

Preforming Vulnerability scan on Metasploitable-2

1. Install Metasploitable-2 from the sourceforge.ne

Link: <https://sourceforge.net/projects/metasploitable/>

2. Install Kali Linux from official website

Link: <https://www.kali.org/get-kali/#kali-platforms>

3. Install the Nessus scanner on Kali Linux

Link: <https://www.tenable.com/products/nessus/nessus-essentials>

The screenshot shows the Tenable Nessus Essentials registration page. At the top, the Tenable logo is on the left, and navigation links (Platform, Products, Solutions, Why Tenable, Resources, Partners, Support, Company) and buttons (Try, Buy) are on the right. The main content area has a heading "Tenable Nessus® Essentials". Below it, a paragraph states: "As part of the Tenable Nessus family, Tenable Nessus Essentials allows you to scan your environment (up to 16 IP addresses per scanner) with the same high-speed, in-depth assessments and agentless scanning convenience that Nessus subscribers enjoy." A note below says: "Please note that Nessus Essentials does not allow you to perform compliance checks or content audits, Live Results or use the Nessus virtual appliance. If you require these additional features, please purchase a Tenable Nessus Professional subscription." Another note mentions: "Using Nessus Essentials for education? Register for Nessus Essentials through the Tenable for Education program to get started." A final note says: "Interested in learning how to use Nessus? Our on-demand course enables the student, through a series of targeted videos, to develop the building". On the right, there is a "Register for an Activation Code" form with fields for First Name, Last Name, and Business Email, a checkbox for "Check to receive updates from Tenable", a link to the Privacy Policy, and a "Get Started" button.

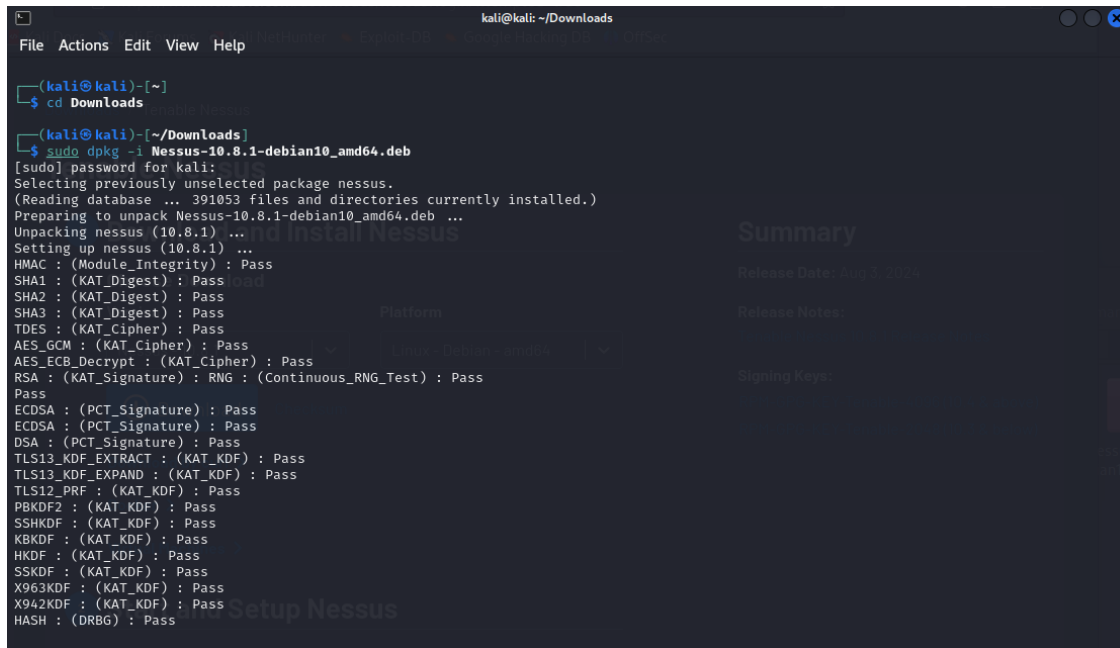
The screenshot shows the Tenable Nessus download page in a web browser. The browser's address bar shows the URL: <https://www.tenable.com/downloads/nessus?loginAttempted=true>. The page has a dark theme. On the left is a sidebar with a list of Tenable products: Tenable Nessus, Tenable Nessus Agent, Tenable Nessus Network Monitor, Tenable Security Center, Integrations, Sensor Proxy, Tenable Log Correlation Engine, Tenable Core, Tenable OT Security, Tenable Identity Exposure, Frictionless, Tenable Cloud Security. The main content area is titled "Tenable Nessus" and has a breadcrumb "Downloads / Tenable Nessus". It is divided into two main sections: "1 Download and Install Nessus" and "2 Start and Setup Nessus". The "Download and Install Nessus" section has a "Choose Download" heading. It features two dropdown menus: "Version" (set to "Nessus - 10.8.1") and "Platform" (set to "Linux - Ubuntu - amd64"). Below these is a blue "Download" button with a download icon, and a "Checksum" link. There are also links for "Download by curl", "Docker", and "Virtual Machines". The "Start and Setup Nessus" section has a heading and a sub-heading "Open Nessus and follow setup wizard to finish setting up Nessus". On the right, there is a "Summary" section with "Release Date: Aug 3, 2024", "Release Notes: Tenable Nessus 10.8.1 Release Notes", and "Signing Keys: RPM-GPG-KEY-Tenable-4096 (10.4 & above), RPM-GPG-KEY-Tenable-2048 (10.3 & below)".

4. Open Shell in Kali Linux and move to Downloads directory

```
cd Downloads
```

5. Download package of Nessus

```
sudo dpkg -i Nessus-10.8.1-debian10_amd64.deb
```



```
kali@kali: ~/Downloads
File Actions Edit View Help

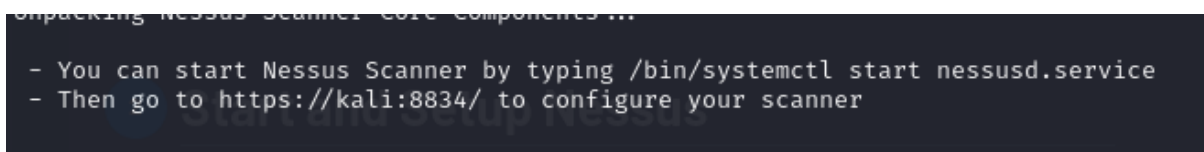
(kali@kali)-[~]
└─$ cd Downloads

(kali@kali)-[~/Downloads]
└─$ sudo dpkg -i Nessus-10.8.1-debian10_amd64.deb
[sudo] password for kali:
Selecting previously unselected package nessus.
(Reading database ... 391053 files and directories currently installed.)
Preparing to unpack Nessus-10.8.1-debian10_amd64.deb ...
Unpacking nessus (10.8.1) ...
Setting up nessus (10.8.1) ...
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
TLS13_KDF_EXTRACT : (KAT_KDF) : Pass
TLS13_KDF_EXPAND : (KAT_KDF) : Pass
TLS12_PRF : (KAT_KDF) : Pass
PBKDF2 : (KAT_KDF) : Pass
SSHKDF : (KAT_KDF) : Pass
KBKDF : (KAT_KDF) : Pass
HKDF : (KAT_KDF) : Pass
SSKDF : (KAT_KDF) : Pass
X963KDF : (KAT_KDF) : Pass
X942KDF : (KAT_KDF) : Pass
HASH : (DRBG) : Pass
```

6. Start Nessus in the system

```
systemctl start nessusd
```

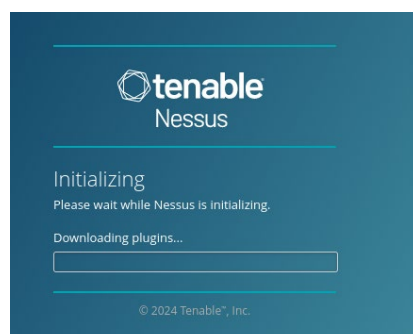
7. Visit the URL given on the command of the download package



```
Unpacking Nessus Scanner Core Components ...

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

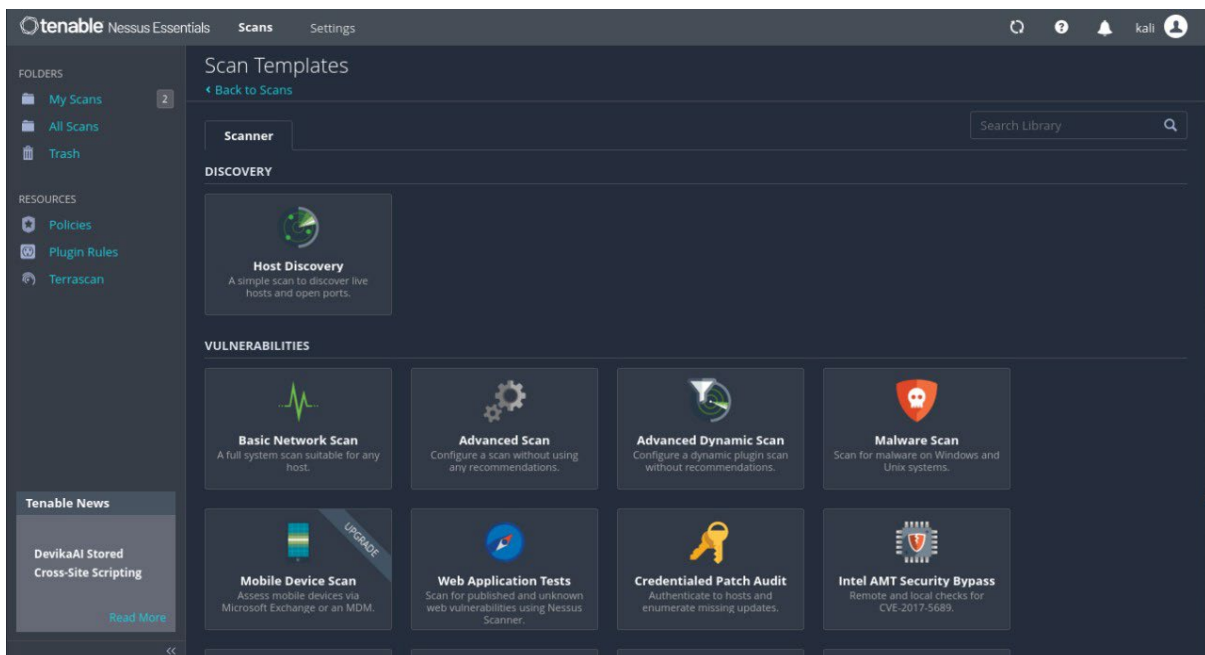
8. Create account or enter the code sent to your email earlier.



9. While the Nessus is installing get the IP address of the Metasploitable-2 system

```
The programs included with the Ubuntu system are free software;  
the exact distribution terms for each program are described in the  
individual files in /usr/share/doc/*/copyright.  
  
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by  
applicable law.  
  
To access official Ubuntu documentation, please visit:  
http://help.ubuntu.com/  
No mail.  
msfadmin@metasploitable:~$ ip a  
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue  
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00  
    inet 127.0.0.1/8 scope host lo  
    inet6 ::1/128 scope host  
        valid_lft forever preferred_lft forever  
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000  
    link/ether 00:0c:29:fa:dd:2a brd ff:ff:ff:ff:ff:ff  
    inet 192.168.137.130/24 brd 192.168.137.255 scope global eth0  
    inet6 fe80::20c:29ff:fefa:dd2a/64 scope link  
        valid_lft forever preferred_lft forever  
3: eth1: <BROADCAST,MULTICAST> mtu 1500 qdisc noop qlen 1000  
    link/ether 00:0c:29:fa:dd:34 brd ff:ff:ff:ff:ff:ff  
msfadmin@metasploitable:~$ _
```

10. Press “New Scan” -> press “Basic Network Scan”.



11. Enter the details and the IP of machine you want to run a scan on.

New Scan / Basic Network Scan
← Back to Scan Templates

Settings Credentials Plugins

BASIC

- General
- Schedule
- Notifications

DISCOVERY

ASSESSMENT

REPORT

ADVANCED

Name REQUIRED

Description

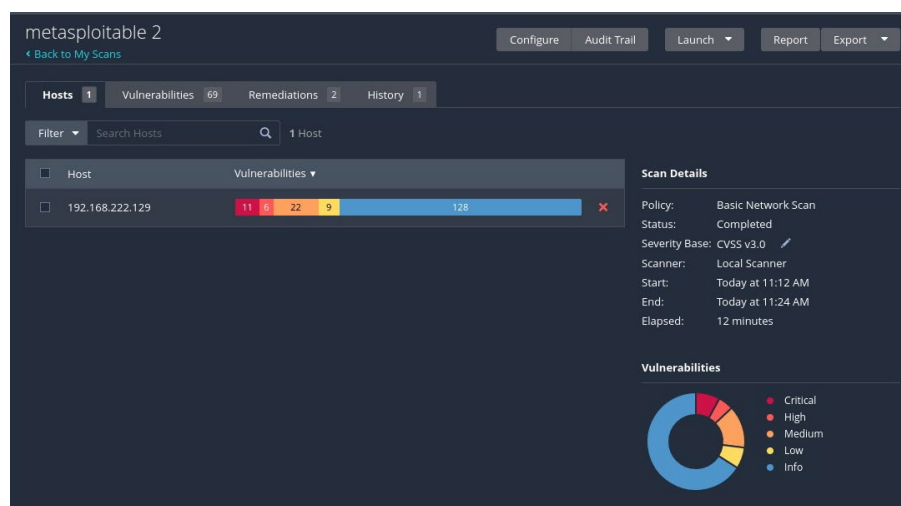
Folder My Scans

Targets
Example: 192.168.1.1-192.168.1.5, 192.168.2.0/24, test.com REQUIRED

Upload Targets Add File

Save Cancel

12. Once the scan is complete you can download the report and also look at the vulnerabilities.



Generate Report

Report Format: ☐ HTML ☒ PDF ☐ CSV

Select a Report Template:

SYSTEM

- Complete List of Vulnerabilities by Host
- Detailed Vulnerabilities By Host
- Detailed Vulnerabilities By Plugin
- Vulnerability Operations

Template Description:
This report provides a summary list of vulnerabilities for each host detected in the scan.

Filters Applied:
None

Formatting Options:
☒ Include page breaks between vulnerability results

Generating... Cancel Save as default