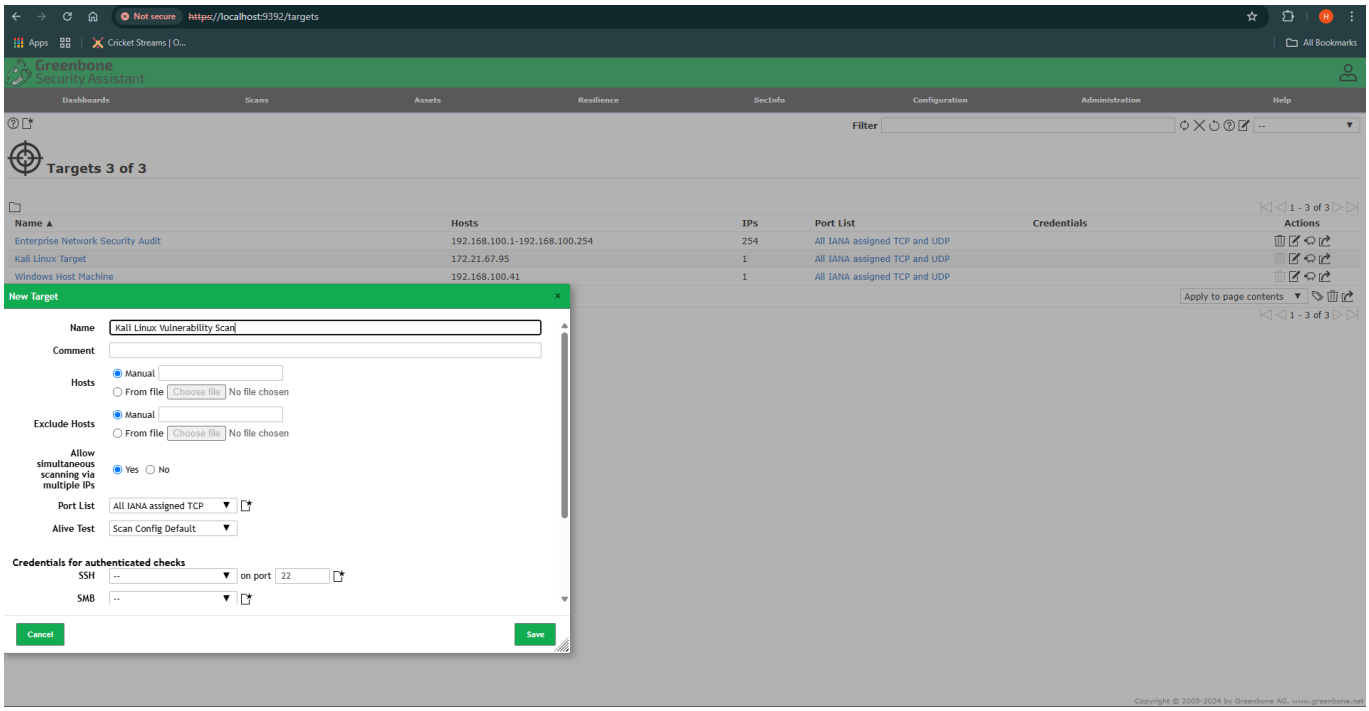
Date: May 31, 2025

OpenVAS Dashboard Overview



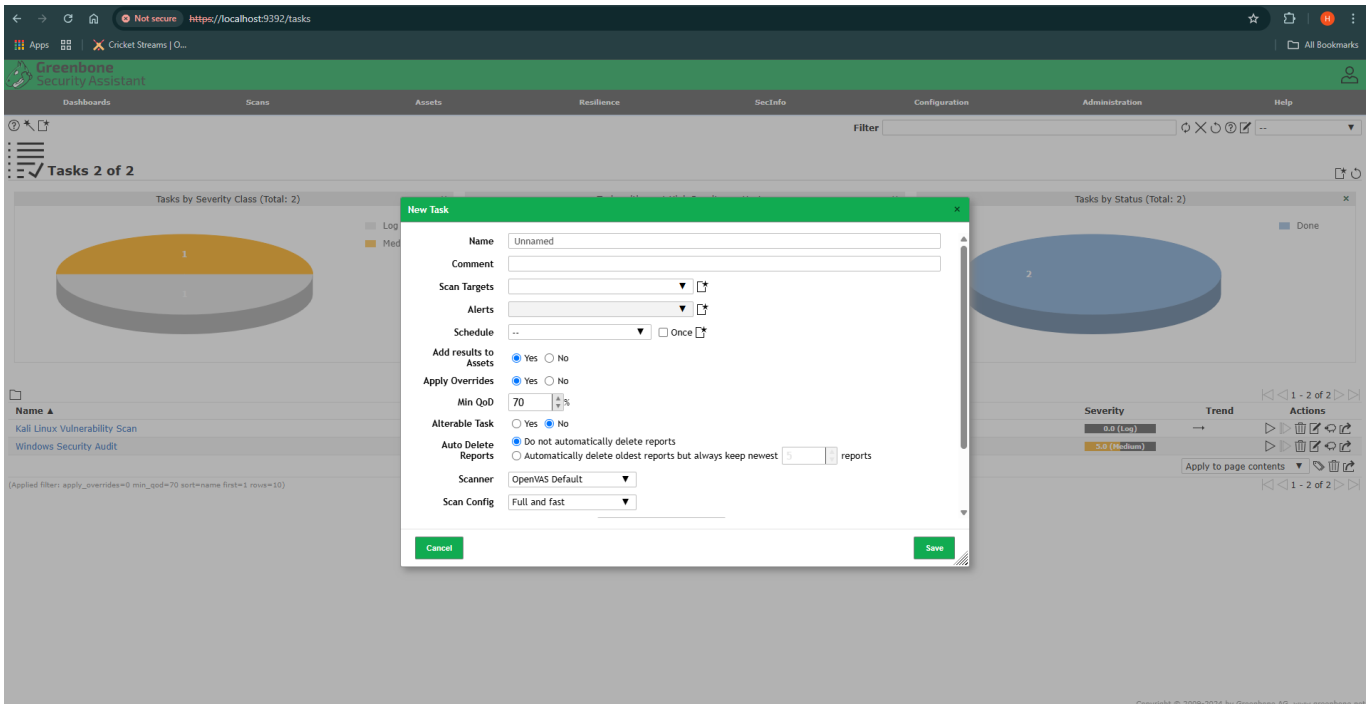
The dashboard provides a comprehensive summary of the vulnerability scanning environment. It shows the distribution of tasks by severity class and NVTs (Network Vulnerability Tests). The charts represent metrics such as CVEs over time and their classification by severity. These visual insights help in quickly identifying the security posture of the scanned assets. The top-right pie chart indicates that out of 4 tasks, two are marked as 'Log', one as 'Medium', and one as 'N/A'. The lower charts also highlight the volume of CVEs created historically and the corresponding escalation in vulnerability disclosures. This centralized view is key for security analysts to understand trends and severity distributions across scanned entities.

Target Configuration in OpenVAS



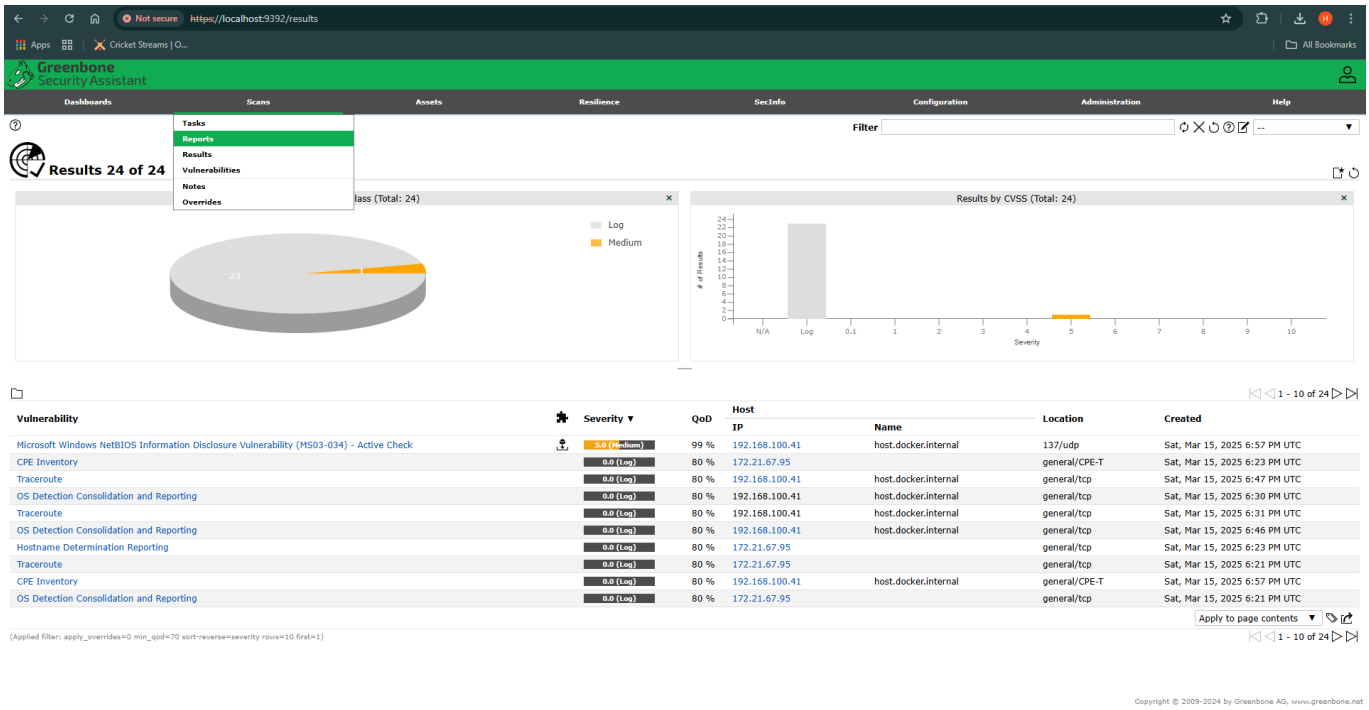
This section demonstrates the configuration of a new target for scanning. The configuration includes setting the name 'Kali Linux Vulnerability Scan' and specifying the IP address of the Kali Linux system. The target definition allows options for manually entering IPs or importing from a file. Other configurable options include simultaneous scanning, port list selection (like all IANA assigned TCP), and alive test methods. Authentication credentials for SSH and SMB are also included, allowing for authenticated scans, which provide deeper insights into the vulnerabilities present. This setup is crucial as it defines what systems will be scanned and under what conditions.

Scan Configuration Settings



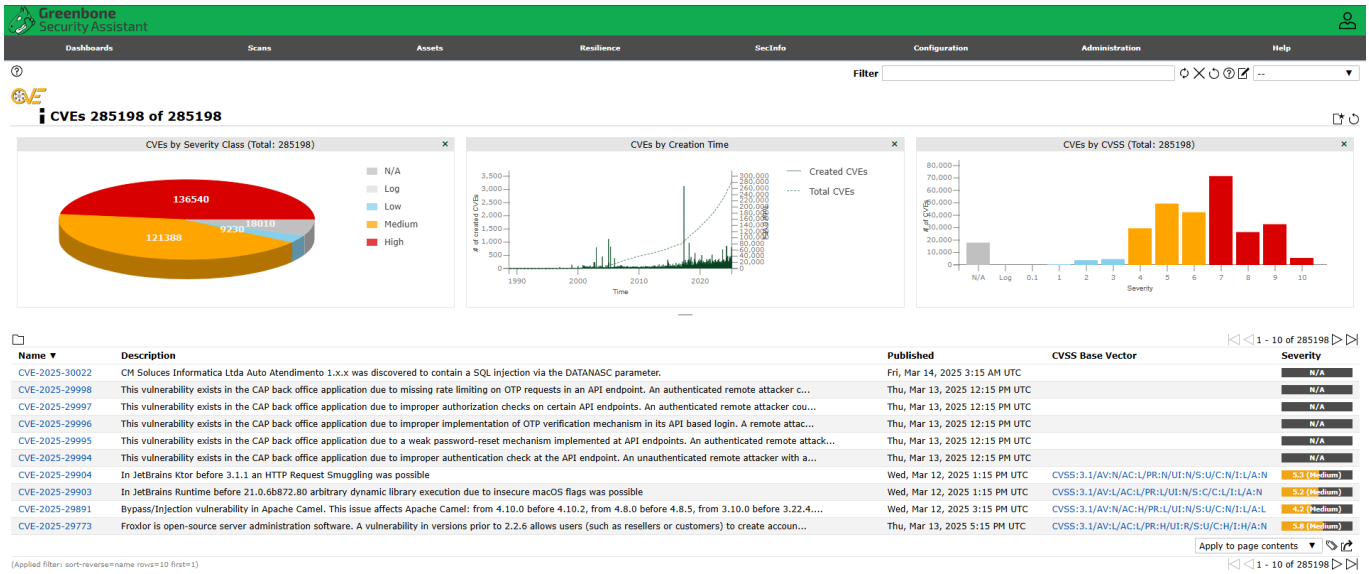
This part illustrates how a new scan task is configured in OpenVAS. Users can name the task, select scan targets, configure alerts, and define schedules. The scan is set to override vulnerabilities, with a minimum Quality of Detection (QoD) threshold of 70%, ensuring that only reliable results are considered. The scanner is set to OpenVAS Default, and the scan configuration is chosen as 'Full and fast', which balances thoroughness and speed. Additionally, the task is made alterable and report deletion is not automated. This configuration allows customization based on the scanning purpose, whether for scheduled audits or one-time checks.

Scan Results Analysis



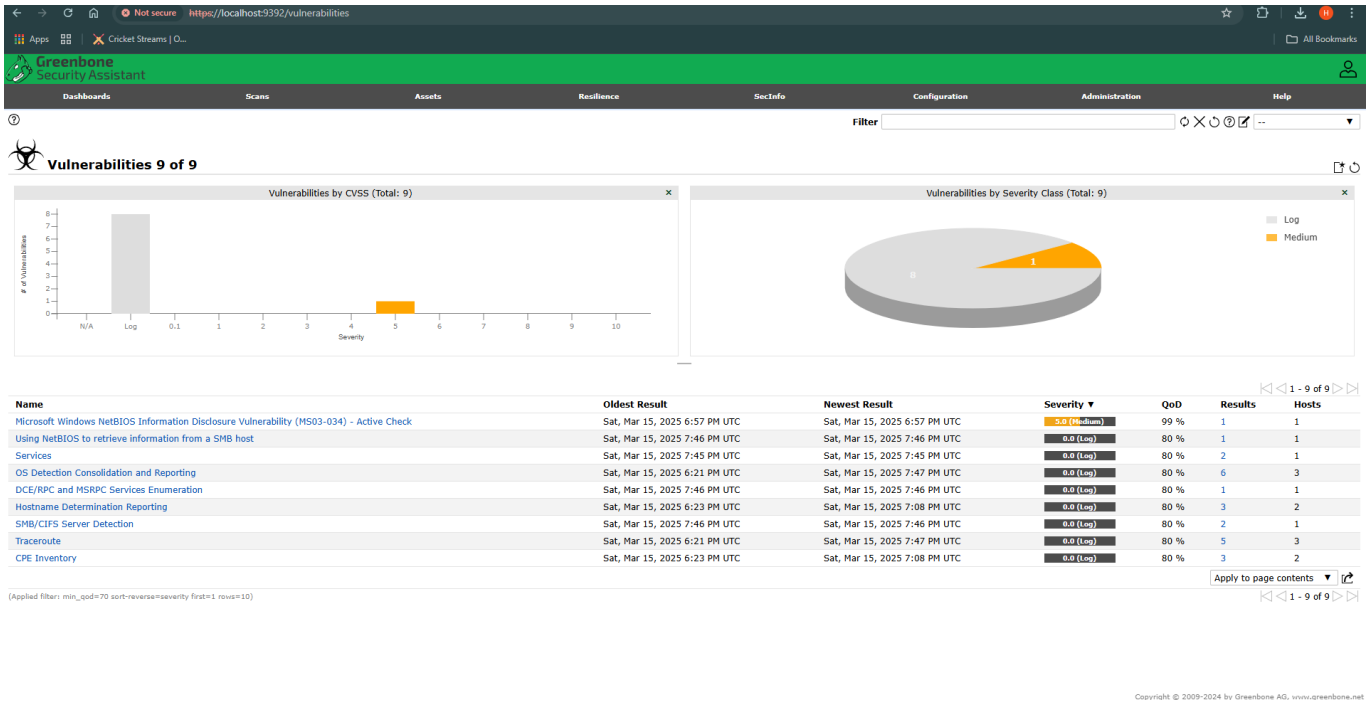
After running the configured scans, the results dashboard summarizes the findings. The graphical section categorizes results by severity and CVSS score. Most results fall into the 'Log' category, indicating informational or low-risk items. One result is classified as 'Medium', suggesting a moderate-risk vulnerability. The bottom table lists details such as vulnerability names, affected hosts, protocols involved, and timestamps. Notably, one medium severity vulnerability relates to NetBIOS information disclosure on a Windows machine. This summary helps in quick evaluation of which hosts need immediate attention based on risk level.

Detailed Scan Report



This detailed view shows the full list of CVEs identified during the scan. The breakdown includes severity classification, number of CVEs over time, and their respective CVSS scores. A pie chart on the left shows a significant number of high-severity CVEs (over 136,000), indicating a large threat landscape. The table at the bottom includes new and significant CVEs such as SQL injection in CM Solucoes and multiple authorization flaws in CAP applications. Each CVE entry contains the name, description, publication date, and severity, offering comprehensive vulnerability intelligence. This is particularly useful for patch management and vulnerability remediation planning.

Vulnerability Details View



This section presents the list of all vulnerabilities detected during the scan on specific hosts. A graphical distribution highlights that most vulnerabilities fall under 'Log' severity, with one classified as 'Medium'. The detailed table lists vulnerabilities such as SMB service detection, NetBIOS exposure, and OS detection reporting. It also shows the number of affected hosts and result timestamps. These findings offer technical insight into how exposed the network or system is and help in planning mitigations such as disabling unnecessary services or improving configuration security.