

# Scanning with Nessus

## Part 1

Nessus is a vulnerability scanner. It is usually used as on external pentesting. We can download Nessus by doing a simple google search and going to the following link:

<https://www.tenable.com/downloads/nessus?loginAttempted=true> and choosing the desired file type based on your OS as shown below:

The screenshot shows the Tenable Downloads page for Nessus. The page has a sidebar with navigation links: Nessus, Nessus Agents, Nessus Network Monitor, Tenable.sc, Integrations, Log Correlation Engine, Tenable Core, Tenable.ot, Web Application Scanning, and Compliance & Audit Files. The main content area is titled 'Downloads / Nessus' and features a 'Jump to: Release' dropdown. A prominent message states 'Need an Activation Code?' with a 'Get Activation Code' button. Below this, the 'Nessus - 8.11.0' section lists various download packages with their respective operating systems, file sizes, and release dates. A 'View Release Notes' link is also present.

Package Name	Operating System	File Size	Release Date	Action
<a href="#">Nessus-8.11.0-debian6_i386.deb</a>	Debian 6, 7, 8, 9 / Kali Linux 1, 2017.3 i386(32-bit)	38.8 MB	Jul 14, 2020	<a href="#">Checksum</a>
<a href="#">Nessus-8.11.0-amzn.x86_64.rpm</a>	Amazon Linux 2015.03, 2015.09, 2017.09, Amazon Linux 2	41.2 MB	Jul 14, 2020	<a href="#">Checksum</a>
<a href="#">Nessus-8.11.0-x64.msi</a>	Windows Server 2008, Server 2008 R2*, Server 2012, Server 2012 R2, 7, 8, 10, Server 2016, Server 2019 (64-bit)	75.7 MB	Jul 14, 2020	<a href="#">Checksum</a>
<a href="#">Nessus-8.11.0-Win32.msi</a>	Windows 7, 8, 10 (32-bit)	69.8 MB	Jul 14, 2020	<a href="#">Checksum</a>
<a href="#">Nessus-8.11.0.dmg</a>	macOS (10.9 - 10.15)	53.4 MB	Jul 14, 2020	<a href="#">Checksum</a>
<a href="#">Nessus-8.11.0-amzn2.aarch64.rpm</a>	Amazon Linux 2 (Graviton2)	38 MB	Jul 14, 2020	<a href="#">Checksum</a>
<a href="#">Nessus-8.11.0-debian6_amd64.deb</a>	Debian 6, 7, 8, 9 / Kali Linux 1, 2017.3 AMD64	40.9 MB	Jul 14, 2020	<a href="#">Checksum</a>

Once we download the file, open a Terminal session and go to the `Downloads` directory where the file is stored using the `cd ~ && cd Downloads` command. Next, use the `dpkg -i <Nessus_Package_File_Name>` command to unpack/depackage the .deb file as shown below:

```
root@kali:~# cd ~ && cd Downloads
root@kali:~/Downloads# dpkg -i Nessus-8.11.0-ubuntu1110_amd64.deb
Selecting previously unselected package nessus.
(Reading database ... 343734 files and directories currently installed.)
Preparing to unpack Nessus-8.11.0-ubuntu1110_amd64.deb ...
Unpacking nessus (8.11.0) ...
Setting up nessus (8.11.0) ...
Unpacking Nessus Scanner Core Components ...

- You can start Nessus Scanner by typing /etc/init.d/nessusd start
- Then go to https://kali:8834/ to configure your scanner

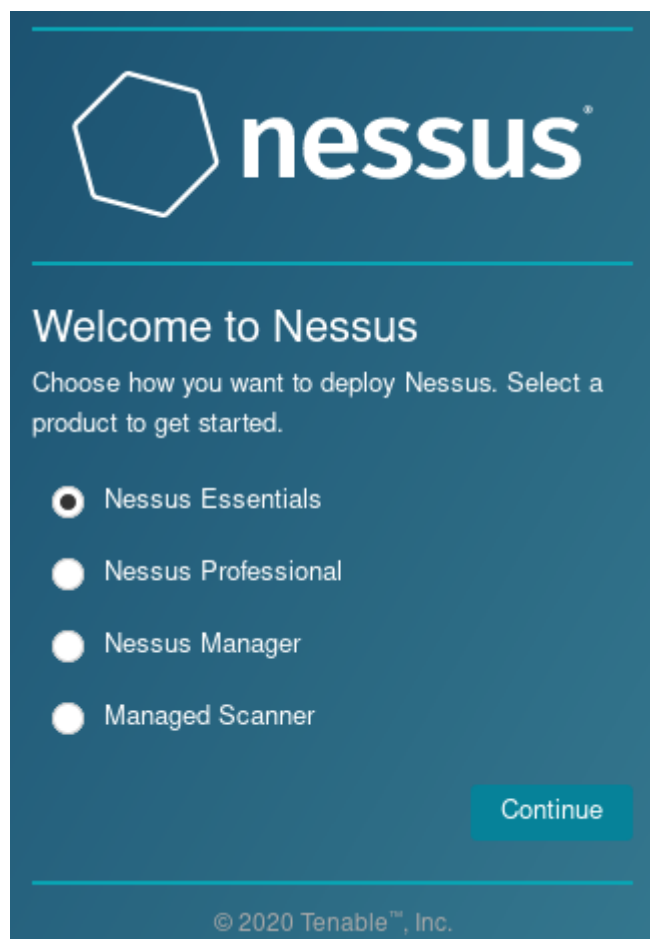
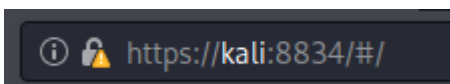
Processing triggers for systemd (245.6-2) ...
root@kali:~/Downloads#
```

The package installed automatically.

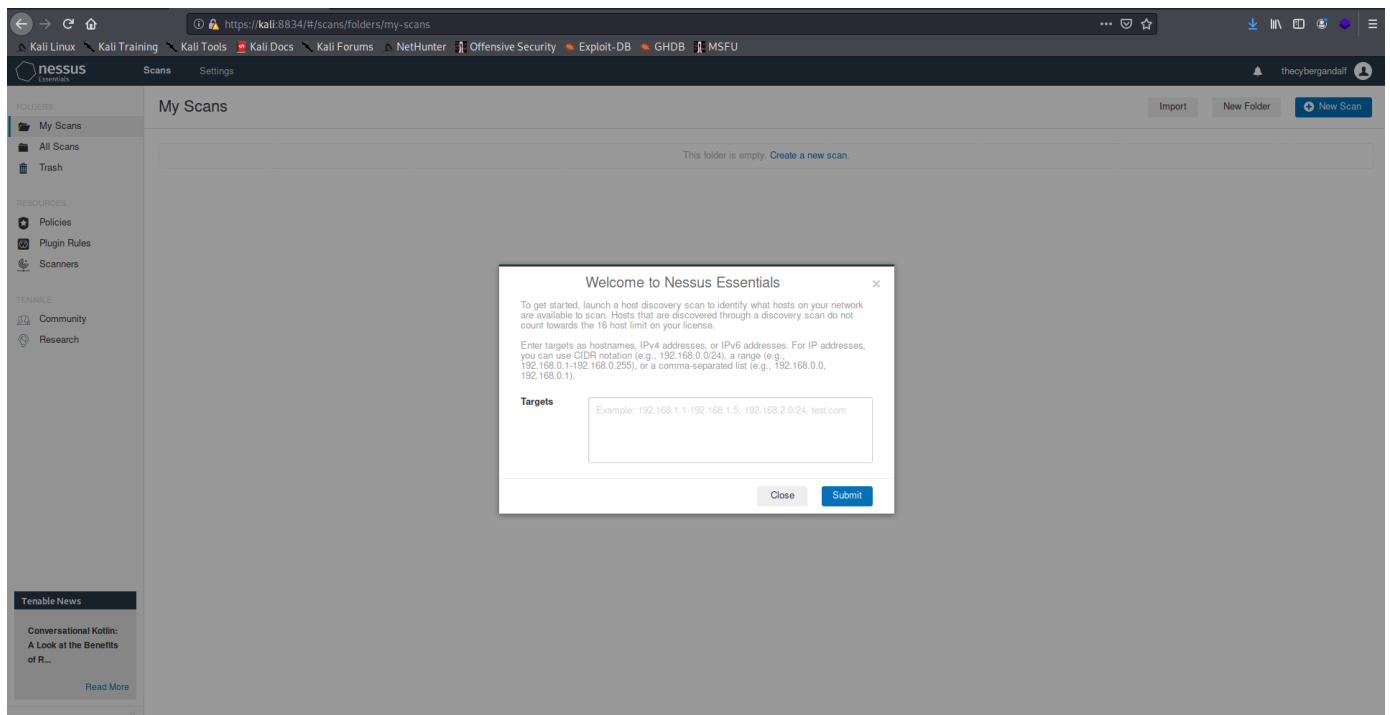
As we can see, we have to use the `/etc/init.d/nessusd start` command to start the Nessus service as shown below:

```
root@kali:~/Downloads# /etc/init.d/nessusd start
Starting Nessus : .
```

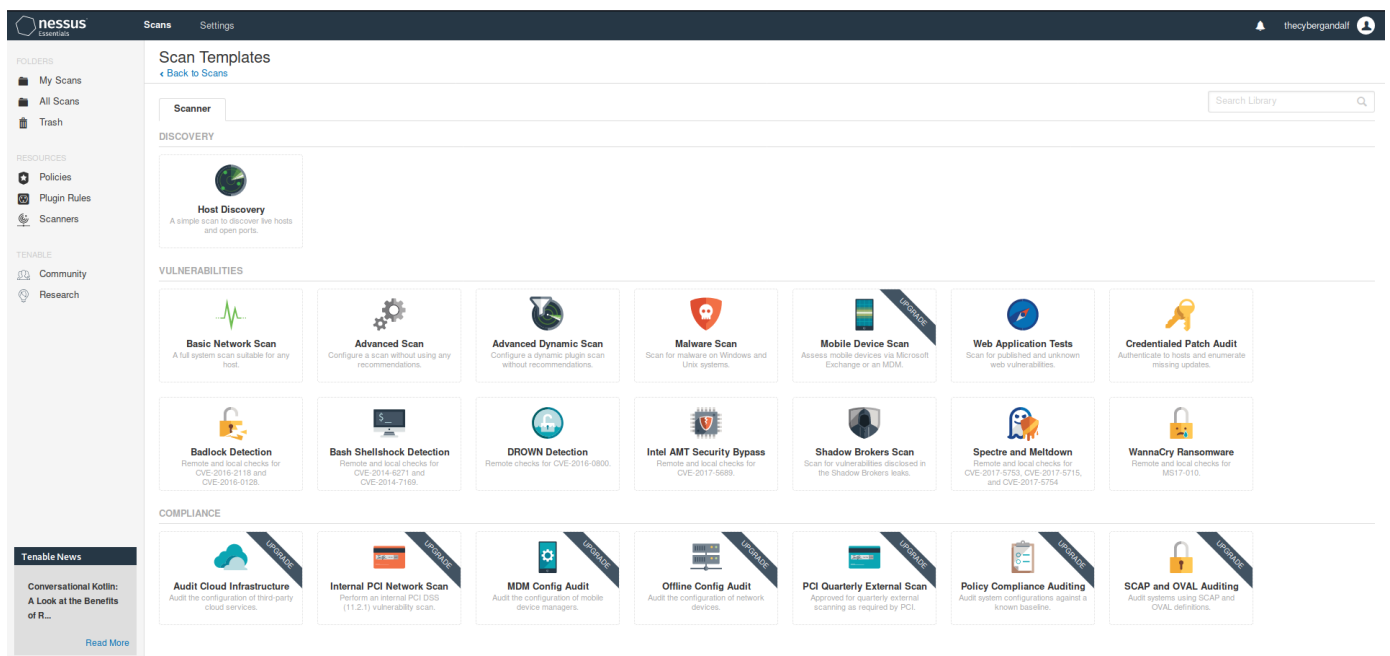
We can also see from the original `dpkg...` command that there is a URL that we can use to access the Nessus GUI, `https://kali:8834/` as shown below. It will give a warning (You can ignore this warning):



We will be using **Nessus Essentials**. You will also need a valid email for an activation code. Go through the process and complete the account creation process. Once the account setup process is done, the system will take some time to download required plugins for full functionality. Once you are done with the process and login, you will be met with this page:



In the **Targets** box, you can enter the IP address of a target or IP address range of targets. We will click on **close** as we are not ready to start scanning. On the top-right corner, click on **New Scan** and we will get this page:



Since we are using the free edition of Nessus, we are allowed to perform scans on any Private IP (network address) and we can scan up to 16 IP addresses at a time.

We will use the **Basic Network Scan** first as shown below:

In the **Settings** tab, select **Basic**. Under **Basic**, select **General**. Since our target is the Kioptrix VM, we did the following:

## New Scan / Basic Network Scan

[← Back to Scan Templates](#)

**Settings** | **Credentials** | **Plugins**

**BASIC**

- General
- [Schedule](#)
- [Notifications](#)

**DISCOVERY**   
**ASSESSMENT**   
**REPORT**   
**ADVANCED**

Name

Description

Folder

Targets

Upload Targets [Add File](#)

Save

[Cancel](#)

Next, go to the **Schedule** option. This option allows you to automate the scans.

The **Notifications** option allows you to send email notifications about scan progress if you have an SMTP server.


Next, go to the **Discovery** menu. Change the **Scan Type** to **Port scan (all ports)** is similar to **p-** in Nmap as shown below:

## New Scan / Basic Network Scan

[← Back to Scan Templates](#)

Settings

Credentials

Plugins 

BASIC >

DISCOVERY ▼

ASSESSMENT >

REPORT >

ADVANCED >

Scan Type

Port scan (all ports) ▼

General Settings:

Always test the local Nessus host

Use fast network discovery

Port Scanner Settings:

Scan all ports (1-65535)

Use netstat if credentials are provided

Use SYN scanner if necessary

Ping hosts using:

TCP

ARP

ICMP (2 retries)

Save ▼

Cancel

Next, go to the **Assessment** option and change the **Scan Type** to **Scan for known web vulnerabilities** as shown below. The other options such as, **Scan for all web vulnerabilities (complex)** might take a longer time:

## New Scan / Basic Network Scan

[← Back to Scan Templates](#)

**Settings** | **Credentials** | **Plugins**

**BASIC** >  
**DISCOVERY** >  
**ASSESSMENT** ✓  
**REPORT** >  
**ADVANCED** >

Scan Type

Scan for known web vulnerabilities ▼

**General Settings:**

Avoid potential false alarms

Enable CGI scanning

**Web Applications:**

Start crawling from "/"

Crawl 1000 pages (max)

Traverse 6 directories (max)

Test for known vulnerabilities in commonly used web applications

Generic web application tests disabled

Save ▼



Cancel

Next, go to the **Report** option, under **Output** leave the default settings.

Next, go to the **Advanced** option and leave the default settings.

Finally, click on **Save**.

Back in the **My scans** folder, click on the "Play" button to launch the scan as shown below:

My Scans			Import	New Folder	New Scan
Search Scans  1 Scan					
<input type="checkbox"/> Name	Schedule	Last Modified ▼			
<input type="checkbox"/> Kioptrix	On Demand	N/A	 		

While the scan is running, we'll go look at some of the other scan types by clicking on **New Scan**.

We will look at **Advanced Scan** as shown below:



### Fragile Devices

- ☐ Scan Network Printers
- ☐ Scan Novell Netware hosts
- ☐ Scan Operational Technology devices

### Wake-on-LAN

List of MAC addresses [Add File](#)

Boot time wait (in minutes)

Save

Cancel

There are more tabs and options that will be discussed in the video (Youtube)

## Part 2

Let's view the results of our Basic Scan. To do this, go to **My Scans**, click on the desired scan, then click on the IP address of the desired host, then click on the gear (Settings) button and select **Disable Groups** to help us view the individual vulnerabilities as shown below:

### My Scans

Import New Folder [New Scan](#)

Search Scans 1 Scan

<input type="checkbox"/>	Name	Schedule	Last Modified
<input type="checkbox"/>	Kioptrix	On Demand	✓ Today at 4:35 PM

Next ==>

### Kioptrix

[Back to My Scans](#)

Configure Audit Trail Launch Report Export

Hosts 1 Vulnerabilities 46 Remediations 3 History 1

Filter Search Hosts 1 Host

<input type="checkbox"/>	Host	Vulnerabilities
<input type="checkbox"/>	192.168.229.133	5 38 60 12 71

### Scan Details

Policy: Basic Network Scan  
Status: Completed  
Scanner: Local Scanner  
Start: Today at 4:30 PM  
End: Today at 4:35 PM  
Elapsed: 5 minutes

### Vulnerabilities



Next ==>



Kioptrix / 192.168.229.133  
[Back to Hosts](#)

ConfigureAudit TrailLaunchReportExport

Vulnerabilities46

FilterSearch Vulnerabilities46 Vulnerabilities

Sev	Name	Family	Count		Host Details
MIXED	OpenSSL (Multiple Issues)	Web Servers	48		192.168.229.133 00:0C:29:B7:CD:07 Linux Kernel 2.4
MIXED	Openbsd Openssh (Multiple Issues)	Gain a shell remotely	5		

Next =>

Kioptrix / 192.168.229.133  
[Back to Hosts](#)

ConfigureAudit TrailLaunchReportExport

Vulnerabilities126

FilterSearch Vulnerabilities126 Vulnerabilities

Sev	Name	Family	Count		Host Details
CRITICAL	OpenSSL Unsupported	Web Servers	2		IP: 192.168.229.133 MAC: 00:0C:29:B7:CD:07 OS: Linux Kernel 2.4 Start: Today at 4:30 PM End: Today at 4:35 PM Elapsed: 5 minutes KB: <a href="#">Download</a>
CRITICAL	OpenSSH < 3.1 Channel Code Off by One Remote Privilege Escalation	Gain a shell remotely	1		
CRITICAL	OpenSSH < 3.4 Multiple Remote Overflows	Gain a shell remotely	1		
CRITICAL	OpenSSH < 3.7.1 Multiple Vulnerabilities	Gain a shell remotely	1		
HIGH	Apache < 1.3.27 Multiple Vulnerabilities (DoS, XSS)	Web Servers	2		
HIGH	Apache < 1.3.28 Multiple Vulnerabilities (DoS, ID)	Web Servers	2		
HIGH	Apache < 1.3.29 Multiple Modules Local Overflow	Web Servers	2		
HIGH	Apache < 1.3.37 mod_rewrite LDAP Protocol URL Handling Overflow	Web Servers	2		
HIGH	Apache Chunked Encoding Remote Overflow	Web Servers	2		
HIGH	Apache mod_ssl ssl_engine_log.c mod_proxy Hook Function Remote Format String	Web Servers	2		
HIGH	mod_ssl ssl_util_uuencode_binary Remote Overflow	Web Servers	2		
HIGH	OpenSSL < 0.9.6e Multiple Vulnerabilities	Web Servers	2		
HIGH	OpenSSL < 0.9.7.beta3 Buffer Overflow	Web Servers	2		
HIGH	OpenSSL < 0.9.8f Multiple Vulnerabilities	Web Servers	2		

Vulnerabilities

Critical

High

Medium

Low

Info

We can click on any vulnerability and examine the details as shown below:

Kioptrix / Plugin #78555  
[Back to Vulnerabilities](#)

ConfigureAudit TrailLaunchReportExport

Vulnerabilities126

CRITICAL OpenSSL Unsupported

Description

According to its banner, the remote web server is running a version of OpenSSL that is no longer supported.

Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it is likely to contain security vulnerabilities.

Solution

Upgrade to a version of OpenSSL that is currently supported.

See Also

<https://www.openssl.org/policies/releasestrat.html>  
<http://www.nessus.org/u74d55548d>

Output

```
Installed version : 0.9.6b
Supported versions : 1.1.0 / 1.0.2
EOL URL           : https://www.openssl.org/policies/releasestrat.html
```

Port	Hosts
443 / tcp / www	192.168.229.133
80 / tcp / www	192.168.229.133

Plugin Details

Severity: Critical

ID: 78555

Version: \$Revision: 1.7 \$

Type: remote

Family: Web Servers

Published: October 17, 2014

Modified: January 12, 2017

Risk Information

Risk Factor: Critical

CVSS v3.0 Base Score: 10.0

CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/SC:C/H:I/A:H

CVSS Base Score: 10.0

CVSS Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C

Vulnerability Information

CPE: cpe:/a:openssl:openssl

Unsupported by vendor: true

We can do this for necessary vulnerabilities such as critical vulnerabilities and we can research and report these.

We can also try to export the vulnerabilities as shown in the video (Youtube).

Do not always trust vulnerability scanners. Always go out and use other tools to find these vulnerabilities.