

PRODUCT OVERVIEW

TENABLE Network Security's active vulnerability scanner, Nessus, is the world-leader in active scanners, featuring high speed discovery, asset profiling and vulnerability analysis of your security posture. Nessus scanners can be distributed throughout an entire enterprise, inside DMZs and across physically separate networks. They can also be made available for ad-hoc scanning, daily scans and quick-response audits. When managed with TENABLE's Security Center, vulnerability recommendations can be sent to the responsible parties, remediation can be tracked and security patches can be managed directly from the Security Center's web interface. Nessus is supported by a world renowned Research Team and has the largest vulnerability knowledge base, making it suitable for even the most complex environments.

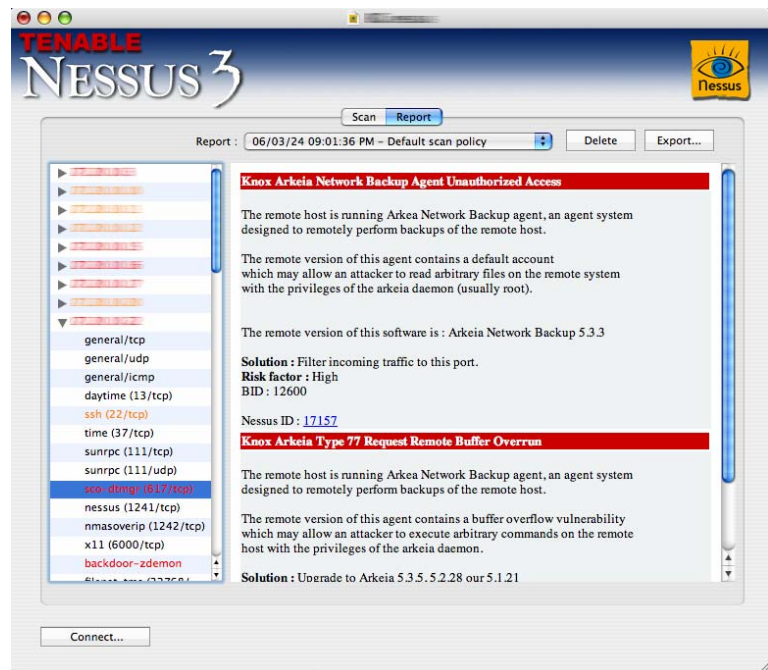


"Nessus is the most widely supported vulnerability scanner in the world as far as we know. With about 13,000 individual vulnerability checks, Nessus draws heavily on the open source community."

The Nessus documentation is very good and there are lots of additional documents available from non-Tenable sources."



"Audit is the driving force behind Tenable's architecture. Tenable's products can be used to audit the compliance of systems against technical security requirements (specific configurations)."
BURTON GROUP



ORGANIZATIONAL BENEFITS

- Nessus is highly accurate, providing the most comprehensive vulnerability assessment to expedite remediation, decrease exposure time and provide audit data for compliance reporting
- TENABLE's Research Team delivers the most timely and thorough checks to your organization, saving time and resources needed to identify new vulnerabilities by your staff
- Nessus is in use by the majority of Fortune 1000 companies, so you can have confidence to deploy Nessus scanners throughout your organization
- TENABLE Network Security offers a "direct feed" of updated vulnerability data, as well as annual support contracts, classroom and web-based training to insure your security team is armed with the most current information
- When managed by TENABLE's Security Center, Nessus can be used to produce compliance reports (SOX, FISMA, .etc) as well as configuration audits of key servers
- Nessus can discover sensitive data when doing credentialed scans to allow you to prioritize security efforts.

FEATURES—Nessus

Complete Assessment and Discovery

Nessus performs sophisticated remote scans and audits of UNIX, Windows and network infrastructures. Nessus discovers networked devices and identifies the operating systems, applications, databases and services running on those assets. Any non-compliant hosts, such as systems running P2P, spyware or malware (worms, Trojans, etc.) are detected and identified. Nessus is capable of scanning all ports on every device, test for open ports and issue remediation strategy suggestions as required. Unlike many other security scanners, it does not make assumptions regarding port use but will detect and test independently. Once the devices are profiled and baselined, subsequent scans can determine any changes to those devices. Nessus provides the data ability to accurately identify inventory and system level configurations. The data, when managed by TENABLE's Security Center, provides system audit reports for regulatory compliance.

High Speed Vulnerability Identification

Nessus performs high speed vulnerability identification on the assets you choose to scan. Nessus scanners can be distributed throughout the enterprise to put the power of Nessus in the hands of the responsible parties. They can be configured to test a range of IP addresses or for MAC addresses if IPs are variable. Nessus can continuously scan your network devices to drastically save time identifying vulnerabilities as they arise. Nessus can scan the systems without needing administrative credentials, but can also test using exploit techniques as required. If credentials are provided during the audit, Nessus can determine an exact list of missing patches and misconfigurations.

Agentless Scanning

Nessus does not require deployment of agents on the target systems. This allows you to rapidly deploy the scanners, eliminates the need for agent patching, and creates a flexible environment that is not dependent on target-specific agents.

Real-time Vulnerability Research

The TENABLE Research Team is comprised of industry experts in vulnerability detection and remediation. Through established relationships with major vendors, this team often supports their efforts directly. The vulnerability knowledge base is updated daily so that the most current checks are available to your organization.

Enterprise Management & Reporting

When used with TENABLE's Security Center, an organization can manage all Nessus scanners within the enterprise. TENABLE's Security Center load balances the scan workload to provide fast completion times. When using multiple scanners, the scan time scan is reduced significantly allowing network audits to be conducted on a more frequent basis. Remediation efforts can be tracked through TENABLE's Security Center.

Commercial Support

TENABLE's Nessus can be deployed with confidence throughout your organization. Support services include a "direct feed" of the latest vulnerability data, keeping the vulnerability checks up to date automatically. Additionally, access to customer support resources is available. Classroom training is offered on a monthly schedule to assure your staff is always current, even if you experience turnovers. If travel is not possible, web-based weekly training sessions are available. Additionally, professional services can be engaged for custom plugins or for deployment assistance.

SUPPORTED PLATFORMS

Operating Systems:

RedHat Enterprise 3
RedHat Enterprise 4
SuSe v9.3
SuSe 10
Fedora v4
Debian v3.1
FreeBSD v5 & 6

Windows 2000, XP, Server 2003

OS X



"Tenable's endpoint compliance checks are similar to credentialed vulnerability scanning in that they also require credentials, but the goal isn't to find vulnerabilities. Vulnerabilities tend to be cut-and-dry; you're vulnerable or you're not. Compliance is trickier. Every environment has slightly different requirements, which increasingly are dictated by laws like HIPAA and GLB. While one organization may require passwords be eight characters long, another may require 16 characters. Neither is right or wrong; they're just different. Endpoint compliance checks validate the settings (such as registry keys, file permissions and particular security settings) for each host against a site's unique policy."

TENABLE Network Security, Inc.
7063 Columbia Gateway Dr.
Suite 100
Columbia, MD 21046
TEL: 1-410-872-0555
www.tenablesecurity.com