tenable network security

Nessus® professional

Nessus Professional Vulnerability Scanner

Nessus Professional, die branchenweit meistgenutzte Lösung für Schwachstellenmanagement, unterstützt Sie dabei, die Angriffsfläche Ihrer Organisation zu verkleinern und die Compliance zu gewährleisten. Nessus bietet schnelles Asset-Profiling, Konfigurationsüberwachung, Zielprofilerstellung, Malware-Erkennung, Bestimmung sensibler Daten und vieles mehr.

Nessus unterstützt mehr Technologien als jede andere Lösung und scannt Betriebssysteme, Netzwerkgeräte, Hypervisoren, Datenbanken, Webserver sowie wichtige Infrastrukturen auf Gefährdungen, Bedrohungen und Compliance-Verletzungen.

Mit der weltweit größten kontinuierlich aktualisierten Bibliothek von Schwachstellen- und Konfigurationsprüfungen sowie der Unterstützung durch das fachkundige Vulnerability Research Team setzt Nessus Maßstäbe in Sachen Geschwindigkeit und Genauigkeit.

Nessus ermöglicht dem Nutzer, die Liste der gefundenen Schwachstellen nach über 20 verschiedenen Kriterien zu sortieren und zu filtern. Schweregrade können individuell angepasst werden und die Problembehebungsübersicht bietet umsetzbare Ergebnisse.

Nessus-Leistungsmerkmale

Reporting and Monitoring

- *Flexible Berichterstellung: Sortieren Sie anpassbare Berichte nach Schwachstelle oder nach Host, erstellen Sie eine Zusammenfassung oder vergleichen Sie Prüfergebnisse und heben Sie Änderungen hervor*
  - *Dateiformate: Nativ (XML), PDF (erfordert Java-Installation auf dem Nessus-Server), HTML und CSV*
- *Gezielte E-Mail-Benachrichtigung über Prüfergebnisse, Empfehlungen zur Problembehebung und Verbesserungen der Prüfkonfiguration*

Nessus wird bereits von mehr als einer Million Nutzern weltweit für die Gefährdungs-, Konfigurations- und Compliance-Bewertung eingesetzt.

Vollständige Schwachstellenabdeckung:

- Virtualisierung & Cloud
- Malware & Botnets
- Konfigurationsüberwachung
- Webanwendungen

Hauptnutzen

- **Verkleinerte Angriffsfläche:** Verhindert Angriffe durch Erkennung von Sicherheitslücken, die geschlossen werden müssen
- **Umfassend:** Entspricht der größten Auswahl an Compliance- und Regulierungsstandards
- **Skalierbar:** Starten Sie mit einer Nessus Professional-Einzelplatzlizenz und upgraden Sie auf Nessus Manager oder Nessus Cloud, wenn Ihre Anforderungen im Bereich Vulnerability Management zunehmen
- **Gesamtbetriebskosten (TCO):** Kompletter Vulnerability Scanner zu einem niedrigen Preis
- **Laufend aktualisiert:** Das Tenable-Research-Team fügt ständig neue Inhalte hinzu
- **Leicht zugänglich:** Per Internetbrowser jederzeit und überall nutzbar

Scanfunktionen

- *Feststellung: Präzise, schnelle Bestandsfeststellung*
- *Prüfung: Gefährdungsprüfung (einschließlich IPv4-/IPv6-/Hybridnetzwerke)*
  - *Nicht-authentifizierte Schwachstellenerkennung*
  - *Authentifizierte Prüfung auf Systemhärtung und fehlende Patches*
- *Abdeckung: Breite Bestandsabdeckung und Profilerstellung*
  - *Netzwerkgeräte: Firewalls/Router/Switches (Juniper, Check Point, Cisco, Palo Alto Networks), Drucker, Speicher*
  - *Offline-Konfigurationsüberwachung von Netzwerkgeräten*
  - *Virtualisierung: VMware ESX, ESXi, vSphere, vCenter, Microsoft, Hyper-V, Citrix Xen Server*
  - *Betriebssysteme: Windows, OS X, Linux, Solaris, FreeBSD, Cisco iOS, IBM iSeries*

  - *Datenbanken: Oracle, SQL Server, MySQL, DB2, Informix/DRDA, PostgreSQL, MongoDB*
  - *Webanwendungen: Webserver, Webservices, OWASP Schwachstellen*
  - *Cloud: Prüft die Konfiguration von Cloudanwendungen wie Salesforce und Cloudinstanzen wie AWS und Rackspace*
  - *Compliance: Sorgt für die Einhaltung behördlicher, regulatorischer und betrieblicher Vorschriften*
  - *Sorgt für die Einhaltung verschiedener PCI DSS-Anforderungen durch Konfigurationsüberwachung und Webanwendungsprüfung*
- *Bedrohungen: Prüft auf Botnets/böswillige Prozesse/Viren*
  - *Erkennt Viren, Malware, Backdoors, mit Botnet-infizierten Systemen kommunizierende*
  - *Hosts, bekannte/unbekannte Prozesse, mit böswilligen Inhalten verknüpfte Webservices*
  - *Compliance-Überwachung: FFIEC, FISMA, CyberScope, GLBA, HIPAA/ HITECH, NERC, PCI, SCAP, SOX*
  - *Konfigurationsüberwachung: CERT, CIS, COBIT/ITIL, DISA STIGs, FDCC, ISO, NIST, NSA*
- *Steuersystemüberwachung: SCADA-Systeme, eingebettete Geräte und ICS-Anwendungen*
- *Überwachung sensibler Inhalte: PII (z. B Kreditkartennummern, SSN)*

Bereitstellung und Management

- *Flexible Bereitstellung: Software, Hardware und virtuelle Appliance können vor Ort oder in der Cloud eines Serviceproviders bereitgestellt werden*
- *Scanoptionen: Unterstützt sowohl nicht-authentifizierte Remote-Prüfungen als auch authentifizierte lokale Prüfungen für umfassendere und genauere Analyse von Online-, Offline- und Remote-Beständen*
- *Konfiguration/Richtlinien: Vorkonfigurierte Richtlinien und Konfigurationsvorlagen*
- *Risikoeinstufungen: CVSS-basierte Gefährdungseinstufung, fünf Schweregrade (Kritisch, Hoch, Mittel, Gering, Info), anpassbare Schweregrade für Neubewertung von Risiken*
- *Priorisierung: Verknüpfung mit Exploit-Frameworks (Metasploit, Core Impact, Canvas und ExploitHub) und Filterung nach Ausnutzbarkeit und Schweregrad*
- *Erweiterbar: RESTful API-Unterstützung für die Integration von Nessus in bestehende Vulnerability Management-Arbeitsabläufe*

Training

Tenable bietet Schulungen für Anwender, die noch nicht mit Nessus gearbeitet haben und die für die optimale Nutzung des Produkts benötigten Kenntnisse und Fähigkeiten erwerben möchten, sowie spezielle Seminare zu Themen wie Compliance-Überwachung für erfahrenere Anwender. Die Kurse können bei Bedarf auf der Tenable-Website abgerufen werden.

Mit Nessus einen Schritt weiter gehen

Für Organisationen, die teamorientiertes Vulnerability Management umsetzen möchten, stehen die folgenden Nessus-Lösungen zur Verfügung:

Nessus Manager
Nessus Manager bietet Zusammenarbeit und zentralisierte Administration über mehrere Scanner hinweg. Binden Sie System- und Netzwerkadministratoren, Forensik- und Response-Teams, Risiko & Compliance sowie Desktop-Support in den Vulnerability Management-Prozess ein. Das branchenweit meistgenutzte Gefährdungs- und Konfigurationsbewertungsprodukt bietet nun auch rollenbasierte gemeinsame Nutzung von Scannern, Richtlinien, Zeitplänen und Prüfergebnissen durch Nutzergruppen beliebiger Größe.

Nessus Cloud
Die von Tenable gehostete Version von Nessus Manager bietet Nessus-Prüffunktionen, gemeinsame Nutzung von Ressourcen und rollenbasierte Zugriffssteuerung für mehrere Nutzer in einer cloudbasierten Lösung. Nessus Cloud kann auch zur Einhaltung der PCI-Vorgaben für die Netzwerkprüfung verwendet werden. Nessus Cloud ist eine PCI-zertifizierte Approved Scanning Vendor (ASV)-Lösung. Beginnen Sie jetzt mit der Prüfung Ihrer Netzwerkumgebung!

Der Nessus-Vorteil

Kunden wählen Nessus aus gutem Grund:

- Höchst präzise Prüfung mit wenigen Fehlmeldungen
- Umfassende Scanfunktionen und Leistungsmerkmale
- Skalierbar für Hunderttausende von Systemen
- Mühelose Bereitstellung und einfaches Management
- Geringe Administrations- und Betriebskosten

tenable®

Weitere Informationen: Besuchen Sie tenable.com
Kontakt: Schreiben Sie an subscriptionsales@tenable.com , oder besuchen Sie tenable.com/contact