What is NESSUS and How Does it Work?

Nessus is a proprietary vulnerability scanner developed by Tenable, Inc. Tenable.io is a subscription-based service. Tenable also contains what was previously known as Nessus Cloud, which used to be Tenable's Software-as-a-Service solution. Nessus is an open-source network vulnerability scanner that uses the Common Vulnerabilities and Exposures architecture for easy cross-linking between compliant security tools. In fact, Nessus is one of the many vulnerability scanners used during vulnerability assessments and penetration testing engagements, including malicious attacks. Nessus is a tool that checks computers to find vulnerabilities that hackers COULD exploit.

Nessus works by testing each port on a computer, determining what service it is running, and then testing this service to make sure there are no vulnerabilities in it that could be used by a hacker to carry out a malicious attack.

Nessus can scan these vulnerabilities and exposures:

- Vulnerabilities that could allow unauthorized control or access to sensitive data on a system
- Misconfiguration (e.g. open mail relay)
- Denials of service (Dos) vulnerabilities
- Default passwords, a few common passwords, and blank/absent passwords on some system accounts

Software flaws, missing patches, malware and misconfiguration errors across a wide range of operating systems, devices and applications are dealt with by Nessus.

The Nessus server is currently available for:

- Unix
- Linux
- FreeBSD

Also, the client is available for:

- Unix-based operating systems
- Windows-based operating systems

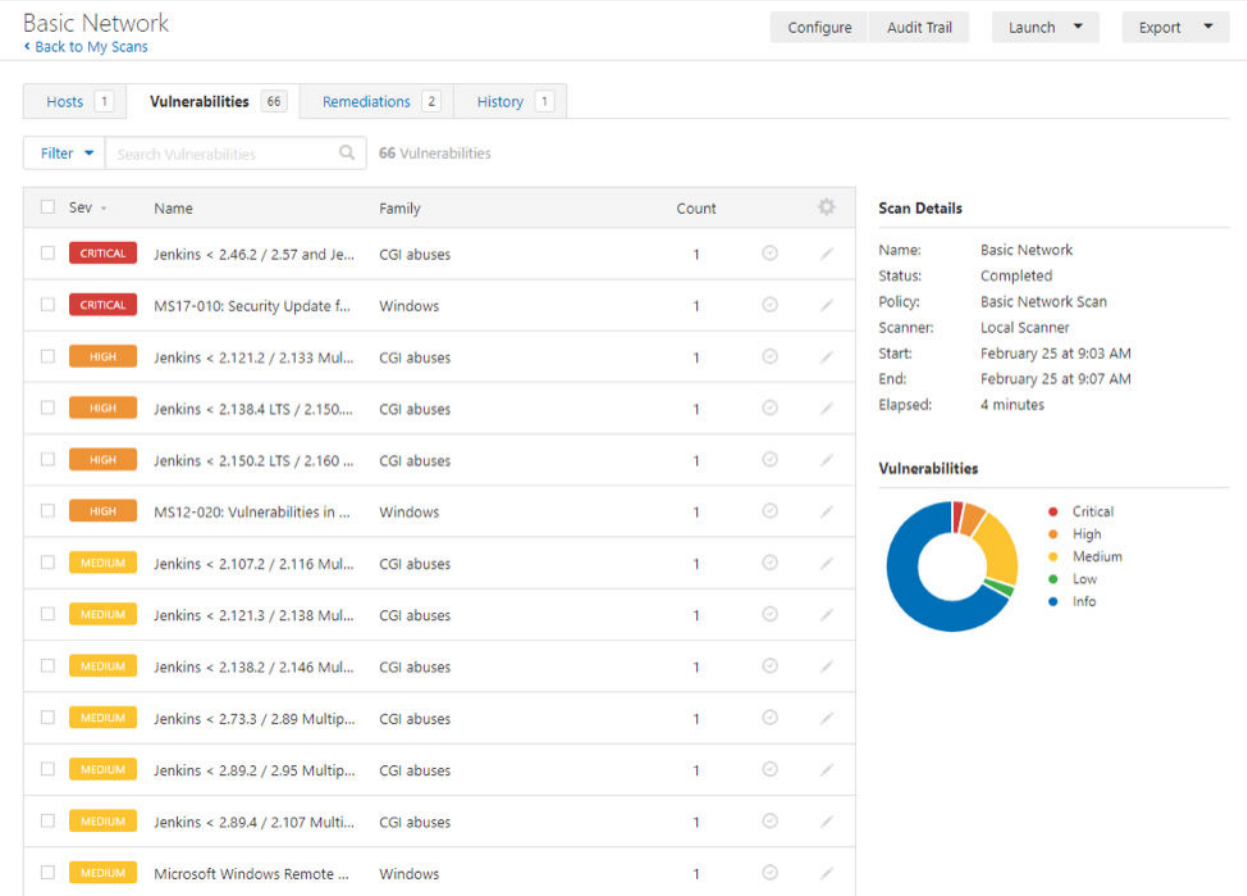
Significant capabilities of Nessus include:

- Scheduled security audits
- Detection of security holes in local or remote hosts
- Simulated attacks to pinpoint vulnerabilities
- Detection of missing security updates and patches

- Nessus Professional perform internal network scans as required by the PCI DSS 11.2.1 requirement.

The results of the scan can be reported in various formats, such as plain text, XML, and HTML.

You cannot use Nessus on a system with a Host-based Intrusion Prevention System (HIPS) installed. Because during the process of scanning a remote target, Nessus must forge TCP/UDP packets and send probes that are often considered “malicious” by HIPS software. If the HIPS system is configured to block malicious traffic, it will interfere with Nessus and cause the scan results to be incomplete or unreliable.



Source: Tenable.com

Nessus Features

- Vulnerability Scanning
- Asset Discovery
- Network Scanning

- Vulnerability Assessment
- Prioritization
- Policy Management
- Web Scanning

What is Nessues Agent?

Nessus Agents provide a flexible way of scanning hosts within your environment without necessarily having to provide credentials to hosts. The agents enable scans to be carried out even when the hosts are offline.

Nessus Agents provide a subset of the coverage in a traditional network scan:

- Scanning of transient endpoints that are not always connected to the local network.
- Scanning assets for which you do not have credentials or could not easily obtain credentials.
- Improving overall scan performance: With agents, the network scan can be reduced to just remote network checks, speeding scan completion time.

Nessus Agents currently support a variety of operating systems including:

- Windows Server 2008 and 2012, and Windows 7 and 8
- Amazon Linux
- CentOS
- Debian Linux
- OS X
- Red Hat Enterprise Linux
- Ubuntu Linux

Versions and Licensing

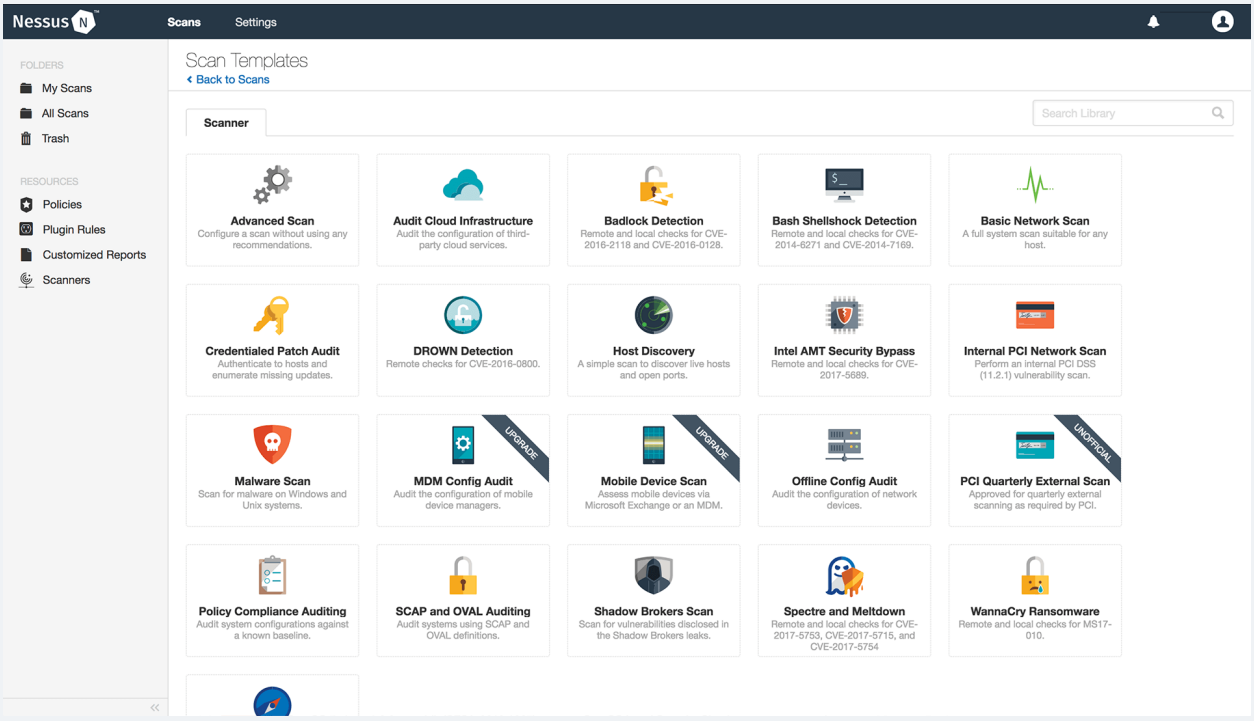
Nessues includes two versions:

- **Nessus Professional**: This version is ideal for consultants, pen testers and security practitioners. With the ability to scan unlimited IPs, a use anywhere, and advanced features such as configuration assessment, Live Results and custom

reporting. Anyway, the IP addresses or hosts that you are scanning from must be licensed. This version does not support Mobile Device Management (MDM).
- **Nessus® Essentials**: This version is free to use to scan any environment, but limited to 16 IP addresses per scanner.

Other advantages and features of the professional version include:

- Advanced Detection Means More Protection
- Plugins Provide Timely Protection
- Accommodate Growth and Scale Safely
- Cost Effective for Companies of All Sizes
- Accurate Visibility into Your Networks



Source: Tenable.com

Vulnerability Scanning with Nessus

Nessus performs its scans by utilizing plugins, which run against each host on the network in order to identify vulnerabilities. For instance, a plugin could be launched and targeted at a host to:

- Identify which operating systems and services are running on which ports

- Identify which software components are vulnerable to attacks (FTP, SSH, SMB and more)

The steps that are followed during scanning are:

- Define scan parameters
- Create scan
- Launch scan
- Analyze scan results

Once all the steps are complete, Nessus runs each host against a database of known vulnerabilities in an attempt to discover which host contains which vulnerabilities.

Ports can be defined in ranges or individually, with valid ports ranging from 1 to 65535.

Nessus gives you the ability to configure your scan based on different scan and policy templates. These templates will determine the settings that will be found within the scan policy settings:

- **Basic**: With this setting, you can specify security-related and organizational aspects of the scan or policy, such as name of the scan, the targets of the scan, whether or not it is scheduled and who has access to it.
- **Discovery**: For defining the ports to be scanned and the methods to be used while conducting this discovery.
- **Assessment**: This setting allows you to determine the type of vulnerability scan to perform and how they are performed.
- **Report**: For determining how scan reports are generated and the information that should be included within them.
- **Advanced**: Here you will define scan efficiency and the operations that the scan should perform.