International Journal of Engineering and Techniques-Volume 11 Issue 5, September - October - 2025

# A Comparative Review of Vulnerability Assessment Tools: Insights from Qualys and Nessus

Rishabh Bhardwaj
LNCT University
Bhopal, (M.P).India
bhardwajrishabh@yahoo.com

Dr.Devdas Saraswat
Assistant Professor
*LNCT University*
Bhopal, (M.P).India
devdass@lnct.ac.in

***Abstract*— The proliferation of cyber threats has intensified the demand for reliable vulnerability assessment tools to identify and mitigate security weaknesses. This review paper systematically examines methodologies and tools for vulnerability assessment, with a focus on comparing industry-leading solutions like Qualys and Nes-sus. Drawing from peer-reviewed studies and industry frameworks, we analyze the standardized steps of vulnerability assessment ranging from planning and data gathering to remediation and continuous monitoring and evaluate how modern tools align with these phases. Our analysis reveals that Qualys excels in cloud-based scalability and compliance reporting, while Nessus dominates in on-premises network scanning depth and plugin diversity. Both tools demonstrate high accuracy in detecting vulnerabilities related to infrastructure, though Nessus reports marginally higher false positives. Open-source alternatives like Open-VAS offer cost-effective solutions but lack enterprise-grade support. The study underscores the importance of tool selection based on organizational infrastructures, threat landscape, and compliance needs. By synthesizing best practices and comparing tool capabilities, this review provides actionable insights for optimizing vulnerability management strategies in dynamic cybersecurity environments.**

***Keywords*— *Cyber threats, Vulnerability assessment, Qualys, Nessus***

## I. INTRODUCTION

This As cyberattacks grow in sophistication, vulnerability assessment remains a critical line of defense for organizations seeking to secure their digital assets [1]. Vulnerability assessment tools, such as Qualys and Nessus, automate the detection of security flaws, enabling proactive risk mitigation [2]. However, the effectiveness of these tools varies significantly depending on factors like deployment models (cloud vs. on-premises), threat coverage, and integration with organizational workflows. While prior studies have compared tools in niche contexts such as Wireless LANs or web applications a holistic review of methodologies and a granular comparison of leading commercial tools is lacking.

This paper addresses this gap by synthesizing the standardized phases of vulnerability assessment, as defined by frameworks like NIST SP 800-30 [3] and ISO 27001 [4], and evaluating how Qualys and Nessus perform at each stage. We answer key questions: What are the core steps in a vulnerability assessment workflow? How do Qualys and Nessus differ in scanning accuracy, scalability, and compliance reporting? What trade-offs exist between commercial and open-source tools?

Our analysis reveals that Qualys' cloud-native architecture supports seamless scalability and real-time dashboards, making it ideal for distributed environments. Nessus, with its extensive plugin library and offline scanning capabilities, is better suited for deep, on-premises network audits. Both tools, however, struggle with zero-day vulnerability detection, highlighting the need for complementary manual testing. Open-source tools like OpenVAS and OWASP ZAP, while cost-effective, often lack advanced reporting features and enterprise support.

The topic of discussion in Table 1 was the description of Qualys and Nessus' capabilities, features and support on multiple platforms.

| Feature / Capability | Qualys | Nessus |
|---|---|---|
| Platform Coverage | Offers broad coverage including cloud (AWS, Azure, GCP), containers, on-premises servers, endpoints, mobile devices, and network equipment. | Primarily focused on on-premises, endpoints, and network devices, but supports cloud and containers with integration. |
| Deployment Model | Cloud-based SaaS platform with agents for hybrid and multi-cloud environments. Minimal on-premises footprint. | Primarily installed as on-premises software; offers Nessus Essentials, Professional, and as part of Tenable.io (cloud-based). |
| Scalability | Highly scalable due to cloud-native architecture; supports enterprise-level, distributed environments. | Scales well for mid-size to large organizations, but enterprise-wide scaling is easier with Tenable.io rather than standalone Nessus. |

| | | |
|---|---|---|
| Integration with Ecosystem | Deep integrations with SIEM, SOAR, ticketing tools, ITSM, and DevOps pipelines; supports continuous compliance and policy monitoring. | Provides integration with SIEM, DevOps, and ITSM systems, though often requires Tenable.io or Tenable.sc for broader ecosystem coverage. |
| Container and Cloud Security | Native container security with image scanning, runtime protection, and cloud posture management. Strong coverage across multi-cloud. | Provides container image scanning and cloud integrations, but advanced cloud security posture management is mainly through Tenable.io. |
| Reporting & Analytics | Centralized dashboards with customizable compliance and risk reports; advanced analytics with threat prioritization. | Offers detailed vulnerability reports, risk scores, and dashboards. Prioritization is present but less advanced compared to Qualys' risk-based approach. |
| Compliance & Policy Support | Strong compliance management features (PCI DSS, HIPAA, ISO, GDPR, etc.), integrated directly into the platform. | Provides compliance scans and configuration audits, but broader governance capabilities are more developed in Tenable's enterprise suite. |
| Automation & Remediation Support | Automated patch management and remediation workflows; integrates directly with ITSM for closed-loop remediation. | Suggests remediation steps; automation and patching workflows require integration with Tenable.io or third-party tools. |
| User Interface & Ease of Use | Web-based, centralized dashboard; designed for enterprise teams with advanced analytics. May feel complex for beginners. | Simpler interface; user-friendly for small to mid-size teams. Easier for standalone vulnerability scanning. |
| Licensing & Cost Model | Subscription-based, tiered by assets and modules; best suited for organizations with complex environments. | Lower entry cost with Nessus Essentials/Professional; cost increases with enterprise use (Tenable.io/Tenable.sc required). |

By contextualizing these findings within established vulnerability assessment methodologies, this review equips organizations with criteria to select tools aligned with their operational needs. It also identifies persistent challenges, such as interoperability gaps and false positives, urging future research into AI-driven prioritization and unified threat intelligence platforms.

## II. RELATED WORK

Recent research on vulnerability assessment tools has focused on comparative evaluations, performance benchmarking, and contextual applicability across diverse environments. These studies highlight the strengths, limitations, and evolving capabilities of tools in addressing modern cyber-security challenges.

The Odun-Ayo et al. [3] conducted a comparative review of vulnerability analysis tools, emphasizing their detection efficacy for common threats such as SQL injection (20% coverage), Cross-Site Scripting (24%), and Denial of Service attacks (21%). Their study revealed that 24% of tools are open source, 12% are free, and most operate on Linux, underscoring the need for tool selection based on specific penetration testing objectives. Similarly, Kejiou and Bekaroo [6] evaluated tools for Wireless LANs (WLANs), including Nessus, OpenVAS, Nexpose, and GFI LanGuard. They observed significant variability in vulnerability coverage and scan durations, noting that granulari-ty of outputs and scan efficiency depend on tool design, rather than scan duration alone.

Chaturvedi et al. [5] advocated for integrating complementary tools like OpenVAS, Wireshark, Nmap, and Metasploit into unified workflows. Their analysis demonstrated that OpenVAS excels in vulnerability scanning, Wireshark in traffic analysis, Nmap in network mapping, and Metasploit in penetration testing, collectively enhancing proactive threat mitigation. Nrk [8] expanded this comparative lens to Nessus, Acunetix, and Nikto, evaluating detection accuracy, CVSS-based risk scoring, ease of use, and cost-effectiveness. The study emphasized Nessus's comprehensive scanning capabilities, Acunetix's web application focus, and Nikto's niche in server vulnerability detection, advocating for organizational alignment in tool selection.

Performance benchmarking studies further refine tool applicability. Jarupunphol et al. [7] tested Burp Suite and OWASP ZAP on a university web application, finding Burp Suite superior in detecting high-risk vulnerabilities aligned with the OWASP Top 10 (2021), while ZAP produced more medium-confidence alerts. Raju [10] explored tools like Nessus, Nmap, and Metasploit on Kali Linux, highlighting Nessus's depth in vulnerability identification, Nmap's network discovery utility, and Metasploit's role in simulating real-world attacks for validation.

A recurring theme across these studies is the absence of a universally optimal tool. Instead, re-searchers stress contextual factors—such as organizational infrastructure, threat landscape, and compliance requirements—as critical to tool selection. For instance, WLAN-specific tools [4] prioritize wireless protocol vulnerabilities, while web application scanners [7] focus on

OWASP-defined risks. Open-source tools like OpenVAS and Nikto are lauded for cost efficiency but may lack advanced features of commercial alternatives like Nessus or Acunetix [3, 6].

Collectively, these works underscore the importance of hybrid approaches, combining automated scanning with manual validation, and integrating tools into iterative workflows for continuous monitoring and remediation. However, gaps remain in addressing zero-day vulnerabilities, interoperability between tools, and scalability in cloud-native environments areas this review paper seeks to explore further.

## III. Methodology

The methodology for using vulnerability assessment tools follows a structured process to ensure comprehensive detection and management of security weaknesses. The process begins with planning and preparation, where the objectives, scope, and resources are clearly defined while ensuring compliance with relevant standards. This is followed by asset discovery and information gathering, which involves creating an inventory of systems, applications, and networks, as well as mapping their configurations and communication flows.

Once assets are identified, the next step is vulnerability identification, where automated scanners such as Nessus, OpenVAS, or Qualys are used to detect flaws, missing patches, or misconfigurations, complemented by manual checks to uncover issues that tools may overlook.

After vulnerabilities are detected, they undergo analysis and validation to eliminate false positives, assess risk context, and classify severity using frameworks like CVSS. Based on this evaluation, vulnerabilities are prioritized by considering factors such as exploitability, impact, and business relevance. The methodology steps are shown in Fig 1.

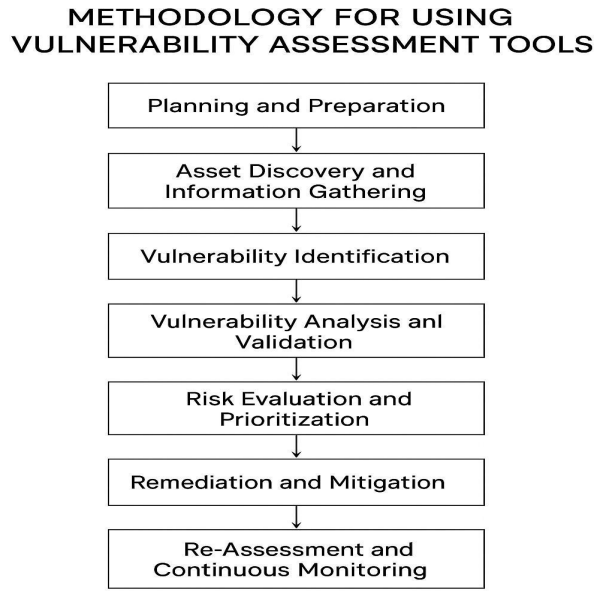


Fig 1: Methodology Steps

The findings are then documented in detailed reports that include both technical details and executive summaries, along with practical remediation recommendations.

The next step is remediation and mitigation, where patches, configuration changes, and compensating controls are applied. Finally, re-assessment and continuous monitoring ensure that vulnerabilities are resolved and that new threats are promptly addressed. This cyclical methodology ensures organizations maintain strong security resilience and adapt effectively to evolving cyber threats. Both tools have the same methodology adopted by the organization.

## IV. Exploring and comparing Qualys and Nessus

This analysis aims to evaluate and compare the vulnerability detection capabilities of two prominent security scanning tools such as Nessus and Qualys, when applied to the same asset under authenticated scanning conditions. The objective is to understand the divergence in detection granularity, severity classification, and volume of vulnerabilities reported by each tool.

An authenticated vulnerability scan was conducted on a single asset using both Nessus and Qualys scanners. Authenticated scans involve credentialed access to the asset, allowing a deeper inspection of system configurations, installed software, and permissions, thereby yielding more comprehensive vulnerability data than unauthenticated scans. The number of vulnerabilities detected.

### *A. Classification of vulnerabilities by severity*

Use either Comparative severity taxonomy: Nessus uses categories such as Critical, High, Medium, and Low, while Qualys follows a numerical severity scale (1 to 5), where 5 indicates the highest risk.

| Severity | Vulnerability tools | |
|---|---|---|
| | ***Nessus*** | ***Qualys*** |
| Critical | **97** | **63** |
| High | **250** | **344** |
| Medium | **138** | **82** |
| Low | **1** | **30** |

Table 2: Nessus and Qualys Severity details

### *B. Techniques and Tools*

The Nessus by Tenable: Utilizes a vulnerability scoring system based on the CVSS (Common Vulnerability Scoring System) and a plugin-based architecture for vulnerability checks.

Qualys VMDR: Employs cloud-based scanning and correlates threat intelligence data with CVSS scores to generate prioritized vulnerability lists.

Both tools leverage credentialed access for authenticated scans, enabling them to inspect installed software, operating system components, misconfigurations, and missing patches.

When running vulnerability assessments, the timing of scans is as critical as the scan configuration itself. Both Qualys and Nessus allow administrators to control when and how often scans occur. Proper timing ensures that assessments do not interfere with business operations while still providing up-to-date security insights.

*C. Quality Assurance*

The Quality assurance discussed below.

- Both scans were executed using updated signatures and plugin sets.
- Default configuration settings for vulnerability classification were retained.
- The asset's configuration remained unchanged between the two scans to preserve consistency.
- Both tools were granted the same privileged credentials to eliminate access-based discrepancies

*D. Limitations and Potential Biases*

The following limitations and potential biases is discussed below.

- *Tool-specific taxonomies*: Disparities in vulnerability classification may result from each tool's proprietary scoring algorithm and interpretation of CVSS vectors.
- *Plugin variability:* Nessus and Qualys maintain different plugin databases, leading to difference in vulnerability identification even under similar scan conditions.
- *Timeframe synchronization:* While assumed to be simultaneous, any lag between scans could allow environmental changes (e.g., patch installation) that slightly skew results.
- *False positives*: Both tools may report non-exploitable or irrelevant vulnerabilities based on heuristic assessments.

*E. Key Findings and Interpretations*

- *Detection Volume:* Nessus identified a greater number of Critical vulnerabilities (97) compared to Qualys (63). Conversely, Qualys detected a higher number of High-severity issues (344 vs. Nessus's 250).

  For the Medium and Low severity levels, Nessus records 138 and 1 vulnerabilities, respectively, whereas Qualys reports 82 medium and 30 low-level vulnerabilities. Medium-level findings often point to weaknesses that could become dangerous if combined with other vulnerabilities, while low-level ones may involve minor misconfigurations or informational alerts. The significant difference in the low-severity category (Nessus: 1 vs. Qualys: 30) suggests that Qualys might provide more granular reporting for less critical issues, which could be useful for long-term system hardening and compliance purposes. Overall, the table highlights that both tools have strengths in different severity ranges, making them complementary in a comprehensive vulnerability management strategy.

- *Severity Distribution Implication:* The more conservative Critical classification by Qualys may reduce alert fatigue but could understate immediate risk. In contrast, Nessus's higher count in critical findings might promote proactive remediation but may also include borderline high-risk items.

*F. Analysis other parameters of the tools.*

- When comparing Qualys and Nessus in table 3, the choice largely depends on the organization's size, infrastructure, and long-term goals.

  Table 3: Comparing Qualys and Nessus at multiple parameter.

| Aspect | Qualys | Nessus |
|---|---|---|
| Tool Capabilities | Delivers vulnerability management, compliance checks, asset discovery, web app scanning, and cloud security posture monitoring. | Specializes in vulnerability assessment, configuration audits, malware detection, and patch validation through plugins. |
| Deployment Model | Cloud-native SaaS platform with lightweight agents and connectors for hybrid and on-premises assets. Centralized, globally scalable. | Primarily deployed as on-premises software or virtual appliance. Supports both agent-based and agentless scanning. Requires manual scaling for large networks. |
| Feature Set | Automated patch prioritization, continuous monitoring, integration with threat intelligence feeds, and strong compliance | Extensive plugin library, rapid CVE coverage, flexible scan customization, and integration with the Tenable ecosystem for broader |

| | | |
|---|---|---|
| | reporting. | capabilities. |
| Detection Accuracy | High accuracy enabled by contextual analysis and cloud-driven intelligence; effective for complex and distributed infrastructures. | Strong accuracy at host and network levels; quick plugin updates ensure timely detection of emerging threats. |
| False Positives | Generally low; contextual intelligence minimizes noise, though incomplete configurations may trigger extra alerts. | Low overall; however, large-scale scans can generate repetitive or redundant results requiring analyst validation. |
| Scalability | Highly scalable due to SaaS delivery model; capable of managing millions of assets across global enterprises. | Suitable for medium to large deployments but scaling across distributed or cloud-heavy environments may require additional Tenable products. |
| Licensing | Subscription-based, priced per asset or service module. Flexible options allow enterprises to scale up as asset inventory grows. | Licensed per number of IPs, assets, or agents. Simple structure but may become costly in very large environments. |
| Cost Considerations | Higher initial investment but cost-effective for enterprises due to all-in-one SaaS capabilities and reduced infrastructure overhead. | Lower entry cost, making it attractive for organizations. Costs can rise significantly when scaling to enterprise levels. |
| Best Fit | The enterprises seeking global scalability, compliance integration, and cloud-native security coverage. | Security teams requiring targeted, fast, and customizable vulnerability scans with lower upfront costs. |

Qualys is better suited for enterprises that require global scalability, compliance reporting, and cloud-native visibility. Its SaaS model eliminates much of the infrastructure overhead, and although its licensing may appear costlier at first, it becomes more economical as asset inventories grow because of integrated features that reduce the need for multiple tools.

Nessus, on the other hand, is an excellent fit for the organizations or teams that need fast, customizable, and precise vulnerability scanning without significant upfront investment. Its simpler licensing makes it easier to adopt, but scaling to enterprise-level environments often increases costs and may require the purchase of other Tenable solutions to match Qualys' breadth.

Interpretation: These results underscore the importance of using multiple tools in a layered security assessment strategy. Each scanner has unique detection strengths—Nessus excels at exposing high-impact vulnerabilities rapidly, while Qualys offers broader visibility into configuration-level and moderately severe issues.

Organizations should interpret vulnerability data contextually, supplementing automated scores with expert analysis to prioritize remediation efforts effectively.

## V. Conclusion

The preferred spelling of the word "acknowledgment" in This review systematically analyzed the methodologies and tools central to vulnerability assessment, with a focused comparison of Qualys and Nessus—two industry-leading solutions. By mapping their capabilities to the standardized phases of vulnerability assessment (planning, detection, prioritization, remediation, and monitoring), the study highlights critical insights for organizations navigating tool selection.

Qualys emerges as a robust choice for cloud-centric environments, offering scalable, real-time scanning and automated compliance reporting aligned with frameworks like GDPR and HIPAA. Its SaaS model simplifies deployment for distributed infrastructures but incurs higher costs for large-scale use. In contrast, Nessus excels in on-premises network environments, leveraging its extensive plugin library and offline scanning capabilities to deliver granular, deep-dive audits. However, its strength in customization is counterbalanced by limited cloud agility and marginally higher false-positive rates. Both tools demonstrate strong performance in detecting the vulnerabilities, though neither fully addresses zero-day threats, underscoring the need for complementary manual testing.

Open-source alternatives like OpenVAS and OWASP ZAP provide cost-effective entry points for smaller organizations but lack the advanced analytics, compliance features, and enterprise support of commercial tools. Across all solutions, persistent challenges such as interoperability gaps, false positives, and siloed reporting frameworks reveal opportunities for innovation. For organizations, the choice between Qualys and Nessus hinges on infrastructure priorities: cloud scalability versus on-premises depth. Future research should explore AI-driven prioritization to reduce false positives, unified platforms for hybrid environments, and enhanced detection mechanisms for emerging threats. By aligning tool capabilities with organizational needs and threat landscapes, businesses can fortify their cybersecurity postures in an era of relentless digital risk. This review consolidates critical criteria for informed decision-making, empowering stake-holders to optimize vulnerability management strategies in alignment with evolving cybersecurity demands.

## REFERENCES


[1] Verma, P., Newe, T., O'Mahony, G.D., Brennan, D. and O'Shea, D., 2025. Towards a Unified Understanding of Cyber Resilience: A Comprehensive Review of Concepts, Strategies, and Future Directions. IEEE Access.

[2] B. J, "VULNTRACK : VULNERABILITY ASSESSMENT AND MANAGEMENT SYSTEM ENHANCED CYBERSECURITY AND MITIGATING SECURITY RISKS," *International Research Journal of Education and Technology (IRJET).*, vol. 6, no. 11, pp. 76–95, Nov. 2024, doi: 10.70127/irjedt.vol.8.issue04.95.

[3] Odun-Ayo, I., Blessing, O., Martins, I., Owoka, E., Owoseni, T., & Omonedo, E. (2024, April). Comparative Review of Vulnerability Analysis Tools. In 2024 International Conference on Science, Engineering and Business for Driving Sustainable Development Goals (SEB4SDG) (pp. 1-6). IEEE.

[4] Kejiou, A. and Bekaroo, G., 2022, October. A review and comparative analysis of vulnerability scanning tools for wireless LANs. In 2022 3rd International Conference on Next Generation Computing Applications (NextComp) (pp. 1-6). IEEE.

[5] Chaturvedi, A., Lakhani, B., Agarwal, T., Moharir, M. and AR, A.K., 2024, August. A Comprehensive Vulnerability Tools Analysis for Security and Control in IT Environment and Organizations. In 2024 5th International Conference on Electronics and Sustainable Communication Systems (ICESC)(pp. 612-618). IEEE.

[6] Nrk, S., 2024. A Comparative Analysis of Vulnerability Management Tools: Evaluating Nessus, Acunetix, and Nikto for Risk Based Security Solutions. arXiv preprint arXiv:2411.19123.

[7] Jarupunphol, P., Seatun, S. and Buathong, W., 2023. Measuring Vulnerability Assessment Tools' Performance on the University Web Application. Pertanika Journal of Science & Technology, 31(6).

[8] Raju, Dr. R. (2024). A Literature Survey on System Security and Network Vulnerability Assessment. Indian Scientific Journal Of Research In Engineering And Management. https://doi.org/10.55041/ijsrem29695

[9] Dybka, J., 2020. Qualys Inc.

[10] Raju R, "A literature survey on system security and network vulnerability assessment," *INTERANTIONAL JOURNAL OF SCIENTIFIC RESEARCH IN ENGINEERING AND MANAGEMENT*, vol. 08, no. 04, pp. 1–5, Apr. 2024, doi: 10.55041/ijsrem29695.

[11] A. Chaturvedi, B. Lakhani, T. Agarwal, N. Mohana, M. Moharir, and A. K. A. R, "A Comprehensive Vulnerability Tools Analysis for Security and Control in IT Environment and Organizations," *IEEE*, pp. 612–618, Aug. 2024, doi: 10.1109/icesc60852.2024.10689860.

[12] M. Alqaradaghi and T. Kozsik, "Comprehensive evaluation of static analysis tools for their performance in finding vulnerabilities in Java code," *IEEE Access*, vol. 12, pp. 55824–55842, Jan. 2024, doi: 10.1109/access.2024.3389955.