tenable network security

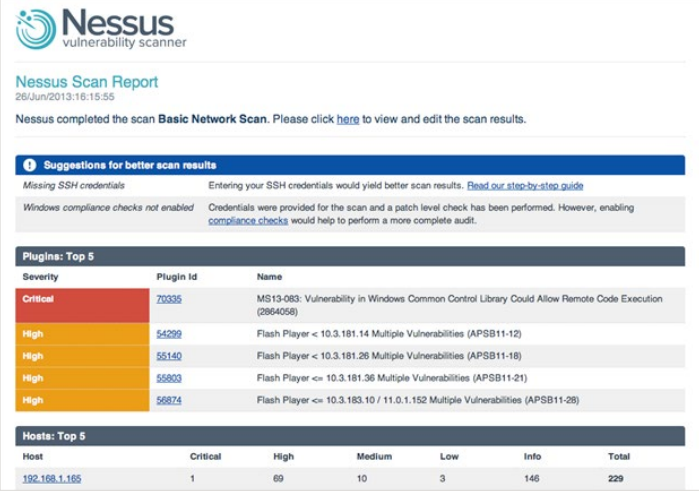
Nessus®

The World's Most Trusted Vulnerability Scanner

Product Overview

Nessus® is the industry's most widely-deployed vulnerability, configuration, and compliance assessment product. Nessus features high-speed discovery, configuration auditing, asset profiling, sensitive data discovery, patch management integration, and vulnerability analysis. With a continuously-updated library of more than 60,000 vulnerability and configuration checks (plugins) and the support of Tenable's expert vulnerability research team, Nessus delivers accuracy to the marketplace. Nessus scales to serve the largest organizations and is quick-and-easy to deploy.

With more than 20,000 customers worldwide, Nessus is trusted by more professionals than any other security and compliance product.



Nessus vulnerability scanner

Nessus Scan Report
26/Jun/2013:16:15:55

Nessus completed the scan **Basic Network Scan**. Please click here to view and edit the scan results.

Suggestions for better scan results

Missing SSH credentials	Entering your SSH credentials would yield better scan results. Read our step-by-step guide
Windows compliance checks not enabled	Credentials were provided for the scan and a patch level check has been performed. However, enabling compliance checks would help to perform a more complete audit.

Plugins: Top 5

Severity	Plugin Id	Name
Critical	70335	MS13-083: Vulnerability in Windows Common Control Library Could Allow Remote Code Execution (2864058)
High	54299	Flash Player < 10.3.181.14 Multiple Vulnerabilities (APSB11-12)
High	55140	Flash Player < 10.3.181.26 Multiple Vulnerabilities (APSB11-18)
High	55803	Flash Player <= 10.3.181.36 Multiple Vulnerabilities (APSB11-21)
High	56874	Flash Player <= 10.3.183.10 / 11.0.1.152 Multiple Vulnerabilities (APSB11-28)

Hosts: Top 5

Host	Critical	High	Medium	Low	Info	Total
192.168.1.165	1	69	10	3	146	229

Targeted Nessus email notifications provide an overview of the scan results, remediation recommendations, and suggestions to improve future scans

Nessus Features

Scanning Capabilities

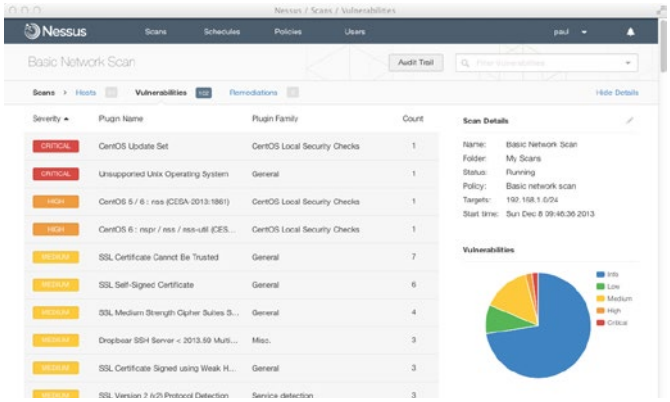
- Accurate, high-speed asset discovery
- Compliance auditing: FFIEC, FISMA, CyberScope Reporting Protocol, GLBA, HIPAA/HITECH, NERC, PCI, SCAP, SOX
- Configuration auditing: CERT, CIS, COBIT/ITIL, DISA STIGs, FDCC, IBM iSeries, ISO, NIST, NSA
- Patch auditing: Includes patch management integration with IBM® TEM for Patch Management, Microsoft® SCCM and WSUS, Red Hat® Network Satellite Server, and VMware® Go
- Control systems auditing: SCADA systems, devices, and applications
- Sensitive content auditing: PII (credit card numbers, SSNs) and intellectual property
- Mobile device auditing: Lists iOS, Android™, and Windows Phone 7 devices accessing the network and detects mobile vulnerabilities
- Vulnerability scanning for:
  - Network devices: Juniper, Cisco, Palo Alto Networks, firewalls, printers, and more
  - Virtual hosts: VMware ESX, ESXi, vSphere, vCenter
  - Operating systems: Windows, Mac, Linux, Solaris, BSD, Cisco iOS, IBM iSeries
  - Databases: Oracle, SQL Server, MySQL, DB2, Informix/DRDA, PostgreSQL
  - Web applications: Web servers, web services, OWASP vulnerabilities
  - Compromise detection: Viruses, malware, backdoors, hosts communicating with botnet-infected systems, web services linking to malicious content
  - IPv4/IPv6/hybrid networks
- Credentialed scanning detects local vulnerabilities and conditions
- Uncredentialed network-based scanning finds new hosts and vulnerabilities

Key Benefits

- Easy customization for your organization
  - Flexible deployment, scanning, and reporting
  - Targeted email notifications of scan results and remediation recommendations
  - Vulnerability modifications
- Rapid, comprehensive security assessment
  - Identify patch status conflicts between Nessus and patch management systems, or among deployed patch managers
  - Consolidated list of patches to apply to become fully patched
- Lower your cyber risks, vulnerabilities, and compliance/audit citation risks
  - Automatic post-scan analysis with attachments stored in scan reports
- Low total cost of ownership (TCO)
  - Scan unlimited number of IPs, as often as you like
  - Nessus subscriptions include software updates, access to compliance and audit files, and support
  - Automatic plugin updates
- Anytime, anywhere access from any Internet browser for improved efficiency

Deployment and Management

- Flexible deployment: Software application, hardware and virtual appliances (including Nessus AMI for Amazon Web Services (AWS) cloud), or as service
- Agentless scanner for easy deployment and maintenance
- Browser-based installation wizard
- Configuration and management via Nessus GUI
  - Easily create policies using a variety of wizards
  - Schedule scans to run once or on recurring basis
- Five criticality levels: Critical Risk, High Risk, Medium Risk, Low Risk, Informational



Nessus provides convenient access to scan details to assist with vulnerability investigations.

Reporting and Monitoring

- Flexible reporting: Customize reports to sort by vulnerability or host, create an Executive Summary, or compare scan reports to highlight changes
  - Native (XML), PDF (requires Oracle Java be installed on Nessus server), CSV, and HTML formats
- Targeted email notifications of scan results, remediation recommendations, and scan improvements

Nessus Deployment Options

Nessus: Software-based Nessus scanner which is licensed per installation. Each active Nessus scanner requires a feed subscription which includes: Unlimited IP scanning for internal and external IPs, access to all plugins and audit policies, free software/plugin updates, and support.

Nessus Perimeter Service™ with Tenable PCI Scanning Service: Software-as-a-service Nessus scanner which can be used to audit Internet-facing IPs for network and web application vulnerabilities and validate PCI Approved Scanning Vendor (ASV) compliance. Nessus Perimeter Service is licensed per end user, and the subscription includes: Unlimited IP scanning for external IPs, Tenable PCI Scanning Service, access to all plugins and audit policies, free plugin updates, and support.

Nessus Auditor Bundles

Nessus training and certification are available for those who are new to using Nessus and want the knowledge and skills to maximize every benefit of the Nessus scanner. Tenable has assembled several Nessus Auditor Bundles which combine subscriptions for Nessus, Nessus Perimeter Service, or both subscriptions, with Nessus On Demand Training and a Certification Exam at a significant cost savings over purchasing these items separately.

Complementary Tenable Products

Organizations can extend the capabilities of Nessus with complementary products from Tenable.

- Tenable Passive Vulnerability Scanner™ (PVS™): Continuously monitors for vulnerabilities and new or transient assets. Analyzes network traffic for insight into services, suspicious network relationships, and compliance violations. Available as a subscription or as part of SecurityCenter CV.
- Tenable SecurityCenter™: Accelerates and simplifies vulnerability and compliance management, with a single console managing distributed Nessus scans and providing advanced analytics and dashboards.
- Tenable SecurityCenter Continuous View: A unique combination of active Nessus scanning, passive PVS detection, and log analysis that discovers and classifies IT assets across the enterprise.

The Nessus Advantage

There are many vulnerability scanners on the market, but millions choose Nessus because it offers:

- Highly-accurate scanning with low false positives
- Comprehensive scanning capabilities and features
- Scalable to hundreds-of-thousands of systems
- Easy deployment and maintenance
- Low cost to administer and operate

For More Information

Questions, purchasing, or evaluation:
subscriptionsales@tenable.com or 443-545-2103
Twitter: @TenableSecurity
YouTube: youtube.com/tenablesecurity
Tenable Blog: blog.tenable.com
Tenable Discussions: discussions.nessus.org
www.tenable.com

tenable™ network security