tenable

6 Ways to Optimize Your Nessus Scans

GET THE MOST OUT OF NESSUS PROFESSIONAL WITH THESE USEFUL FEATURES

Contents:

The attack surface in your network is continually evolving, and new vulnerabilities are disclosed every day. No organization is immune to cyberattacks.

Introduction
Discover your vulnerabilities

The attack surface in your network is continually evolving, and new vulnerabilities are disclosed every day. No organization is immune to cyberattacks. You cannot hope to keep up with threats without conducting regular vulnerability assessments of your network. You need reliable vulnerability assessment.

Nessus Professional from Tenable is the ideal foundation for these efforts, and its dependability has made it the world's #1 vulnerability assessment solution.

But Nessus' capabilities go far beyond basic examination of your network. Let's explore how you can solve some of your most pressing vulnerability assessment challenges with some of the advanced features of the solution.

Credentialed Scanning

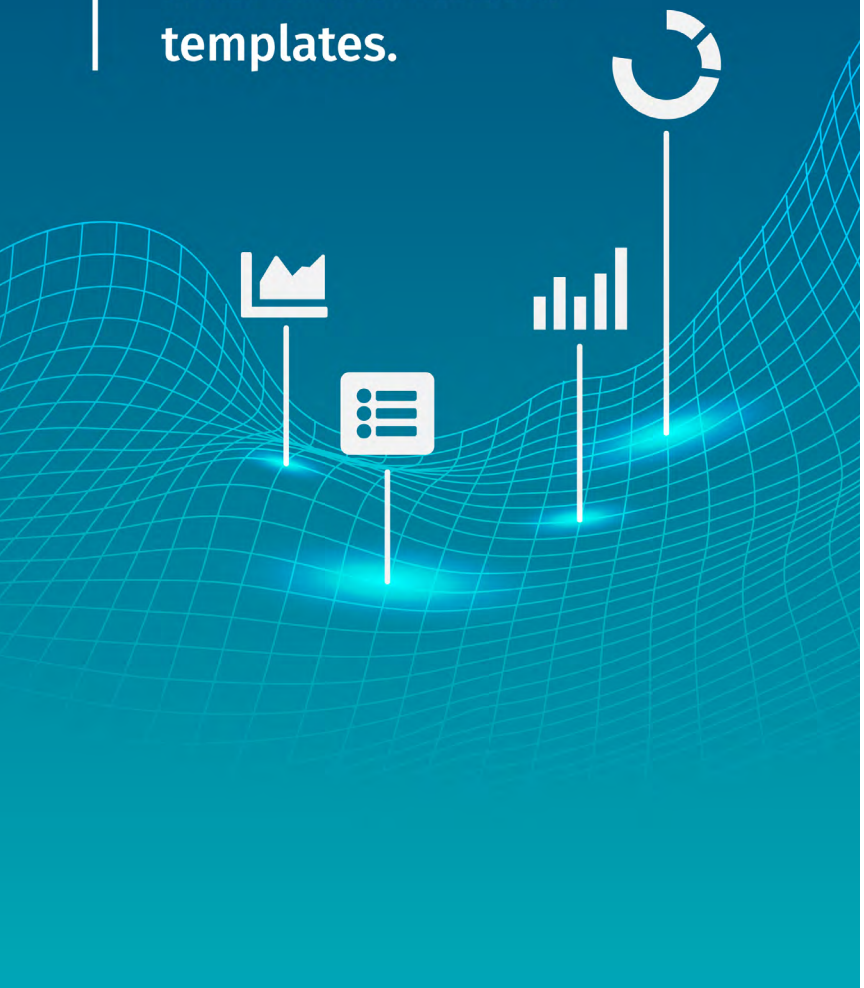
About 90% of vulnerabilities can only be detected via **credentialed scanning.** Furthermore, it can help you adhere to compliance and regulatory standards that require credentialed vulnerability assessment in order to fulfill specific requirements within the benchmark.

Scanning on a regular basis with credentials is essential. Comprehensive credentialed scanning means more thorough assessment (a typical credentialed scan of a Windows host yields 7x the results compared to a non-credentialed scan), along with recommendations for discovered flaws.

Nessus Professional allows for credentialed scans that serve Windows and SSH hosts, cloud platforms (Amazon Web Services, Azure and Salesforce), databases (MySQL, MongoDB and more), Microsoft SCCM patch management and numerous plaintext authentication frameworks ranging from HTTP to FTP.

Get more accurate results by expanding the scope of your assessment.

Quickly and accurately conduct compliance audits with customizable templates.



Compliance Auditing

Compliance audits ensure that your diverse IT assets adhere to all regulatory and internal standards your organization follows. With Nessus Professional, you get greater control of what and how you audit.

Numerous pre-built audit templates are featured in Nessus for common frameworks including PCI DSS, HIPAA, NIST and CIS Benchmarks. Editing these templates is simple: Visit the **Tenable Community**, download the raw audit files and alter them as you see fit using a plain-text editor of choice. You can also easily add your own audit policies to handle unique network needs.

Always remember that **compliance audits** aren't a replacement for vulnerability scans. Running both is essential for comprehensive oversight.

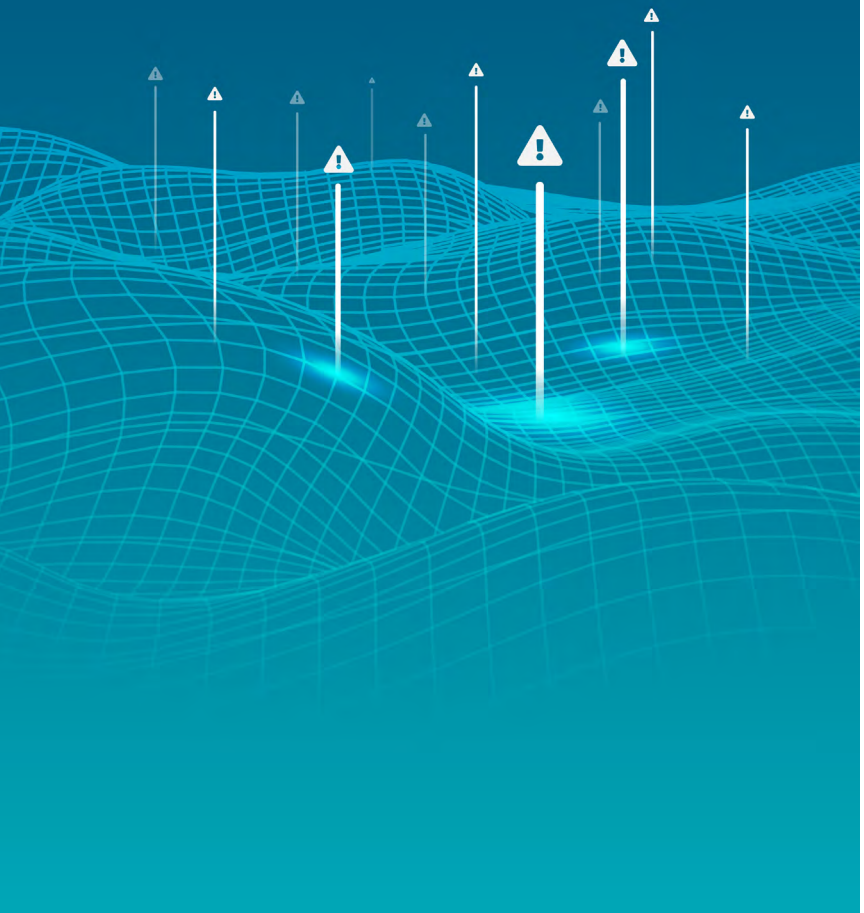
Offline Configuration Auditing

Auditing your network infrastructure to ensure compliant operation is essential, yet network downtime and service interruption can have a serious business impact. Configuration auditing is typically handled by scanning the configuration file of the asset in question. But scanning a gateway or front-facing switch can bring your entire network down for the duration of the scan. Nessus Professional bridges the gap by allowing you to conduct this critical task offline.

Offline configuration audits run much faster and don't interfere with infrastructure, keeping business operations running without interruption. Nessus Professional's offline configuration auditing functions can assist with a variety of network infrastructure assets. Further, it can assess the system for compliance with mandatory standards, like the Gramm–Leach–Bliley Act (GLBA), and voluntary codes your organization uses such as the CIS OS or database standards.

Avoid network downtime and service interruption with offline configuration checks.

Expedite vulnerability scans to save time and resources.



Live Results

New vulnerabilities are emerging every day. If you're concerned about specific emerging threats, you don't want to wait until the close of business to determine if you're at risk.

Active vulnerability scanning is the core function of Nessus: the platform's bread and butter. But conducting daily scans, while an attractive notion to the most meticulous infosec professionals, is daunting and unfortunately impractical for many organizations. Full-fledged scanning requires other operations to slow down or stop completely, which is why it's often done outside regular business hours.

Live Results threads this needle perfectly; it automatically performs an offline vulnerability assessment with every plugin update, leveraging data from past scans. If Live Results identifies potential vulnerabilities, you can easily run a scan to validate the results—saving valuable time and resources without compromising infosec integrity.

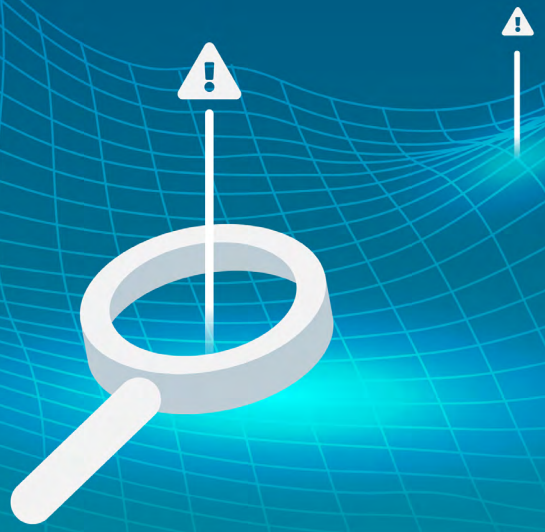
Dynamic Vulnerability Scanning

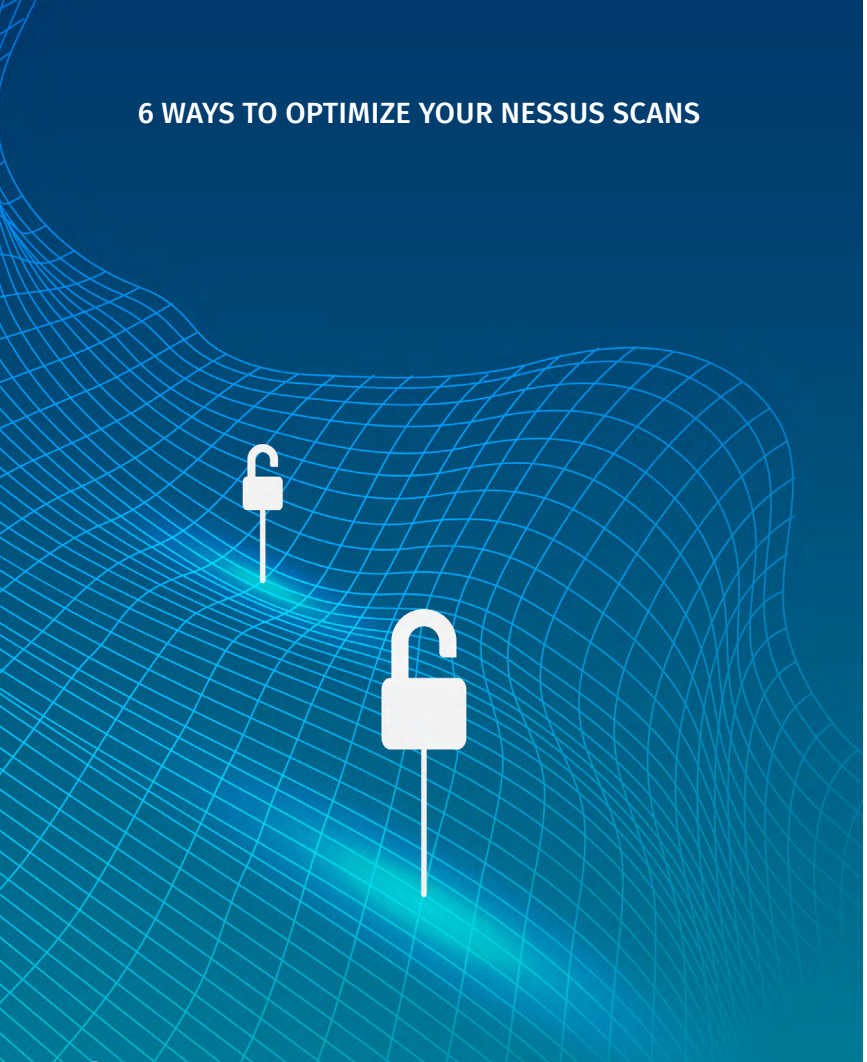
What if traditional scanning isn't quite right for your situation? Perhaps you want to look solely at how vulnerable (or strong) your web server is. Or maybe you'd like to check for all of the CVEs noted in the latest NIST bulletin, or search specifically for Microsoft IIS vulnerabilities.

Selecting a subset of all CVEs and performing comprehensive assessments on those specific points of potential risk – e.g., newer or older entries to the National Vulnerability Database (NVD), web server vulnerabilities, CVEs that allow for data theft and so on – is simple through Nessus Professional's dynamic vulnerability scanning feature. The interface allows you to avoid common scan-policy pitfalls, such as looking on a plugin-by-plugin basis instead of enabling plugin families.

Use a broad range of criteria - CVE publication date, IP ranges and much more - to create a laser-focused scan for segments of your system that need your immediate, undivided attention. This is particularly useful for following up a Live Results scan that found potential CVEs.

Easily adjust your scans to focus on your top priorities.





Increase efficiency by focusing on vulnerabilities that matter most to your organization.

Vulnerability Filtering

Proper vulnerability filtering allows for effective organization of remediation activities. Filtering allows you to identify critical weaknesses more efficiently by dividing Common Vulnerabilities and Exposures (CVEs) into distinct categories, examining each segment to find the vulnerabilities with the greatest damage potential so you can work to address them first.

But there's more to filtering than that. Perhaps you're seeking the CVEs that specifically endanger certain hosts on your network, or allow for specific categories of compromise. Maybe you have a critical application you want to secure immediately.

Filtering in Nessus Professional offers a simple, user-friendly interface through which to quickly review aptly categorized vulnerabilities. Additionally, through "vulnerability snoozing," you can temporarily hide details of CVEs that are less immediate, keeping you focused on the most pressing threats.

Conclusion

Maximize your vulnerability assessments

The cybersecurity landscape is continually evolving. Every organization has unique needs and challenges.

Embracing the full scanning capabilities of Nessus Professional allows you to take your vulnerability assessments to the next level – optimizing results while saving time and resources. You can significantly mitigate exposure to the biggest cyberthreats by creating a unique set of vulnerability scanning and assessment practices tailored to particular organizational needs.

Nessus Professional's industry-leading vulnerability coverage and accuracy ensure you get a clear view of vulnerabilities across your environment – a must in this threat-rich era.

READY TO LEARN MORE?

View the Nessus Resource Center or visit the Tenable Community.

www.tenable.com