

Nessus

Vulnerability Scanner

Deepak Rawat

March/2024



Nessus is a renowned vulnerability scanner developed by **Tenable, Inc.** It plays a crucial role in identifying security weaknesses within IT infrastructures. Here are the key points to get you started:

1. **Purpose and Functionality:**

- Nessus scans target networks to uncover vulnerabilities such as software bugs, backdoors, and other potential security risks.
- It helps security professionals assess the security posture of systems, networks, and applications.

2. **Features and Capabilities:**

- **High-Speed Asset Discovery:** Nessus rapidly identifies devices and services on your network.
- **Target Profiling:** Understands the characteristics of each target system.
- **Configuration Auditing:** Assesses system configurations against best practices.
- **Malware Detection:** Identifies signs of malicious activity.
- **Sensitive Data Discovery:** Locates sensitive information.
- And much more!

3. **Licensing Options:**

- **Nessus Essentials:** The free version allows scanning up to 16 IPs.
- **Tenable.io:** A subscription-based service for enterprise use. It facilitates sharing scanners, schedules, and scan results among teams.
- **Nessus Agents:** Flexible scanning without host credentials, even when hosts are offline.
- **Nessus Professional:** Widely deployed across industries for vulnerability assessment.
- **Nessus Manager** (no longer sold): Previously used for collaboration and monitoring assets.

4. **Community-Driven Optimization:**

- Tenable continuously refines Nessus based on community feedback.
- It remains one of the most accurate and comprehensive vulnerability assessment solutions available.

Installation:

Install Tenable Nessus on Linux

Caution: If you install a Nessus Agent, Manager, or Scanner on a system with an existing Nessus Agent, Manager, or Scanner running `nessusd`, the installation process will kill all other `nessusd` processes. You may lose scan data as a result.

Note: Tenable Nessus does not support using symbolic links for `/opt/nessus/`.

To install Nessus on Linux:

1. [Download](#) the Tenable Nessus package file.
2. From the command line, run the Tenable Nessus installation command specific to your operating system.

Example Tenable Nessus install commands:

- **Debian/Kali and Ubuntu**

```
# dpkg -i Nessus-<version number>-debian6_amd64.deb
```

- **FreeBSD**

```
# pkg add Nessus-<version number>-fbsd10-amd64.txz
```

- **Red Hat**

```
# yum install Nessus-<version number>-es6.x86_64.rpm
```

- **SUSE**

```
# sudo zypper install Nessus-<version number>-suse12.x86_64.rpm
```

3. From the command line, restart the `nessusd` daemon.

Example Tenable Nessus daemon start commands:

- **CentOS, Debian/Kali, Fedora, Oracle Linux, Red Hat, SUSE, and Ubuntu**

```
# systemctl start nessusd
```

- **FreeBSD**

```
# service nessusd start
```

4. Open Tenable Nessus in your browser.
 - To access a remotely installed Tenable Nessus instance, go to `https://<remote IP address>:8834` (for example, `https://111.49.7.180:8834`).
 - To access a locally installed Tenable Nessus instance, go to `https://localhost:8834`.

5. Perform the remaining [Tenable Nessus installation steps](#) in your browser.

Install Tenable Nessus on Windows

Caution: If you install a Nessus Agent, Manager, or Scanner on a system with an existing Nessus Agent, Manager, or Scanner running `nessusd`, the installation process will kill all other `nessusd` processes. You may lose scan data as a result.

Note: Tenable Nessus does not support using symbolic links for `/opt/nessus/`.

Note: You may be required to restart your computer to complete installation.

Download Nessus Package File

Download Tenable Nessus from the [Tenable Downloads site](#).

Start Nessus Installation

1. Navigate to the folder where you downloaded the Nessus installer.
2. Next, double-click the file name to start the installation process.

Complete the Windows InstallShield Wizard

1. First, the **Welcome to the InstallShield Wizard for Tenable, Inc. Nessus** screen appears. Select **Next** to continue.
2. On the **License Agreement** screen, read the terms of the Tenable, Inc. Nessus software license and subscription agreement.
3. Select the **I accept the terms of the license agreement** option, and then click **Next**.
4. On the **Destination Folder** screen, select the **Next** button to accept the default installation folder. Otherwise, select the **Change** button to install Nessus to a different folder.
5. On the **Ready to Install the Program** screen, select the **Install** button.

The **Installing Tenable, Inc. Nessus** screen appears and a **Status** indication bar shows the installation progress. The process may take several minutes.

After the **InstallShield Wizard** completes, the **Welcome to Nessus** page loads in your default browser.

If the page does not load, do one of the following steps to open Tenable Nessus in your browser.

- To access a remotely installed Nessus instance, go to `https://<remote IP address>:8834` (for example, `https://111.49.7.180:8834`).
- To access a locally installed Nessus instance, go to `https://localhost:8834`.

Install Tenable Nessus on macOS

Caution: If you install a Nessus Agent, Manager, or Scanner on a system with an existing Nessus Agent, Manager, or Scanner running `nessusd`, the installation process will kill all other `nessusd` processes. You may lose scan data as a result.

Note: Tenable Nessus does not support using symbolic links for `/opt/nessus/`.

Download Tenable Nessus Package File

[Download](#) the Tenable Nessus package file.

To install Nessus with the GUI installation package:

Extract the Nessus Files

Double-click the `Nessus-<version number>.dmg` file.

Start Nessus Installation

Double-click **Install Nessus.pkg**.

Complete the Tenable, Inc. Nessus Server Install

When the installation begins, the **Install Tenable, Inc. Nessus Server** screen appears and provides an interactive navigation menu.

Introduction

The **Welcome to the Tenable, Inc. Nessus Server Installer** window provides general information about the Nessus installation.

1. Read the installer information.
2. To begin, select the **Continue** button.

License

1. On the **Software License Agreement** screen, read the terms of the **Tenable, Inc.** Nessus software license and subscription agreement.
2. **OPTIONAL:** To retain a copy of the license agreement, select **Print** or **Save**.
3. Next, select the **Continue** button.
4. To continue installing Nessus, select the **Agree** button, otherwise, select the **Disagree** button to quit and exit.

Installation Type

On the **Standard Install on <DriveName>** screen, choose one of the following options:

- Select the **Change Install Location** button.
- Select the **Install** button to continue using the default installation location.

Installation

When the **Preparing for installation** screen appears, you are prompted for a username and password.

1. Enter the **Name** and **Password** of an administrator account or the root user account.
2. On the **Ready to Install the Program** screen, select the **Install** button.

Next, the **Installing Tenable, Inc. Nessus** screen appears and shows a **Status** indication bar for the remaining installation progress. The process may take several minutes.

Summary

1. When the installation is complete, the **The installation was successful** screen appears. After the installation completes, select **Close**.
2. Open Tenable Nessus in your browser.
 - To access a remotely installed Nessus instance, go to `https://<remote IP address>:8834` (for example, `https://111.49.7.180:8834`).
 - To access a locally installed Nessus instance, go to `https://localhost:8834`.
3. Perform the remaining [Nessus installation steps](#) in your browser.

To install Nessus from the command line:

1. Open Terminal.
2. Run the following commands in the listed order:
 - a. `sudo hdiutil attach <Nessus .dmg package>`
 - b. `sudo installer -package /Volumes/Nessus\ Install/Install\ Nessus.pkg -target /`
 - c. `sudo hdiutil detach /Volumes/Nessus\ Install`
3. Open Tenable Nessus in your browser.
 - To access a remotely installed Nessus instance, go to `https://<remote IP address>:8834` (for example, `https://111.49.7.180:8834`).
 - To access a locally installed Nessus instance, go to `https://localhost:8834`.
4. Perform the remaining [Nessus installation steps](#) in your browser.

Install Tenable Nessus on Raspberry Pi

Tenable Nessus 10.0.0 and later supports scanning on the Raspberry Pi 4 Model B with a minimum of 8GB memory.

1. Download the Tenable Nessus Raspberry Pi OS package file from the [Tenable Downloads site](#).
2. From a command prompt or terminal window, run the Tenable Nessus installation command:

```
dpkg -i Nessus-<version>-raspberrypios_armhf.deb
```

3. From a command prompt or terminal window, start the nessusd daemon by running the following command:

```
/bin/systemctl start nessusd.service
```

4. Open Tenable Nessus in your browser.
 - To access a remotely installed Tenable Nessus instance, go to `https://<remote IP address>:8834` (for example, `https://111.49.7.180:8834`).
 - To access a locally installed Tenable Nessus instance, go to `https://localhost:8834`.
5. Perform the remaining [Tenable Nessus installation steps](#) in your browser.

Deploy Tenable Nessus as a Docker Image

You can deploy a managed Tenable Nessus scanner or an instance of Tenable Nessus Professional as a Docker image to run on a container. Tenable provides two base Tenable Nessus images: Oracle Linux 8 and Ubuntu. You can configure the Tenable Nessus instance with environment variables to configure the image with the settings you configure automatically. Using operators and variables, you can deploy the Tenable Nessus image as linked to Tenable Vulnerability Management or Tenable Security Center.

Tenable does not recommend deploying Tenable Nessus in a Docker container that shares a network interface controller (NIC) with another Docker container.

Note: Tenable Nessus does not support storage volumes. Therefore, if you deploy a new Tenable Nessus image, you will lose your data and need to reconfigure Tenable Nessus. However, while deploying the new image, you can configure any initial user and linking information with environment variables, as described in step 2 of the following procedure.

Before you begin:

- Download and install Docker for your operating system.

- Access the Tenable Nessus Docker image from <https://hub.docker.com/r/tenable/nessus>.

To deploy Tenable Nessus as a Docker image:

1. In your terminal, use the docker pull command to get the image.

```
$ docker pull tenable/nessus:<version-OS>
```

For the *<version-OS>* tag, you must specify the Tenable Nessus version and whether you are pulling Oracle Linux 8 or Ubuntu. You can use the latest tag in place of a specific Tenable Nessus version (for example, latest-ubuntu).

2. Use the docker run command to run your image.
 - Use the operators with the appropriate options for your deployment, as described in [Operators](#).
 - To preconfigure Tenable Nessus, use the -e operator to set environment variables, as described in [Environment Variables](#).

Note: Tenable recommends using environment variables to configure your instance of Tenable Nessus when you run the image. If you do not include environment variables such as an activation code, username, password, or linking key (if creating a managed Tenable Nessus scanner), you must configure those items later.

3. If you did not include environment variables, complete any remaining configuration steps in the command-line interface or Tenable Nessus configuration wizard.

To stop and remove Tenable Nessus as a Docker image:

- To stop and remove the container, see [Remove Tenable Nessus as a Docker Container](#).

How To: Run Your First Vulnerability Scan with Nessus

Get your Nessus vulnerability assessment tool up and running with these five easy steps.



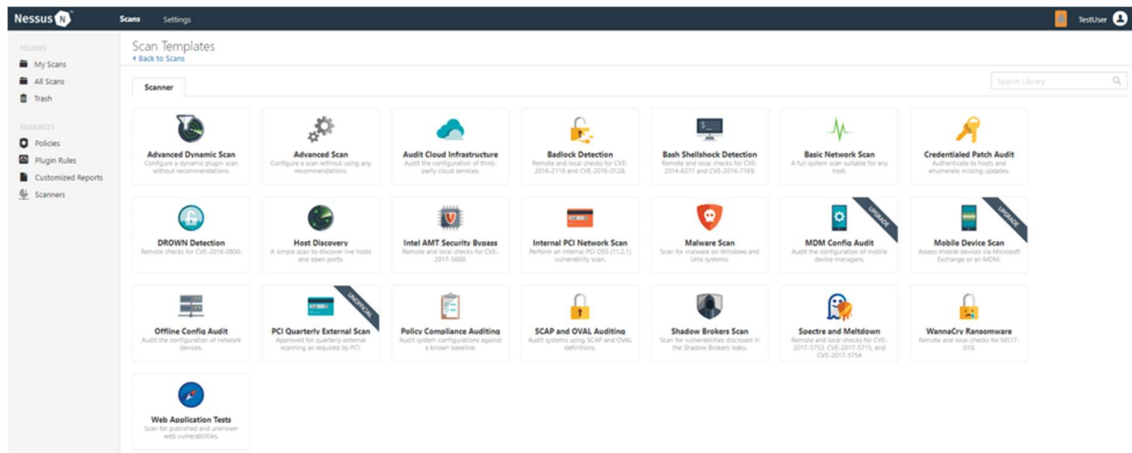
With Nessus, you can gain full visibility into your network by conducting a vulnerability assessment. Read on as we guide you through the five steps to run your first Nessus scan. (If you have not yet installed Nessus, please click [here](#) to see the installation guide.)

Step 1: Creating a Scan

Once you have installed and launched Nessus, you're ready to start scanning. First, you have to create a scan. To create your scan:

- In the top navigation bar, click Scans.
- In the upper-right corner of the My Scans page, click the New Scan button.

Step 2: Choose a Scan Template



Next, click the scan template you want to use. Scan templates simplify the process by determining which settings are configurable and how they can be set. For a detailed explanation of all the options available, refer to [Scan and Policy Settings](#) in the Nessus User Guide.

A scan policy is a set of predefined configuration options related to performing a scan. After you create a policy, you can select it as a template in the User Defined tab when you create a scan. For more information, see [Create a Policy](#) in the Nessus User Guide.

The Nessus interface provides brief explanations of each template in the product. Some templates are only available when you purchase a fully licensed copy of Nessus Professional.

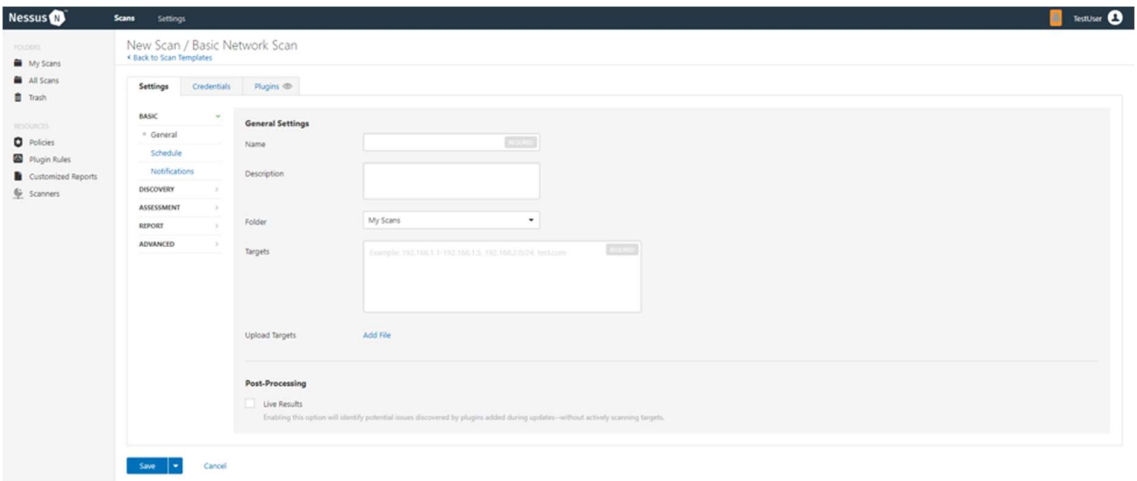
To see a full list of the types of templates available in Nessus, see [Scan and Policy Templates](#). To quickly get started with Nessus, use the Basic Network Scan template.

Step 3: Configure Scan Settings

Prepare your scan by configuring the [settings](#) available for your chosen template. The Basic Network Scan template has several default settings preconfigured, which allows you to quickly perform your first scan and view results without a lot of effort.

Follow these steps to run a basic scan:

1. Configure the settings in the Basic Settings section.



The following are Basic settings:

Setting	Description
Name	Specifies the name of the scan or policy. This value is displayed on the Nessus interface.
Description (Optional)	Specifies a description of the scan or policy.
Folder	Specifies the folder where the scan appears after being saved.
Targets	Specifies one or more targets to be scanned. If you select a target group or upload a targets file, you are not required to specify additional targets.

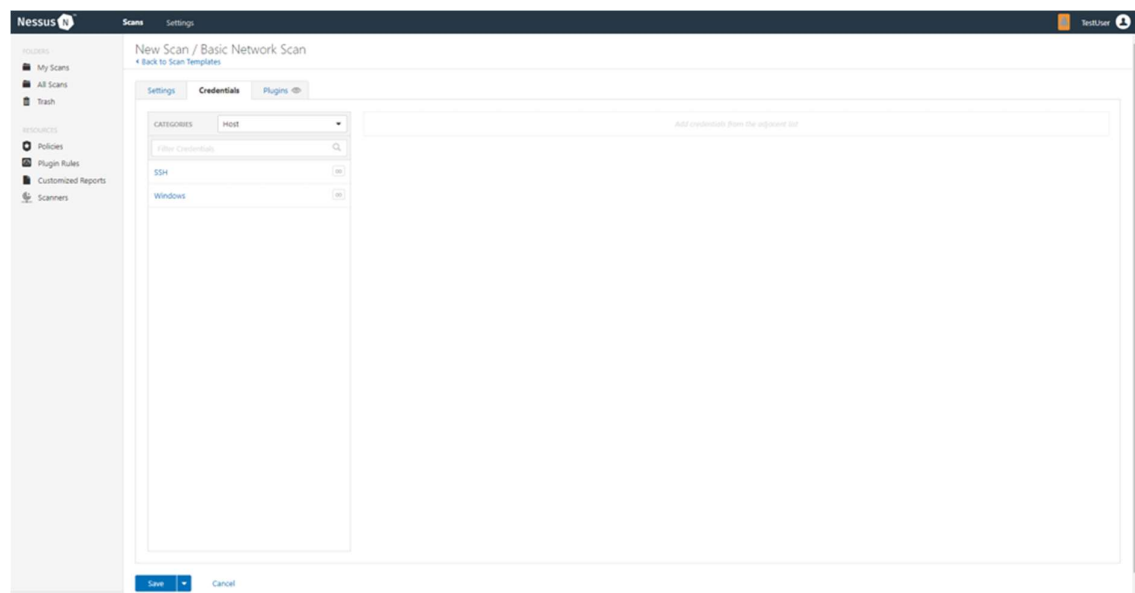
2. Configure remaining settings

Although you can leave the remaining settings at their pre-configured default, Tenable recommends reviewing the Discovery, Assessment, Report and Advanced settings to ensure they are appropriate for your environment.

For more information, see the [Scan Settings](#) documentation in the Nessus User Guide.


3. Configure Credentials

Optionally, you can configure Credentials for a scan. This allows credentialed scans to run, which can provide much more complete results and a more thorough evaluation of the vulnerabilities in your environment.



4. Launch Scan

After you have configured all your settings, you can either click the Save button to launch the scan later, or launch the scan immediately.

If you want to launch the scan immediately, click the  button, and then click Launch. Launching the scan will also save it.

The time it takes to complete a scan involves many factors, such as network speed and congestion, so the scan may take some time to run.

Step 4: Viewing Your Results

Viewing scan results can help you understand your organization's security posture and vulnerabilities. Color-coded indicators and customizable viewing options allow you to tailor how you view your scan's data.

You can view scan results in one of several views:

Page	Description
Hosts	Displays all scanned targets.
Vulnerabilities	List of identified vulnerabilities, sorted by severity.
Remediations	If the scan's results include remediation information, this list displays all remediation details, sorted by the number of vulnerabilities.
Notes	Displays additional information about the scan and the scan's results.
History	Displays a list of scans: Start Time, End Time, and the Scan Statuses.

Viewing scan results by vulnerabilities gives you a view into potential risks on your assets.

Basic Network
← Back to My Scans

ConfigureAudit TrailLaunch▼Export▼

Hosts1Vulnerabilities66Remediations2History1


Filter▼Search Vulnerabilities66 Vulnerabilities

<input type="checkbox"/>	Sev	Name	Family	Count		
<input type="checkbox"/>	CRITICAL	Jenkins < 2.46.2 / 2.57 and Je...	CGI abuses	1	🔄	✎
<input type="checkbox"/>	CRITICAL	MS17-010: Security Update f...	Windows	1	🔄	✎
<input type="checkbox"/>	HIGH	Jenkins < 2.121.2 / 2.133 Mul...	CGI abuses	1	🔄	✎
<input type="checkbox"/>	HIGH	Jenkins < 2.138.4 LTS / 2.150...	CGI abuses	1	🔄	✎
<input type="checkbox"/>	HIGH	Jenkins < 2.150.2 LTS / 2.160 ...	CGI abuses	1	🔄	✎
<input type="checkbox"/>	HIGH	MS12-020: Vulnerabilities in ...	Windows	1	🔄	✎
<input type="checkbox"/>	MEDIUM	Jenkins < 2.107.2 / 2.116 Mul...	CGI abuses	1	🔄	✎
<input type="checkbox"/>	MEDIUM	Jenkins < 2.121.3 / 2.138 Mul...	CGI abuses	1	🔄	✎
<input type="checkbox"/>	MEDIUM	Jenkins < 2.138.2 / 2.146 Mul...	CGI abuses	1	🔄	✎
<input type="checkbox"/>	MEDIUM	Jenkins < 2.73.3 / 2.89 Multip...	CGI abuses	1	🔄	✎
<input type="checkbox"/>	MEDIUM	Jenkins < 2.89.2 / 2.95 Multip...	CGI abuses	1	🔄	✎
<input type="checkbox"/>	MEDIUM	Jenkins < 2.89.4 / 2.107 Multi...	CGI abuses	1	🔄	✎
<input type="checkbox"/>	MEDIUM	Microsoft Windows Remote ...	Windows	1	🔄	✎

Scan Details

Name: Basic Network
Status: Completed
Policy: Basic Network Scan
Scanner: Local Scanner
Start: February 25 at 9:03 AM
End: February 25 at 9:07 AM
Elapsed: 4 minutes

Vulnerabilities



● Critical
● High
● Medium
● Low
● Info

To view vulnerabilities:

1. In the top navigation bar, click Scans.
2. Click the scan for which you want to view results.
3. Do one of the following:
 - Click a specific host to view vulnerabilities found on that host.
 - Click the Vulnerabilities tab to view all vulnerabilities.
4. (Optional) To sort the vulnerabilities, click an attribute in the table header row to sort by that attribute.

5. Clicking on the vulnerability row will open the vulnerability details page, displaying plugin information and output for each instance on a host.

Finance Department Test PCI Scan
CURRENT RESULTS: TODAY AT 9:02 AM

Hosts > Vulnerabilities 27

MEDIUM Microsoft Windows SMB NULL Session Authentication

Description
The remote host is running Microsoft Windows. It is possible to log into it using a NULL session (i.e., with no login or password).
Depending on the configuration, it may be possible for an unauthenticated, remote attacker to leverage this issue to get information about the remote host.

Solution
Apply the following registry changes per the referenced Technet advisories:
Set:
- HKLM\SYSTEM\CurrentControlSet\Control\LSA\RestrictAnonymous=1
- HKLM\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters\restrictnullsessaccess=1
Remove BROWSER from:
- HKLM\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters\NullSessionPipes
Reboot once the registry changes are complete.

See Also
<http://support.microsoft.com/kb/q143474/>
<http://support.microsoft.com/kb/q246261/>
[http://technet.microsoft.com/en-us/library/cc785969\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/cc785969(WS.10).aspx)

Output
It was possible to bind to the \browser pipe

Port Hosts
445 / top / cifs

Plugin Details
Severity: Medium
ID: 26920
Version: \$Revision: 1.30 \$
Type: remote
Family: Windows
Published: 2007/10/04
Modified: 2012/02/29

Risk Information
Risk Factor: Medium
CVSS Base Score: 5.0
CVSS Vector: CVSS2#AV:N/AC:L/Au:N/CP:1/N/A/N
CVSS Temporal Vector: CVSS2#E:U/RL:U/RC:ND
CVSS Temporal Score: 4.3

Vulnerability Information
Exploit Available: false
Exploit Ease: No known exploits are available
Vulnerability Pub Date: 1999/07/14

Reference Information
CVE: CVE-1999-0519, CVE-1999-0520, CVE-2002-1117
OSVDB: 299, 8230
BID: 494

Step 5: Reporting Your Results

Chances are your job isn't done yet. You need to report your findings to your team.

Scan results can be exported in several file formats. Some of these report formats are customizable, while others are designed to be imported into another application or product, such as Microsoft Excel or Tenable.sc. For an explanation of the various report formats and the purpose of each, see the [Nessus User Guide](#).

To Export a Scan Report:

1. Start from a scan's results page
2. In the upper-right corner, click Export.
3. From the drop-down box, select the format in which you want to export the scan results.
4. Click Export to download the report.