INFOSECTRAIN

Educate. Excel. Empower.

Vulnerability Scanning with Nessus

A PRACTICAL GUIDE

Q What is Nessus?

Nessus, developed by Tenable, is a powerful vulnerability scanner trusted by organizations worldwide to identify vulnerabilities in their IT infrastructure. It scans networks, servers, and applications to detect weaknesses that attackers could exploit. Nessus Professional is widely used in enterprise environments, while Nessus Essentials (formerly Nessus Home) is available for personal use, offering limited scanning capabilities for home networks.

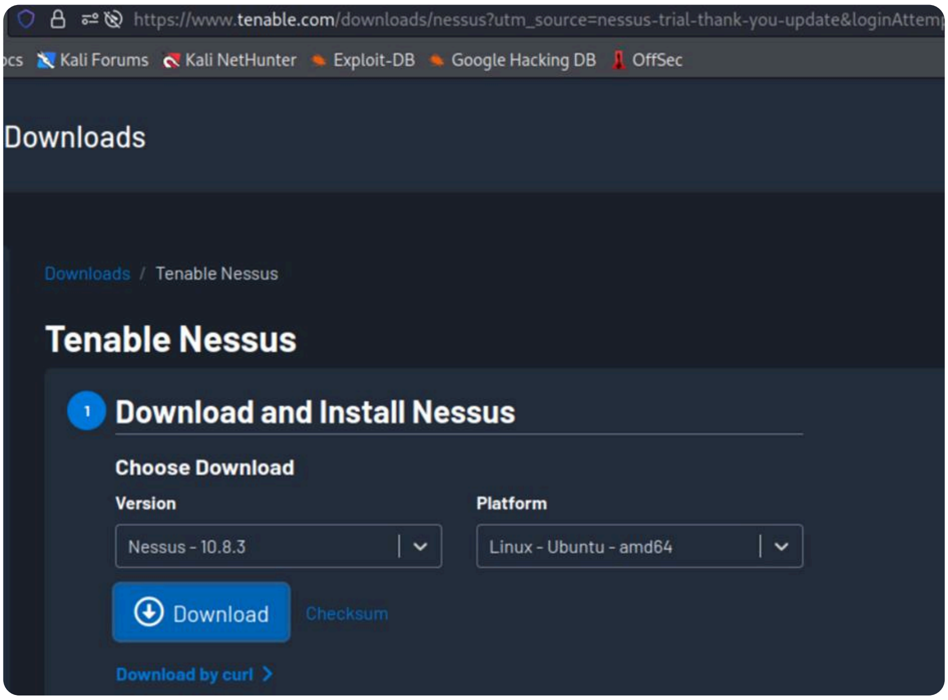
Why Nessus?

The appeal of Nessus lies in its robust scanning engine, ease of use, and comprehensive coverage of vulnerabilities. It has one of the most extensive vulnerability databases, which is regularly updated to include the latest security issues. The scanner is capable of identifying misconfigurations, missing patches, default credentials, and more—making it an invaluable tool for security professionals.

Setting Up Nessus

Download and Install Nessus:

Visit the Tenable website to download the version suitable for your needs—Nessus Professional for business users or Nessus Essentials for home use.



https://www.tenable.com/downloads/nessus?utm_source=nessus-trial-thank-you-update&loginAttem

Downloads

Downloads / Tenable Nessus

Tenable Nessus

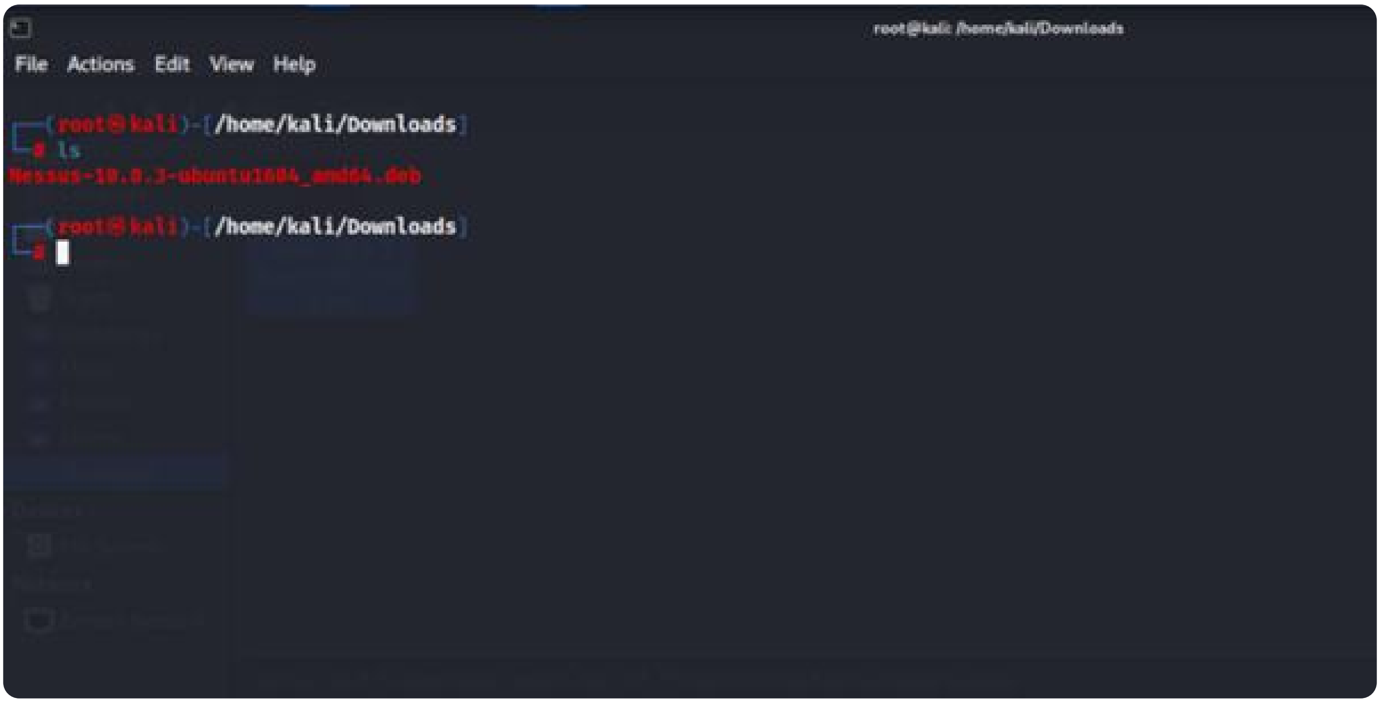
1 Download and Install Nessus

Choose Download

Version: Nessus - 10.8.3

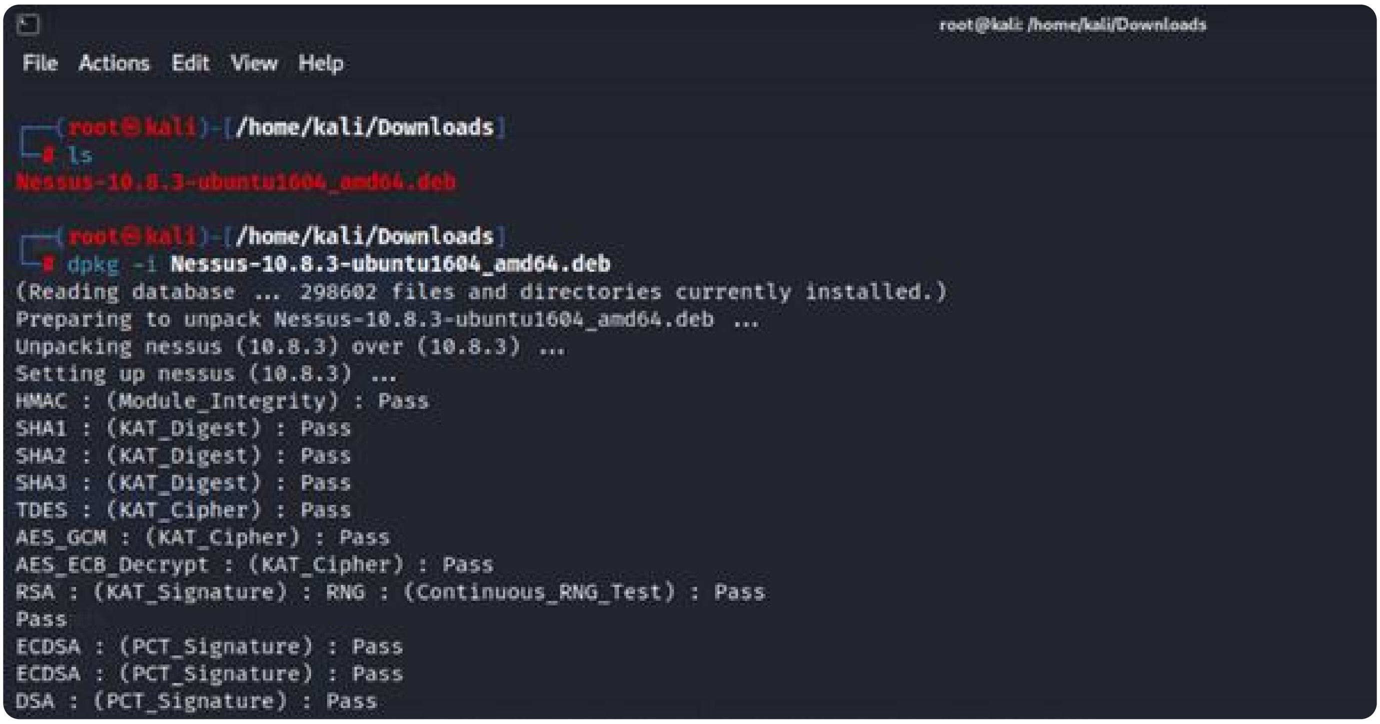
Platform: Linux - Ubuntu - amd64

Installation



```
┌──(root㉿kali)-[/home/kali/Downloads]
└─# ls
Nessus-10.8.3-ubuntu1604_amd64.deb

┌──(root㉿kali)-[/home/kali/Downloads]
└─# █
```

For installation, open the terminal and go to the download directory.

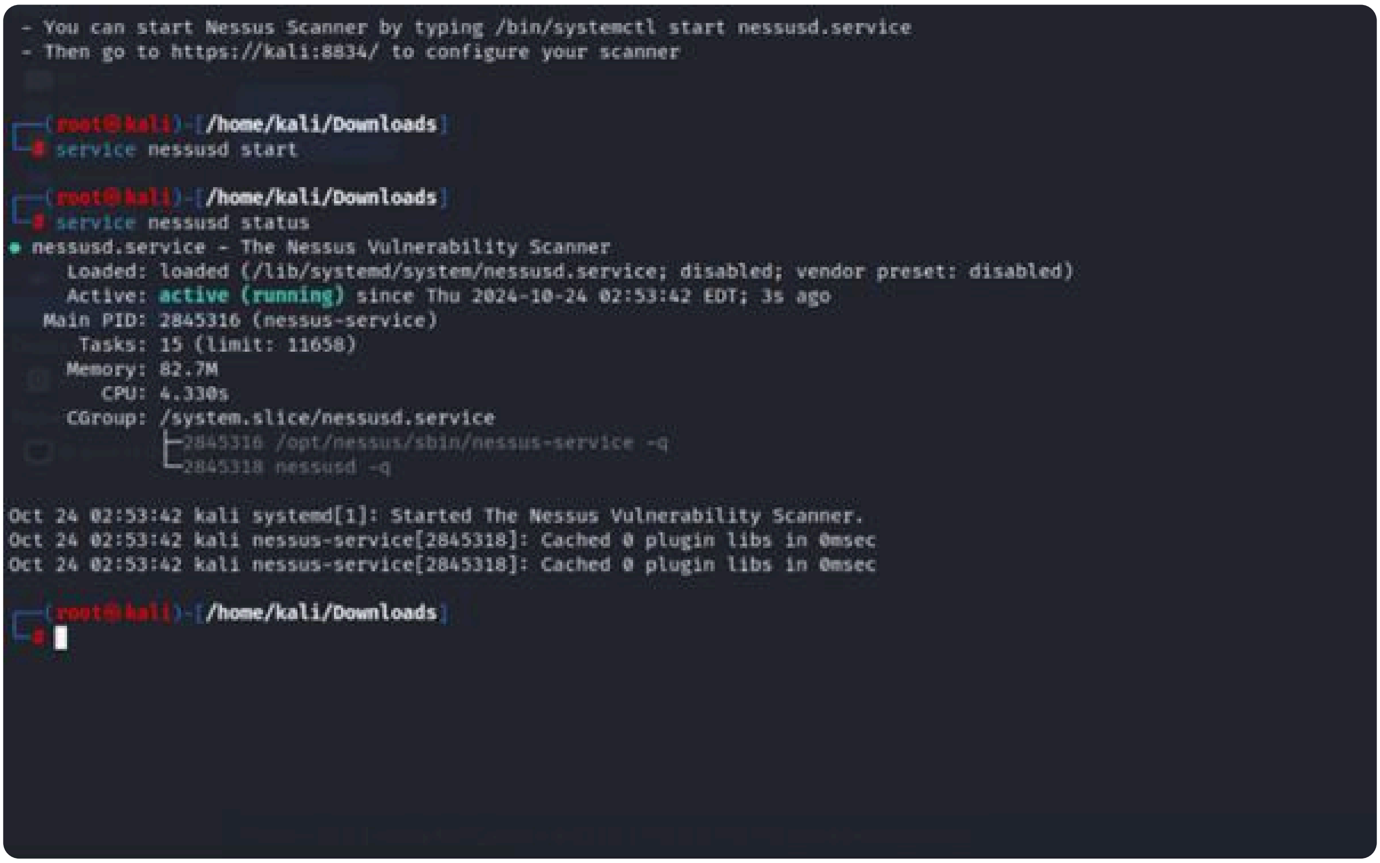


```
┌──(root㉿kali)-[/home/kali/Downloads]
└─# ls
Nessus-10.8.3-ubuntu1604_amd64.deb

┌──(root㉿kali)-[/home/kali/Downloads]
└─# dpkg -i Nessus-10.8.3-ubuntu1604_amd64.deb
(Reading database ... 298602 files and directories currently installed.)
Preparing to unpack Nessus-10.8.3-ubuntu1604_amd64.deb ...
Unpacking nessus (10.8.3) over (10.8.3) ...
Setting up nessus (10.8.3) ...
HMAC : (Module_Integrity) : Pass
SHA1 : (KAT_Digest) : Pass
SHA2 : (KAT_Digest) : Pass
SHA3 : (KAT_Digest) : Pass
TDES : (KAT_Cipher) : Pass
AES_GCM : (KAT_Cipher) : Pass
AES_ECB_Decrypt : (KAT_Cipher) : Pass
RSA : (KAT_Signature) : RNG : (Continuous_RNG_Test) : Pass
Pass
ECDSA : (PCT_Signature) : Pass
ECDSA : (PCT_Signature) : Pass
DSA : (PCT_Signature) : Pass
```

For installation, use the following command :
# dpkg -i Nessus-10.8.3-ubuntu1604_amd64.deb

Start the nessus service-
service nessusd start

And for confirming whether the nessus service has been started or not, we can confirm it with:
service nessusd status



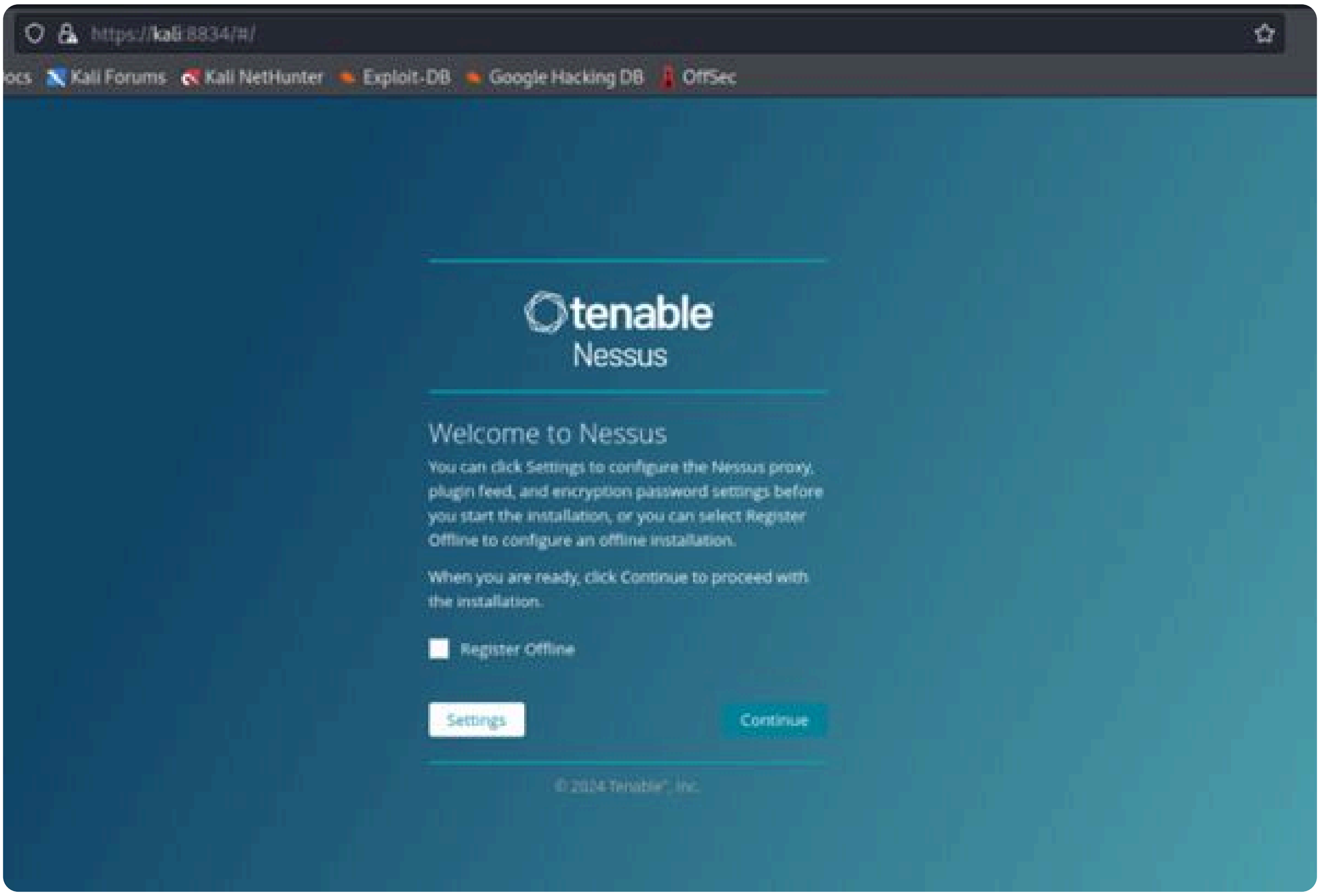
```
- You can start Nessus Scanner by typing /bin/systemctl start nessusd.service
- Then go to https://kali:8834/ to configure your scanner

┌──(root㉿kali)-[/home/kali/Downloads]
└─# service nessusd start

┌──(root㉿kali)-[/home/kali/Downloads]
└─# service nessusd status
● nessusd.service - The Nessus Vulnerability Scanner
     Loaded: loaded (/lib/systemd/system/nessusd.service; disabled; vendor preset: disabled)
     Active: active (running) since Thu 2024-10-24 02:53:42 EDT; 3s ago
   Main PID: 2845316 (nessus-service)
      Tasks: 15 (limit: 11658)
     Memory: 82.7M
        CPU: 4.330s
     CGroup: /system.slice/nessusd.service
             ├─2845316 /opt/nessus/sbin/nessus-service -q
             └─2845318 nessusd -q

Oct 24 02:53:42 kali systemd[1]: Started The Nessus Vulnerability Scanner.
Oct 24 02:53:42 kali nessus-service[2845318]: Cached 0 plugin libs in 0msec
Oct 24 02:53:42 kali nessus-service[2845318]: Cached 0 plugin libs in 0msec

┌──(root㉿kali)-[/home/kali/Downloads]
└─# 
```

Activate Your License:

you’ll need to activate your license. Nessus Essentials requires a free license key, while Nessus Professional comes with a paid license and a free trial of 7 days.

Configuration by using the command

```
#service nessusd start
#service nessusd status
```



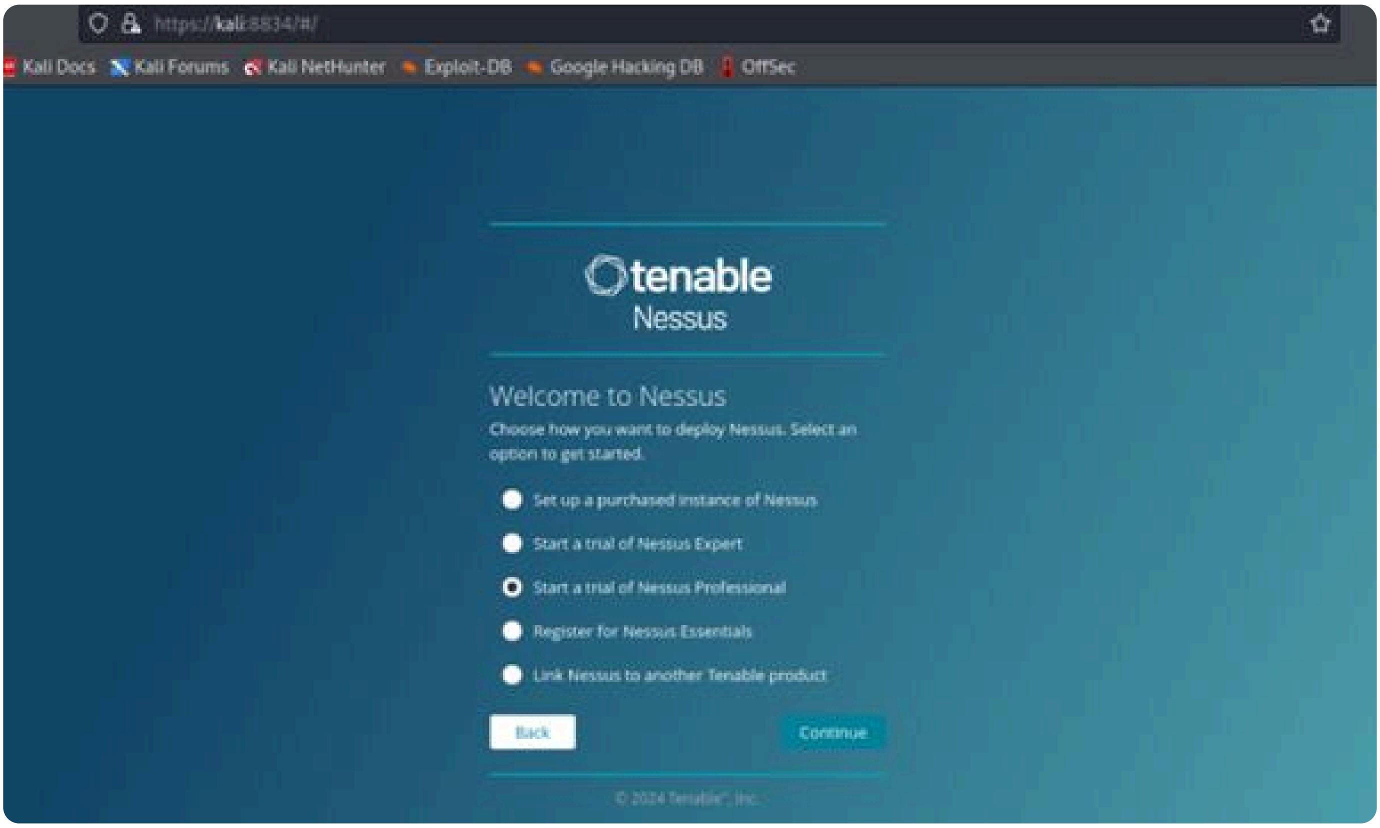
Welcome to Nessus

You can click Settings to configure the Nessus proxy, plugin feed, and encryption password settings before you start the installation, or you can select Register Offline to configure an offline installation.

When you are ready, click Continue to proceed with the installation.

□ Register Offline

For setup, click on the checkbox register offline and then continue

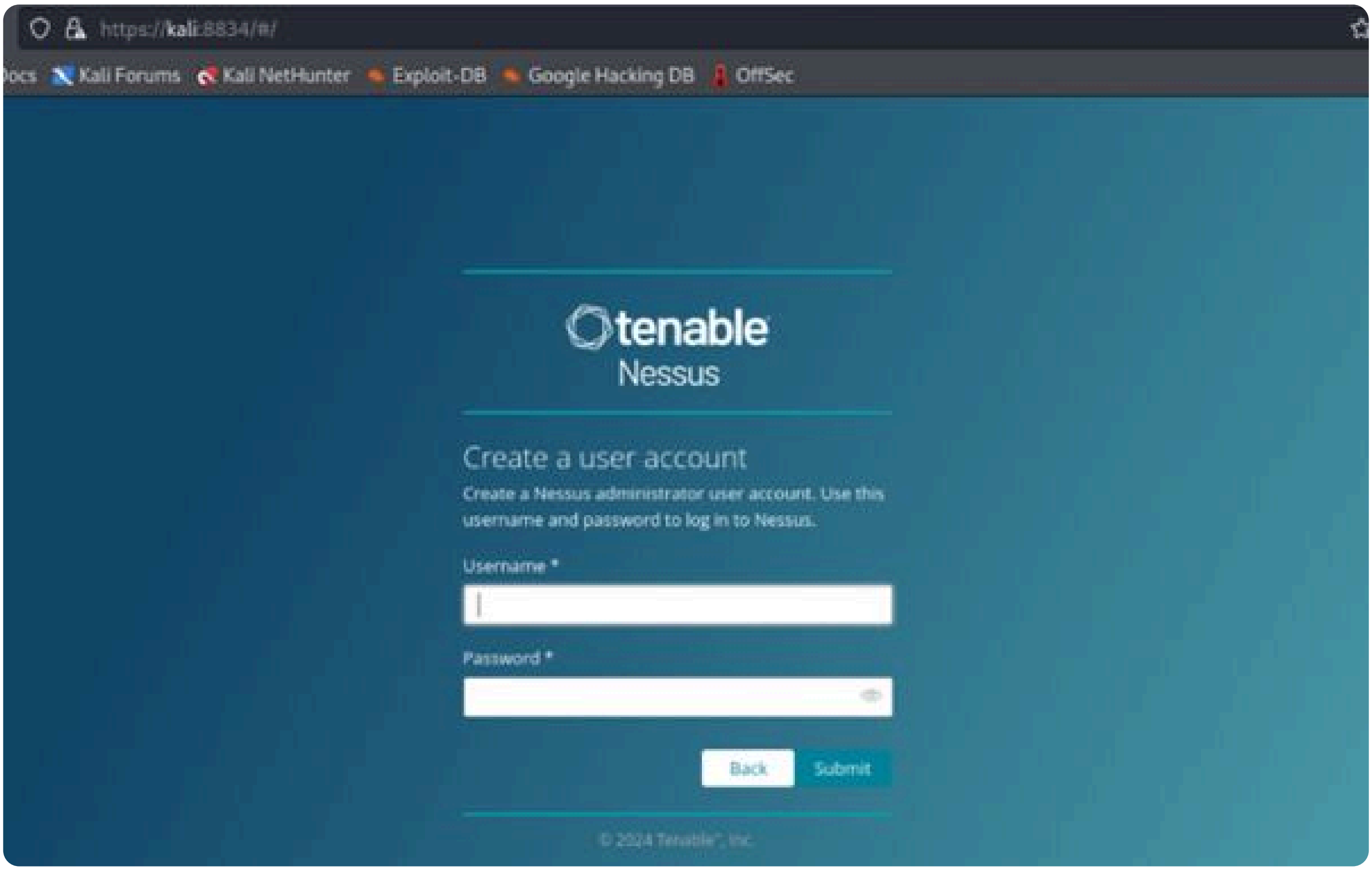


Welcome to Nessus

Choose how you want to deploy Nessus. Select an option to get started.

- ○ Set up a purchased instance of Nessus
- ○ Start a trial of Nessus Expert
- ● Start a trial of Nessus Professional
- ○ Register for Nessus Essentials
- ○ Link Nessus to another Tenable product

© 2024 Tenable®, Inc.



Create a user account

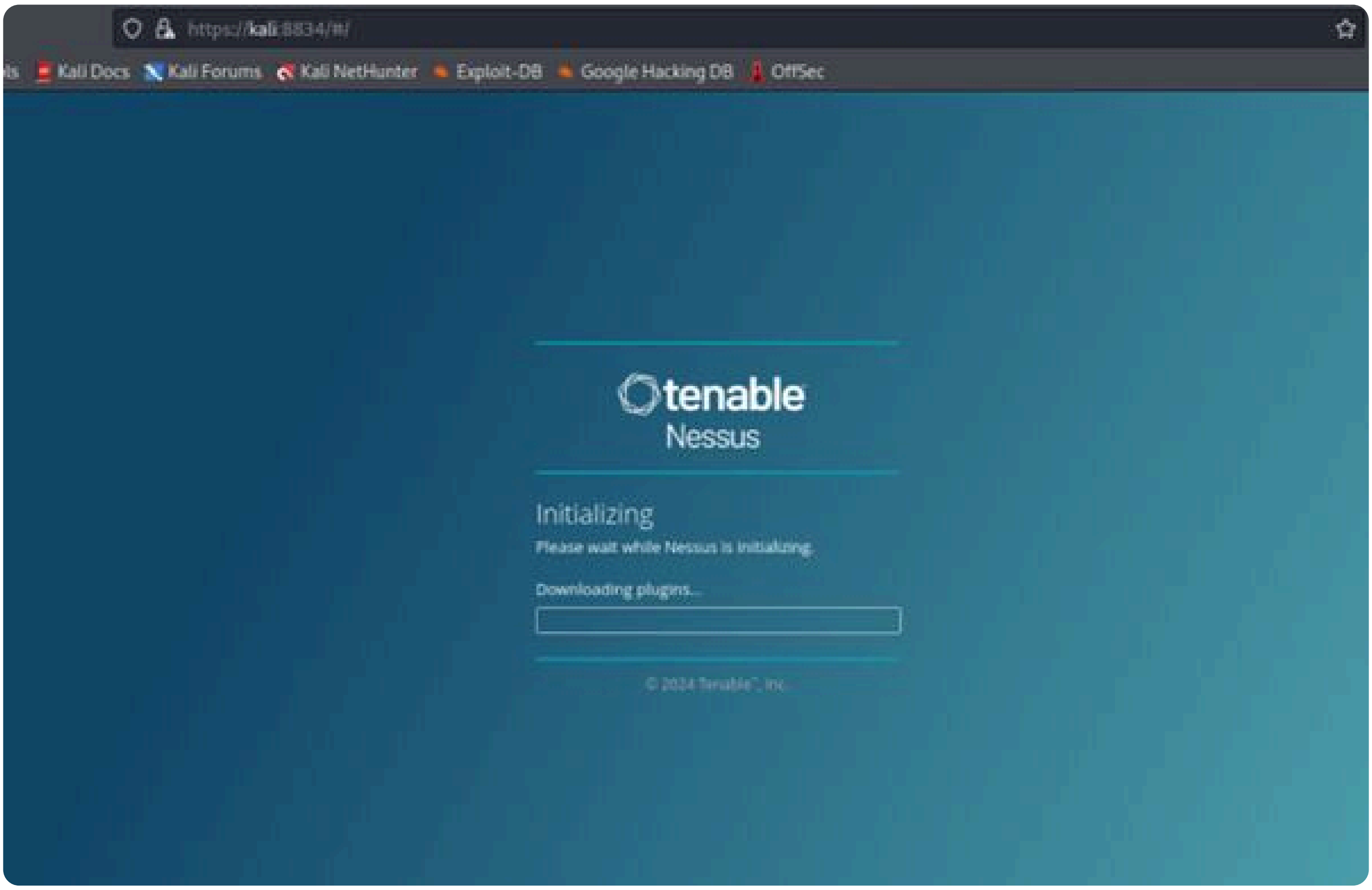
Create a Nessus administrator user account. Use this username and password to log in to Nessus.

Username *

Password *

© 2024 Tenable®, Inc.

Create new user account by giving user id and password



Initializing

Please wait while Nessus is initializing.

Downloading plugins...

© 2024 Tenable™, Inc.

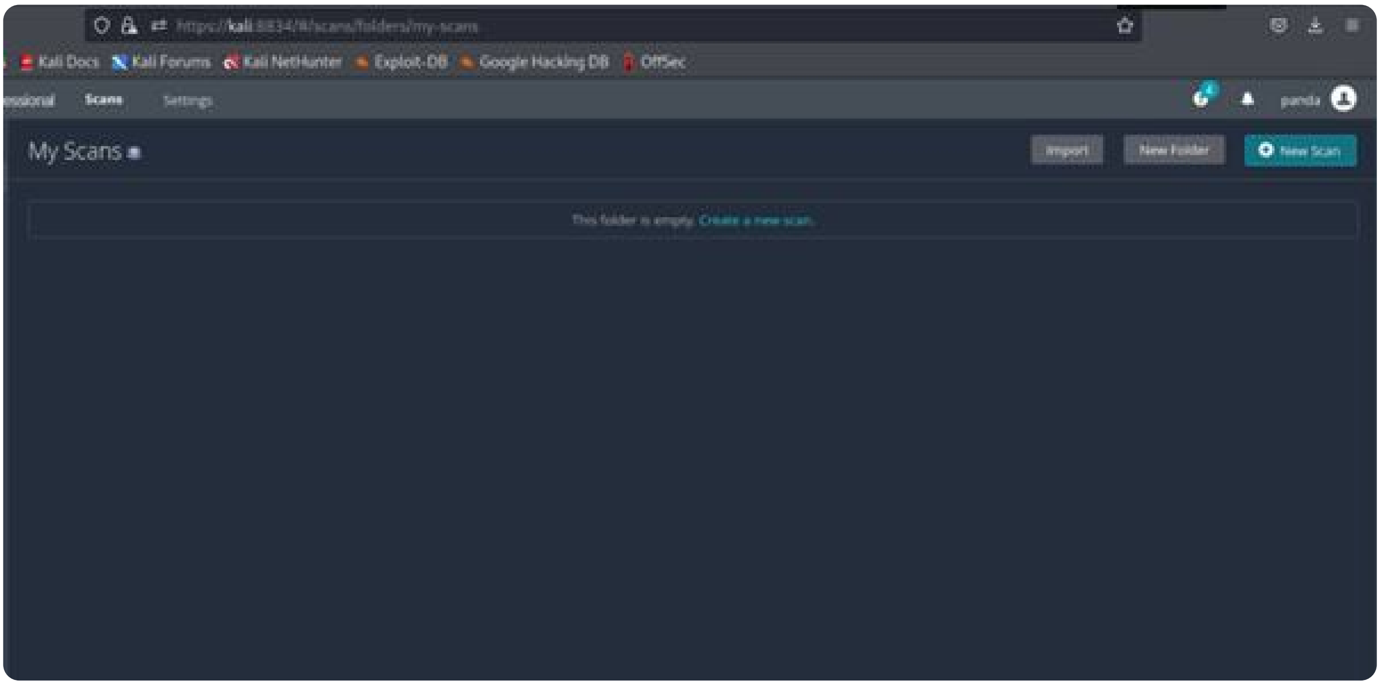
Set Up the Scanner:

Once Nessus is installed, you will be prompted to configure the scanner. You can choose from various scan types depending on your objectives (e.g., vulnerability assessment, compliance scans, or custom configurations).

1 Performing a Vulnerability Scan with Nessus

To start using Nessus Professional, you'll need to access the Nessus Professional dashboard through your web browser. By default, the Nessus Professional service runs on port 8834, so you can access it using the following URL:

```
https://localhost:8834/
```



https://kali:8834/#/scans/folders/my-scans

My Scans

This folder is empty. Create a new scan.

Log in with your Nessus Professional credentials to access the dashboard.

2 Create a New Scan

Once you're logged in, click on the “**New Scan**” button to initiate a scan. Nessus Professional offers several templates to choose from, depending on your requirements:

- **Basic Network Scan:** A general vulnerability scan for networks.
- **Advanced Scan:** Provides detailed control over scan parameters.
- **Web Application Test:** Designed to identify vulnerabilities in web applications.

For our example, let's assume you want to perform a **Basic Network Scan.**

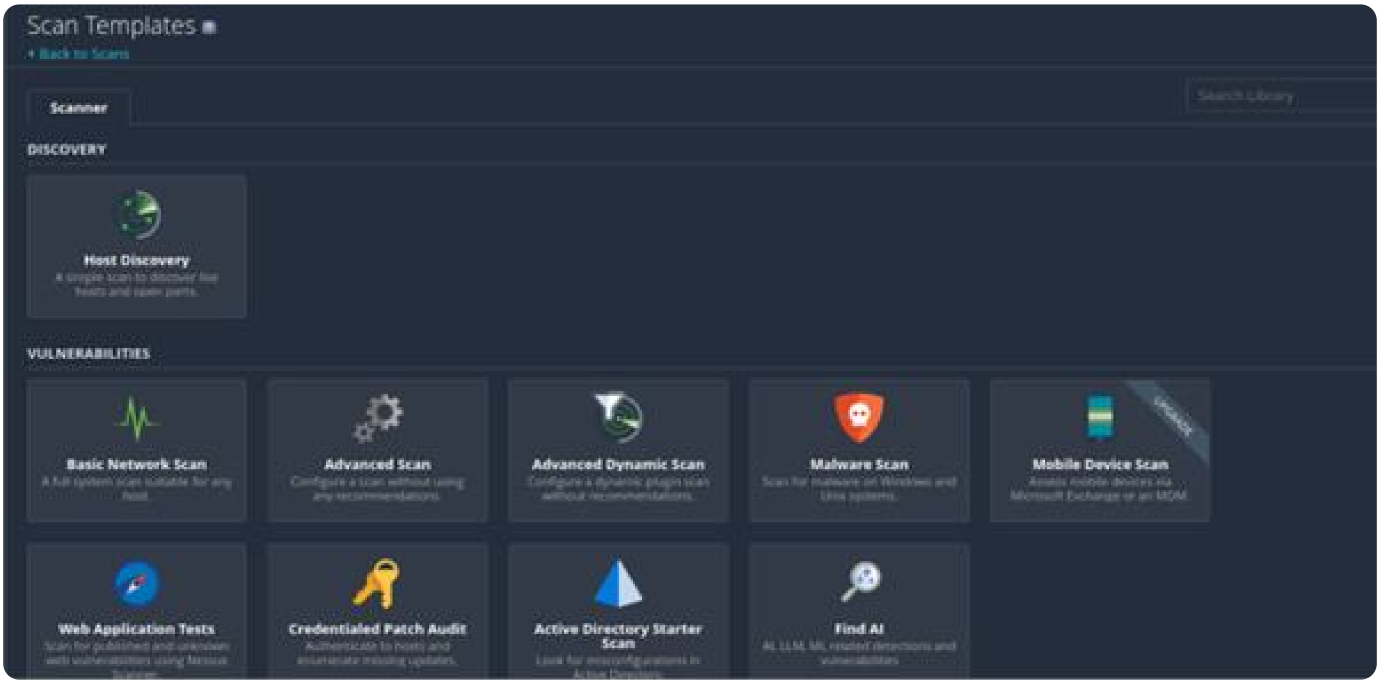
- Navigate to the **Scans** tab.
- Click on **New Scan.**
- Select **Basic Network Scan** from the list of available templates.

3 Configure Scan Settings

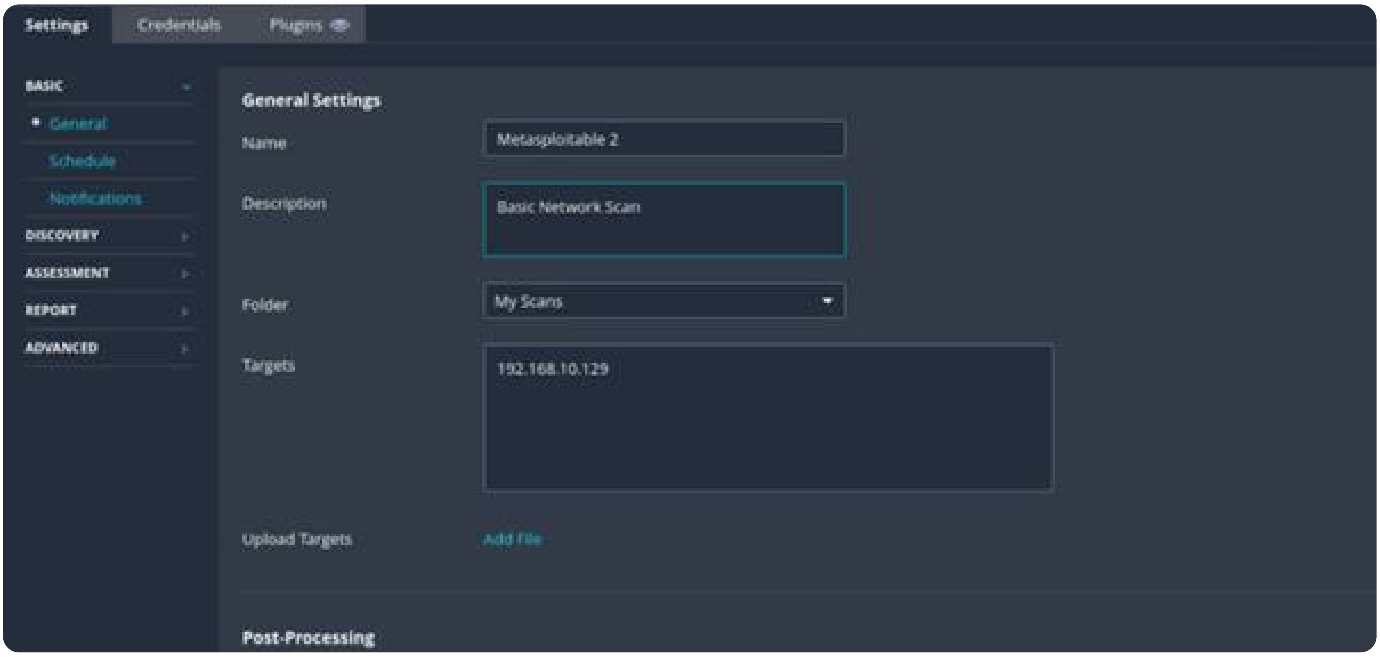
Once you select a scan template, you will need to configure the scan settings. This includes specifying your target, scan schedule, and any additional options like port ranges or scan timeouts.

Steps:

- **Name:** Provide a descriptive name for your scan (e.g., "Internal Network Scan").
- **Target:** Enter the target(s) for the scan.


Scan Templates
‹ Back to Scans
Scanner
Search Library
DISCOVERY
Host Discovery
A simple scan to discover live hosts and open ports.
VULNERABILITIES
Basic Network Scan
A full system scan suitable for any host.
Advanced Scan
Configure a scan without using any recommendations.
Advanced Dynamic Scan
Configure a dynamic plugin scan without recommendations.
Malware Scan
Scan for malware on Windows and Unix systems.
Mobile Device Scan
Assess mobile devices via Microsoft Exchange or an MDM.
UPGRADE
Web Application Tests
Scan for published and unknown web vulnerabilities using Nessus Scanner.
Credentialed Patch Audit
Authenticate to hosts and enumerate missing updates.
Active Directory Starter Scan
Look for misconfigurations in Active Directory.
Find AI
AI, LLM, ML related detections and vulnerabilities

- **Range of IP Addresses**



General Settings

Name: Metasploitable 2

Description: Basic Network Scan

Folder: My Scans

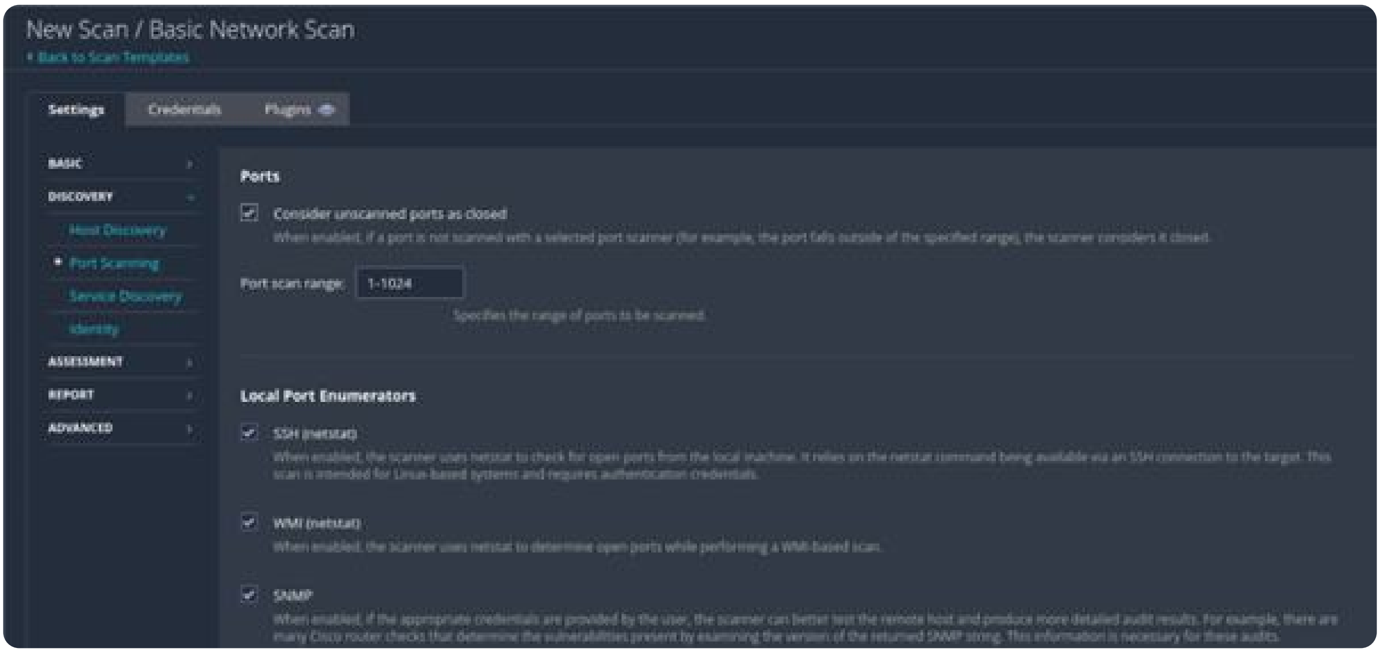
Targets: 192.168.10.129

Upload Targets

Post-Processing

Set up the scan with the target IP, specify the project name along with a detailed description, and ensure all output is saved to your "scan" folder.

- **Port Range:** If you want to scan a specific range of ports, configure the Port Range field. For example, to scan common ports: 1-1024, 8080, 8443



Ports

☑ Consider unscanned ports as closed
When enabled, if a port is not scanned with a selected port scanner (for example, the port falls outside of the specified range), the scanner considers it closed.

Port scan range: 1-1024
Specifies the range of ports to be scanned.

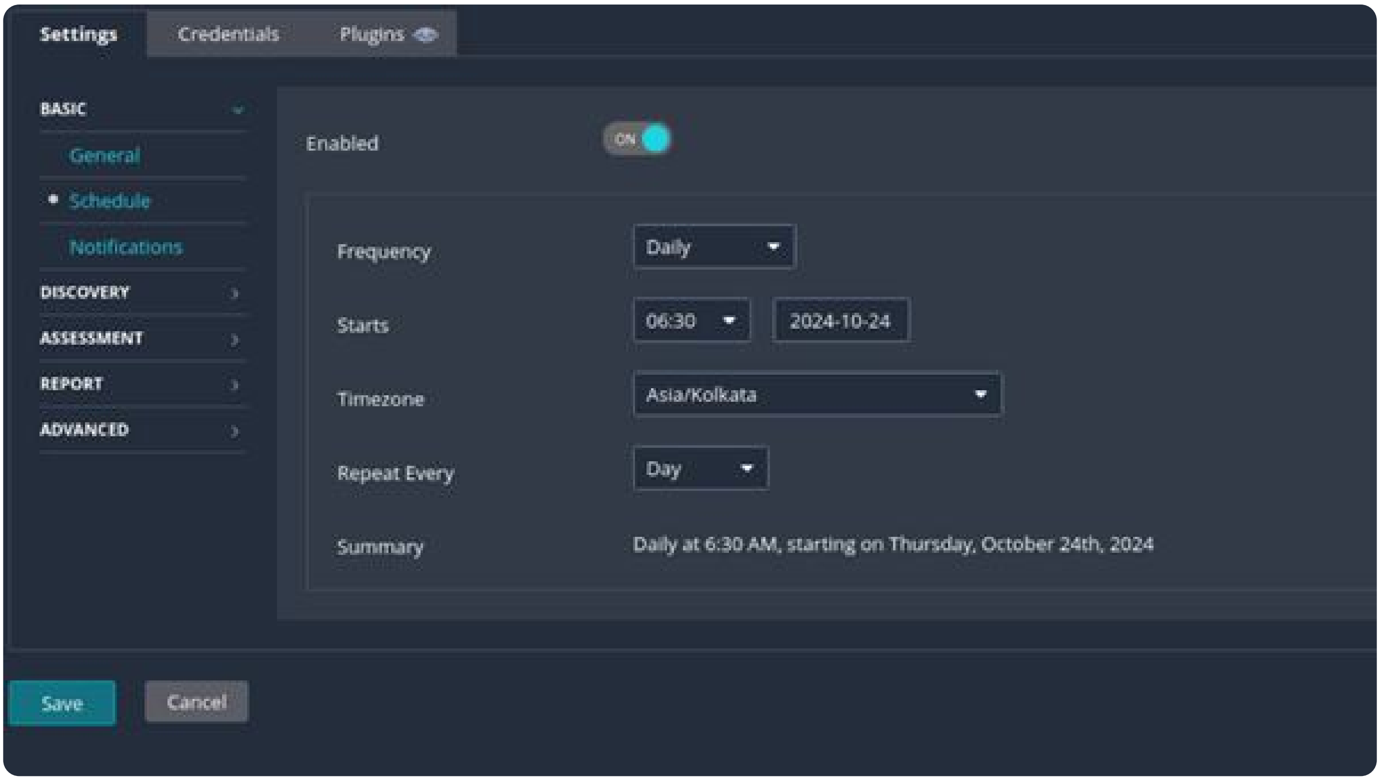
Local Port Enumerators

☑ SSH (netstat)
When enabled, the scanner uses netstat to check for open ports from the local machine. It relies on the netstat command being available via an SSH connection to the target. This scan is intended for Linux-based systems and requires authentication credentials.

☑ WMI (netstat)
When enabled, the scanner uses netstat to determine open ports while performing a WMI-based scan.

☑ SNMP
When enabled, if the appropriate credentials are provided by the user, the scanner can better test the remote host and produce more detailed audit results. For example, there are many Cisco router checks that determine the vulnerabilities present by examining the version of the returned SNMP string. This information is necessary for these audits.

- **Schedule:** If you want to automate the scan, you can set it to run periodically (e.g., daily or weekly) under the **Schedule** tab. **Daily Scan** (scheduled at 6:30 PM every day):



Enabled: ON

Frequency: Daily

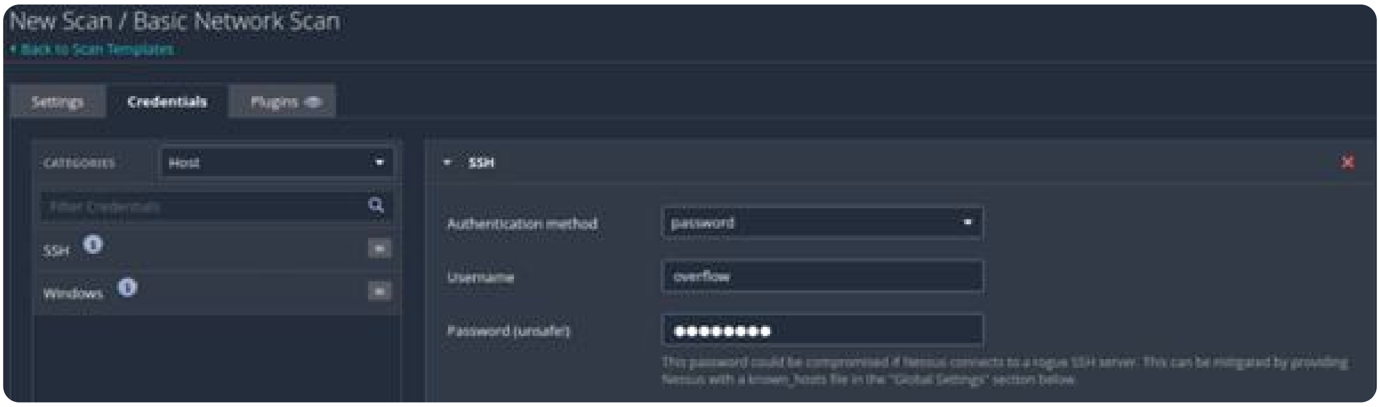
Starts: 06:30 2024-10-24

Timezone: Asia/Kolkata

Repeat Every: Day

Summary: Daily at 6:30 AM, starting on Thursday, October 24th, 2024

- **Configure Authentication:** If your scan targets servers or devices requiring authentication, you can configure credentials such as SSH or SMB to gain deeper insights. Here's how to specify credentials in the scan configuration: SSH Authentication:



Authentication method: password

Username: overflow

Password (unsafe): ●●●●●●●●●

This password could be compromised if Nessus connects to a rogue SSH server. This can be mitigated by providing Nessus with a known_hosts file in the "Global Settings" section below.

4 Run the Scan

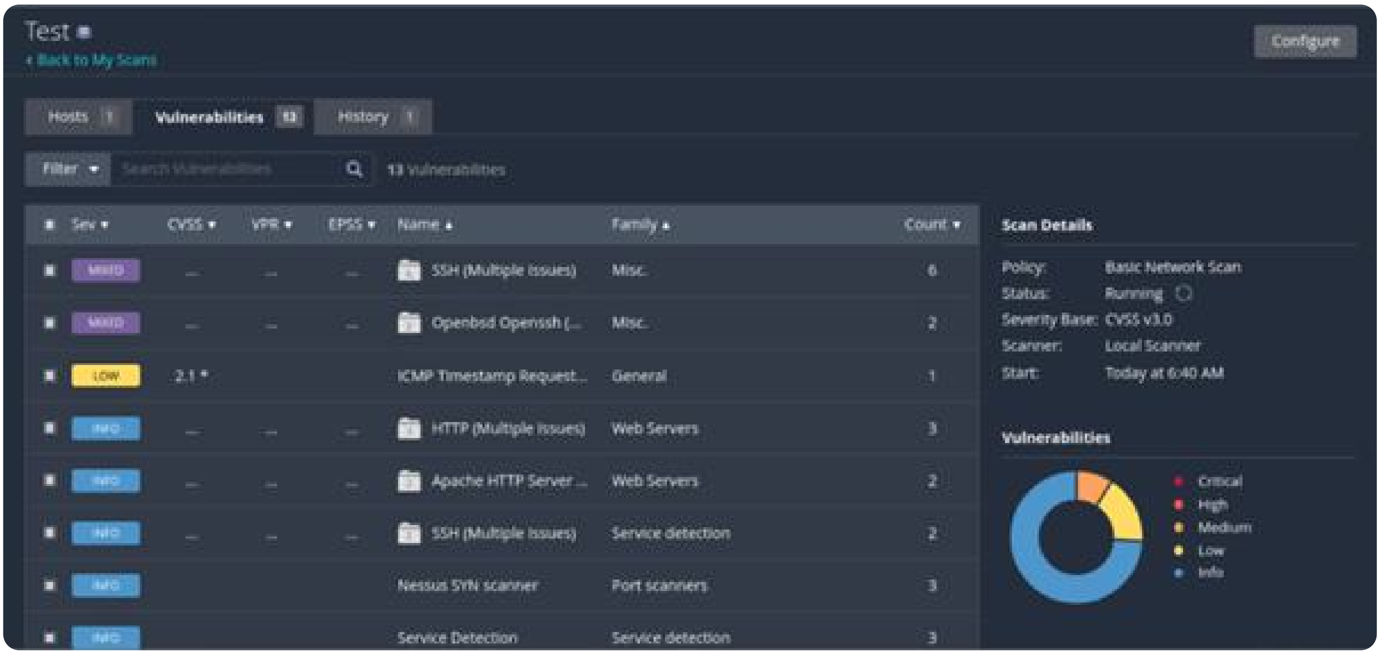
After configuring the scan settings, you're ready to launch the scan. Nessus Professional will immediately begin scanning the target network, and the time required will vary based on the network's size and complexity.

- Click Save to save the scan configuration.
- Click Launch to start the scan immediately.

5 Monitor the Scan Progress

Once the scan is launched, Nessus Professional will display the progress in real-time within the web interface. The status bar will show how far along the scan is, and once completed, the results will be available for review.

You can view the scan progress under the Scans tab, where you will see the percentage of the scan completed, the time elapsed, and the number of vulnerabilities detected so far.



Sev ▾	CVSS ▾	VPR ▾	EPSS ▾	Name ▴	Family ▴	Count ▾
MIXED	–	–	–	SSH (Multiple Issues)	Misc.	6
MIXED	–	–	–	Openbsd Openssh (...	Misc.	2
LOW	2.1 *			ICMP Timestamp Request...	General	1
INFO	–	–	–	HTTP (Multiple Issues)	Web Servers	3
INFO	–	–	–	Apache HTTP Server ...	Web Servers	2
INFO	–	–	–	SSH (Multiple Issues)	Service detection	2
INFO				Nessus SYN scanner	Port scanners	3
INFO				Service Detection	Service detection	3

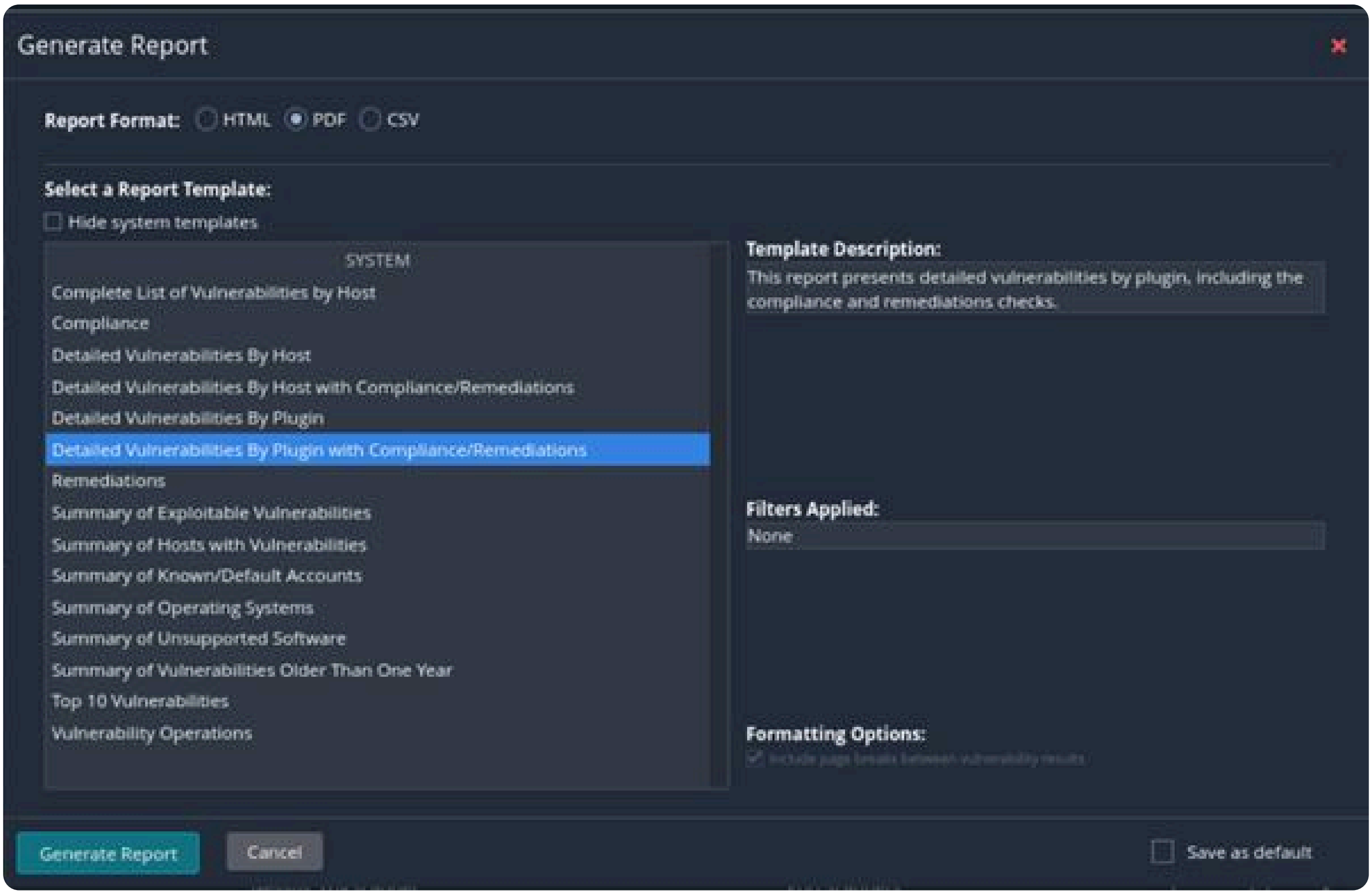
Scan Details

Policy: Basic Network Scan
Status: Running
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 6:40 AM

Vulnerabilities

6 View and Analyze Scan Results

After the scan is completed, Nessus Professional will generate a comprehensive report outlining the vulnerabilities discovered. Each vulnerability will be categorized by its severity:
Download Scan Results in CSV Format:



Generate Report

Report Format: ○ HTML ● PDF ○ CSV

Select a Report Template:
□ Hide system templates

SYSTEM
- Complete List of Vulnerabilities by Host
- Compliance
- Detailed Vulnerabilities By Host
- Detailed Vulnerabilities By Host with Compliance/Remediations
- Detailed Vulnerabilities By Plugin
- Detailed Vulnerabilities By Plugin with Compliance/Remediations
- Remediations
- Summary of Exploitable Vulnerabilities
- Summary of Hosts with Vulnerabilities
- Summary of Known/Default Accounts
- Summary of Operating Systems
- Summary of Unsupported Software
- Summary of Vulnerabilities Older Than One Year
- Top 10 Vulnerabilities
- Vulnerability Operations

Template Description:
This report presents detailed vulnerabilities by plugin, including the compliance and remediations checks.

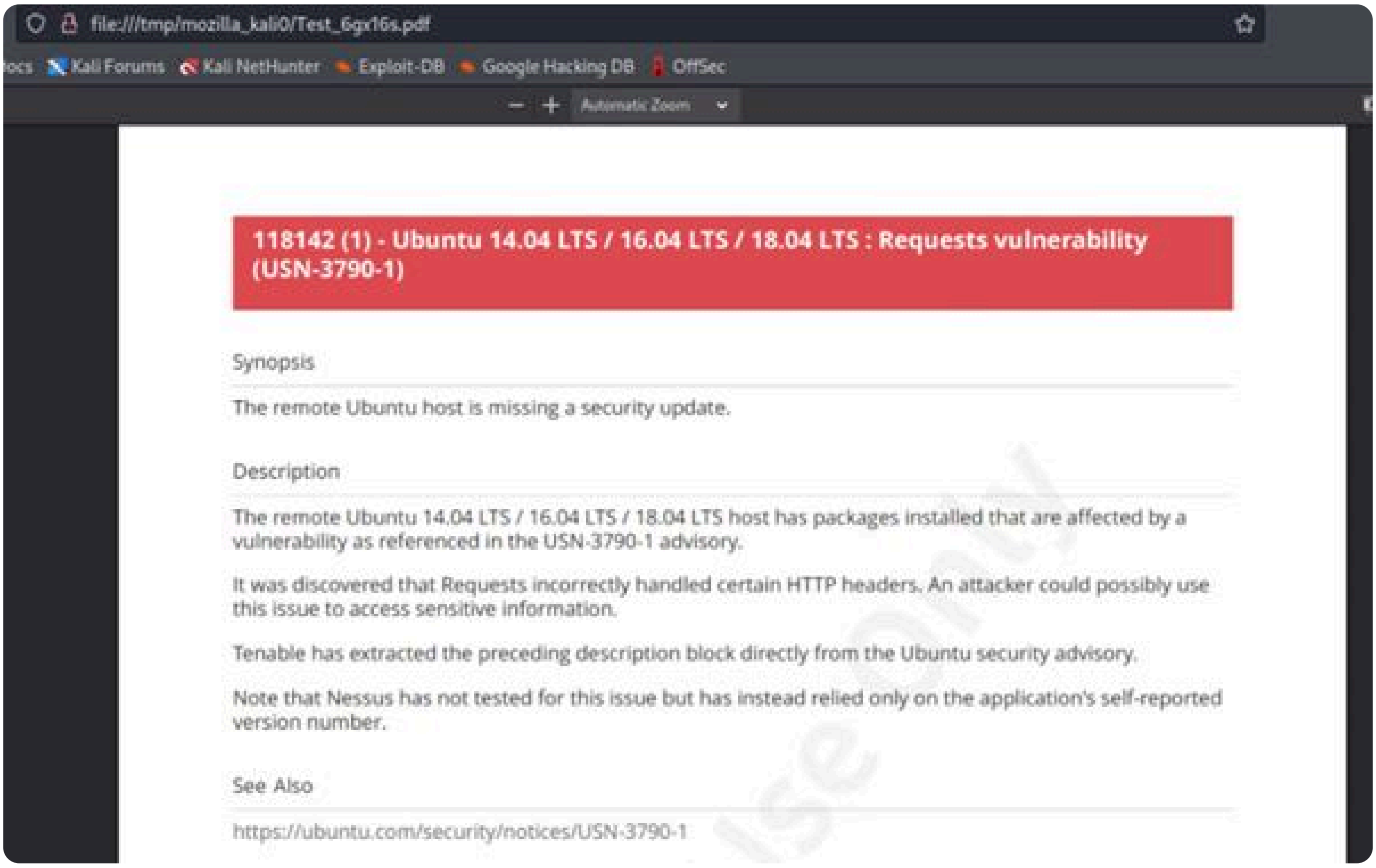
Filters Applied:
None

Formatting Options:
☑ Include page breaks between vulnerability results

7 Exporting Results

You can export the scan results in different formats from the Nessus Professional web interface by following these steps:

- Open the scan results page.
- Click on Export.
- Choose the desired format (e.g., PDF, CSV, HTML).
- Save the file to your desired location.



118142 (1) - Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS : Requests vulnerability (USN-3790-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-3790-1 advisory.

It was discovered that Requests incorrectly handled certain HTTP headers. An attacker could possibly use this issue to access sensitive information.

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

https://ubuntu.com/security/notices/USN-3790-1

8 Remediation and Continuous Scanning

Once vulnerabilities are identified, prioritize remediation based on their severity. After addressing the critical vulnerabilities, you can continuously monitor the environment by scheduling periodic scans.

Following these steps allows you to conduct an effective vulnerability scan using Nessus Professional, helping you secure your network against potential threats. Regular scans and diligent remediation are key components in maintaining a secure and resilient network environment.

KEEP LEARNING WITH

INFOSECTRAIN

Educate. Excel. Empower.