tenable

Nessus NP™ Professional

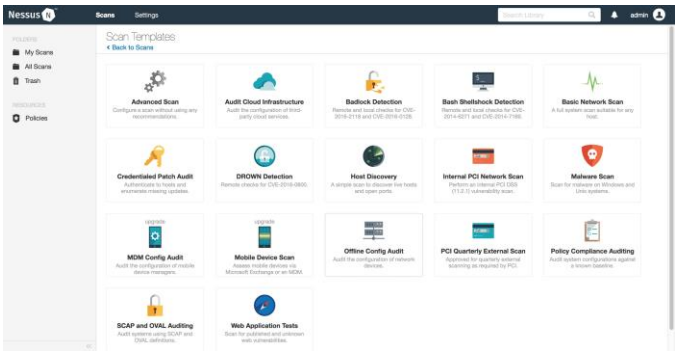
Nessus has been deployed by more than one million users across the globe for vulnerability, configuration and compliance assessments

Nessus Professional Vulnerability Scanner

Consultants and organizations around the world use Nessus® Professional to reduce their IT attack surface and ensure compliance. Nessus features high-speed asset discovery, configuration auditing, target profiling, malware detection, sensitive data discovery and more.

Nessus supports more technologies than competitive solutions, scanning operating systems, network devices, next generation firewalls, hypervisors, databases, web servers and critical infrastructure for vulnerabilities, threats and compliance violations.

With the world's largest continuously updated library of vulnerability and configuration checks, and the support of Tenable's expert vulnerability research team, Nessus sets the standard for vulnerability scanning speed and accuracy.



Complete Vulnerability Coverage

- Software flaws
- Malware & botnets
- Configuration auditing
- Physical, virtual and cloud coverage

Use Nessus Professional in your Consulting Practice

- ***Unlimited assessments:*** No limit to the number of IPs you scan or the number of assessments you run
- **Easily transferable license:** Quickly and easily transfer your license between computers
- ***Reporting***: Email a report to your customer once the scan is complete and add your name and logo to reports
- ***Use with popular penetration testing tools:*** Correlate scan data with exploit frameworks such as Metasploit, Core Impact, Canvas and ExploitHub

Nessus Features

Reporting

- Customize reports to sort by vulnerability or host, create an executive summary or compare scan results to highlight changes
  - Native (XML), PDF (requires Java be installed on Nessus server), HTML and CSV formats
- Add your own name and/or logo to reports
- Targeted email notifications of scan results, remediation recommendations and scan configuration improvements
- Automate report downloads using the API

Scanning Capabilities

- Discovery: Accurate, high-speed asset discovery
- Scanning: Vulnerability scanning (including IPv4/IPv6/hybrid networks)
  - Un-credentialed vulnerability discovery
  - Credentialed scanning for system hardening and missing patches
  - Meets PCI DSS requirements for internal vulnerability scanning
- Coverage: Broad asset coverage and profiling
  - Network devices: firewalls/routers/switches (Juniper, Check Point, Cisco, Palo Alto Networks), printers, storage
  - Offline configuration auditing of network devices

- Virtualization VMware ESX, ESXi, vSphere, vCenter, Microsoft, Hyper-V, Citrix Xen Server
- Operating systems: Windows, OS X, Linux, Solaris, FreeBSD, Cisco iOS, IBM iSeries
- Databases: Oracle, SQL Server, MySQL, DB2, Informix/DRDA, PostgreSQL, MongoDB
- Cloud: Scans the configuration of cloud applications like Salesforce and cloud instances like Amazon Web Services, Microsoft Azure and Rackspace
- Compliance: Helps meet government, regulatory and corporate scanning requirements
- Helps to enforce PCI DSS requirements for secure configuration, system hardening, malware detection, and access controls

- Threats: Botnet/malicious, process/anti-virus auditing
  - Detect viruses, malware, backdoors, hosts communicating with botnet-infected systems, known/unknown processes, web services linking to malicious content
  - Compliance auditing: FFIEC, FISMA, CyberScope, GLBA, HIPAA/ HITECH, NERC, SCAP, SOX
  - Configuration auditing: CERT, CIS, COBIT/ITIL, DISA STIGs, FDCC, ISO, NIST, NSA, PCI
- Control Systems Auditing: SCADA systems, embedded devices and ICS applications
- Sensitive Content Auditing: PII (e.g., credit card numbers, SSNs)

The Nessus Advantage

Customers choose Nessus because it is:

- ***Easy-to-use***: Policy creation is simple and only requires a few clicks to scan an entire corporate network
- ***Comprehensive***: Supports more technologies and identifies more vulnerabilities than competitive solutions
- ***Low cost***: Vulnerability scanning in a low total cost of ownership (TCO) product
- ***Fast and accurate***: High-speed accurate scanning with low false positives
- ***Timely protection***: Tenable researchers quickly deliver plug-ins to identify the latest vulnerabilities and threats
- ***Scalable***: Move to Tenable.io or other Tenable solutions as your vulnerability management needs increase

Deployment and Management

- Flexible deployment: software or virtual appliance deployed on-premises or in a service provider's cloud.
- Flexible licensing: Easily transfer a Nessus license across multiple laptops to support pools of consultants and/or laptops.
- Scan options: Supports both non-credentialed, remote scans and credentialed, local scans for deeper, granular analysis of assets that are online as well as offline or remote.
- Configuration/policies: Out-of-the-box policies and configuration templates.
- Risk scores: Vulnerability ranking based on CVSS, five severity levels (Critical, High, Medium, Low, Info), customizable severity levels for recasting of risk.
- Prioritization: Correlation with exploit frameworks (Metasploit, Core Impact, Canvas and ExploitHub) and filtering by exploitability and severity.

Training

Tenable offers training for those who are new to using Nessus and want the knowledge and skills to maximize use of the product, as well as focused topics like compliance auditing for more advanced users. Courses are available on-demand via the Tenable website.

tenable™

For More Information: Please visit tenable.com
Contact Us: Please email us at subscriptionsales@tenable.com or visit tenable.com/contact

Copyright 2017 Tenable, Inc. All rights reserved. Tenable Network Security, Nessus, SecurityCenter, SecurityCenter Continuous View and Log Correlation Engine are registered trademarks of Tenable, Inc. Tenable, Tenable.io, Assure, and The Cyber Exposure Company are trademarks of Tenable, Inc. All other products or services are trademarks of their respective owners.
EN-DEC07-2017-V8