Name：[Waqar Hassan]

RegId：[221523]

Vulnerability Assessment And Reverse Engineering Lab

Tenable Nessus Scanning

To find vulnerabilities in systems or networks using the Nessus Vulnerability Scanner, you first need to understand how to install it.

In this step-by-step guide, we'll briefly discuss Nessus and then show you how to download, install, and run it on both Kali and Windows. This allows you to choose the platform that best suits your needs.

We'll also briefly show you how to run Nessus in Kali, set up a scan, and interpret the results.

Finally, we'll show you how to create a report that will allow you to analyze and present the results of your vulnerability scans in an organized manner.

If you're ready to learn how to install Nessus, let's get started.

What is Nessus?

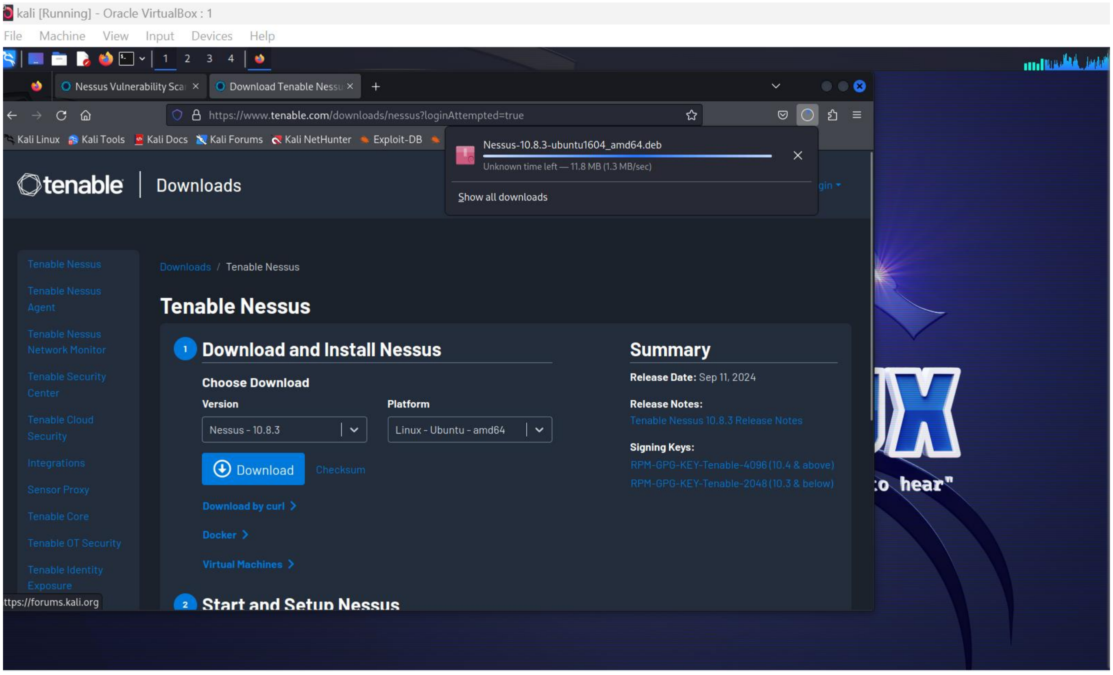
Nessus is a powerful tool from Tenable that can scan networks, operating systems, databases and applications for vulnerabilities.

It provides detailed reports on security weaknesses and prioritizes them based on their severity.

It scans and looks for bad configuration, missing patches and CVEs (Common Vulnerabilities and Exposures) and is often used in security assessments and penetration testing.

here is the complete installation process

Complete Installation



https://www.tenable.com/downloads/nessus?loginAttempted=true

Nessus-10.8.3-ubuntu1604_amd64.deb
Unknown time left — 11.8 MB (1.3 MB/sec)

Tenable Nessus

1 Download and Install Nessus

Choose Download

Version: Nessus - 10.8.3

Platform: Linux - Ubuntu - amd64

Summary

Release Date: Sep 11, 2024

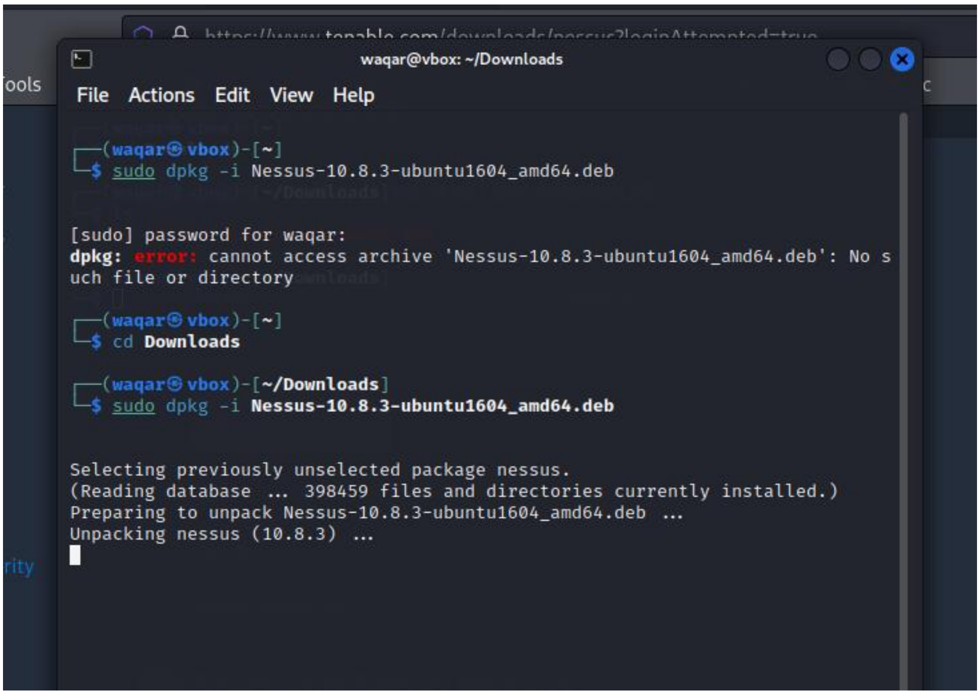
Release Notes: Tenable Nessus 10.8.3 Release Notes

Signing Keys:
RPM-GPG-KEY-Tenable-4096 (10.4 & above)
RPM-GPG-KEY-Tenable-2048 (10.3 & below)

2 Start and Setup Nessus

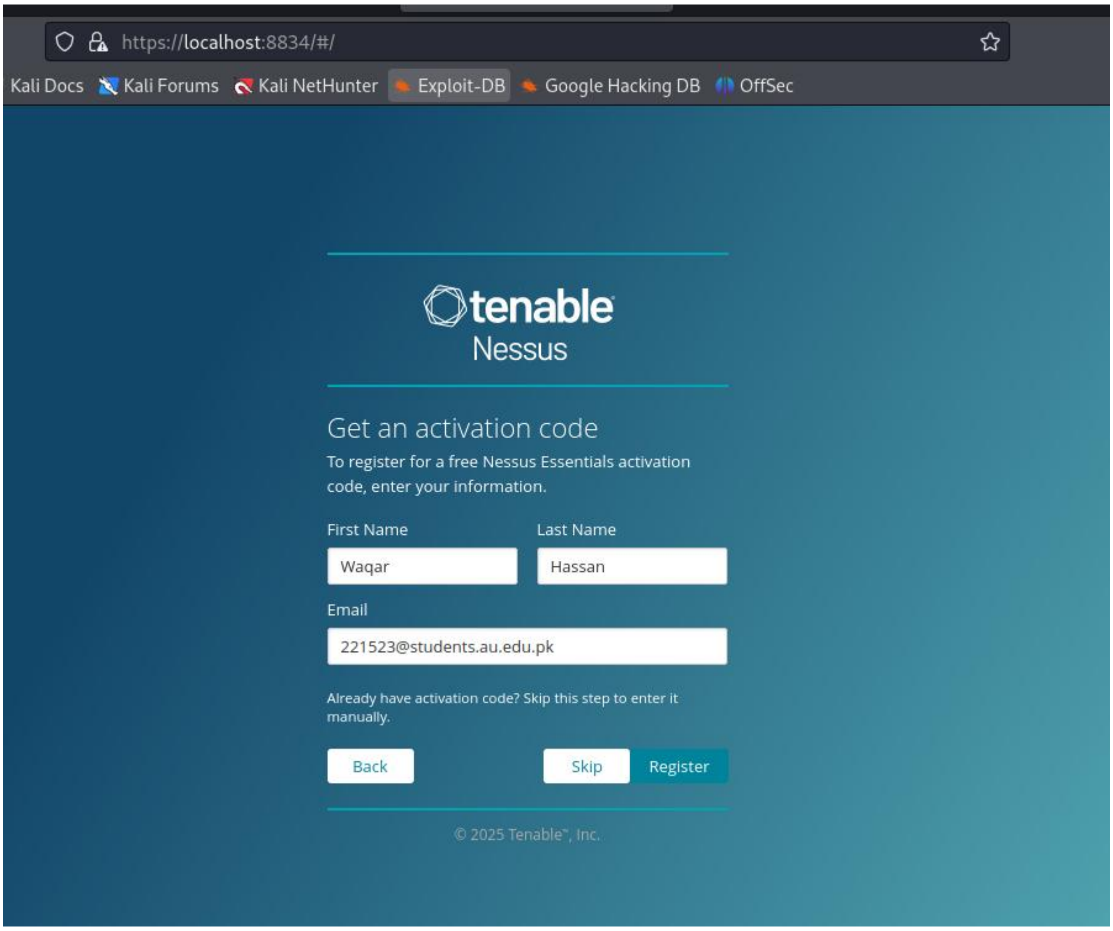
ttps://forums.kali.org

Commands running



```
┌──(waqar㉿vbox)-[~]
└─$ sudo dpkg -i Nessus-10.8.3-ubuntu1604_amd64.deb

[sudo] password for waqar:
dpkg: error: cannot access archive 'Nessus-10.8.3-ubuntu1604_amd64.deb': No s
uch file or directory

┌──(waqar㉿vbox)-[~]
└─$ cd Downloads

┌──(waqar㉿vbox)-[~/Downloads]
└─$ sudo dpkg -i Nessus-10.8.3-ubuntu1604_amd64.deb


Selecting previously unselected package nessus.
(Reading database ... 398459 files and directories currently installed.)
Preparing to unpack Nessus-10.8.3-ubuntu1604_amd64.deb ...
Unpacking nessus (10.8.3) ...
█
```

Activation Application



Get an activation code

To register for a free Nessus Essentials activation code, enter your information.

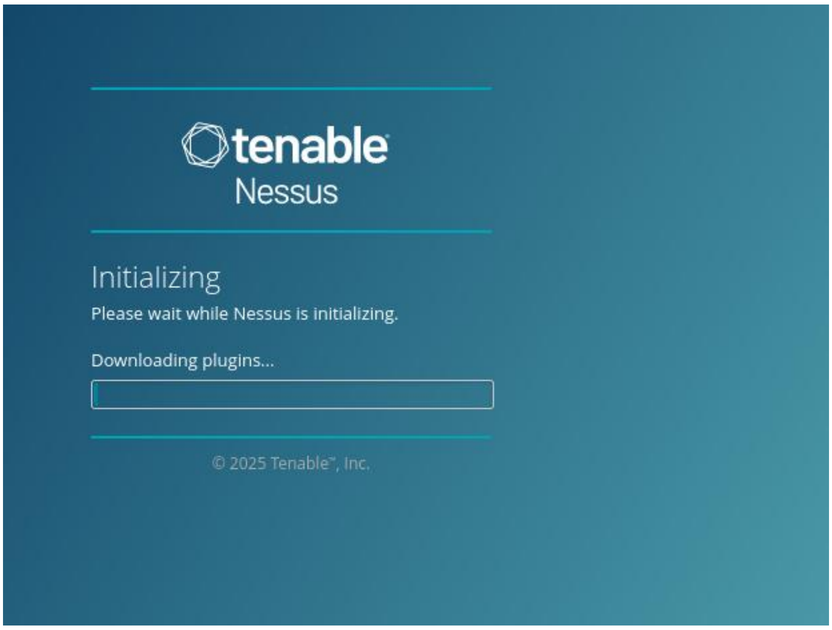
First Name: Waqar

Last Name: Hassan

Email: 221523@students.au.edu.pk

Already have activation code? Skip this step to enter it manually.

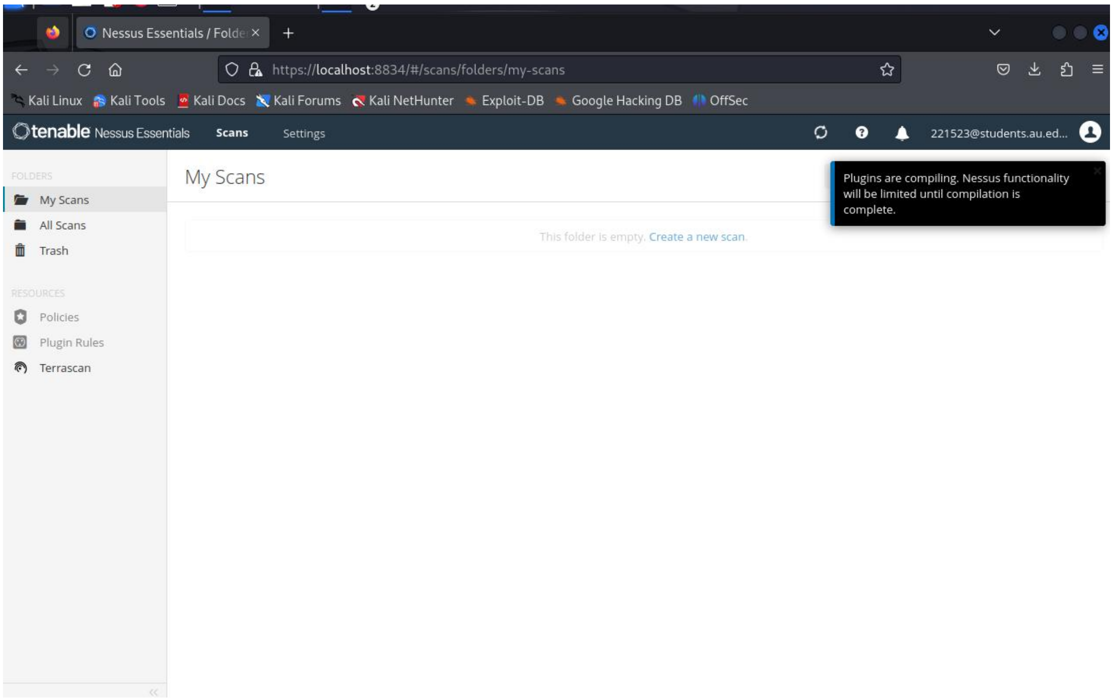
Downloading Plugins



Initializing

Please wait while Nessus is initializing.

Downloading plugins...

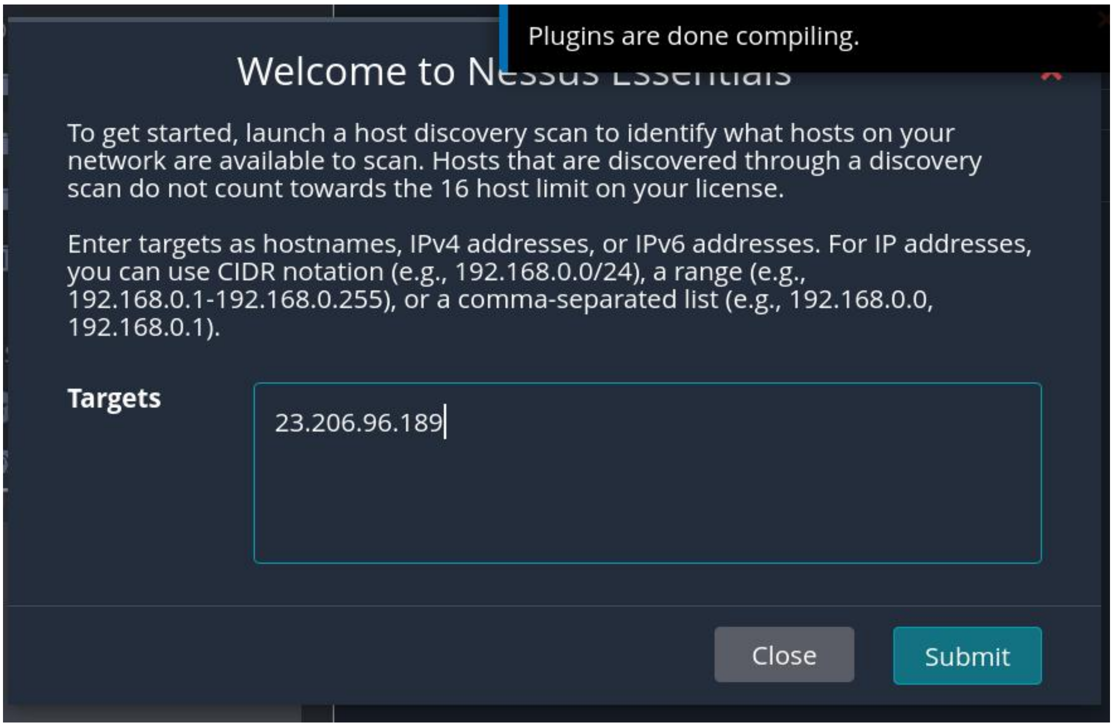


My Scans

Plugins are compiling. Nessus functionality will be limited until compilation is complete.

This folder is empty. Create a new scan.

Scanning On Starbucks bugbounty Program



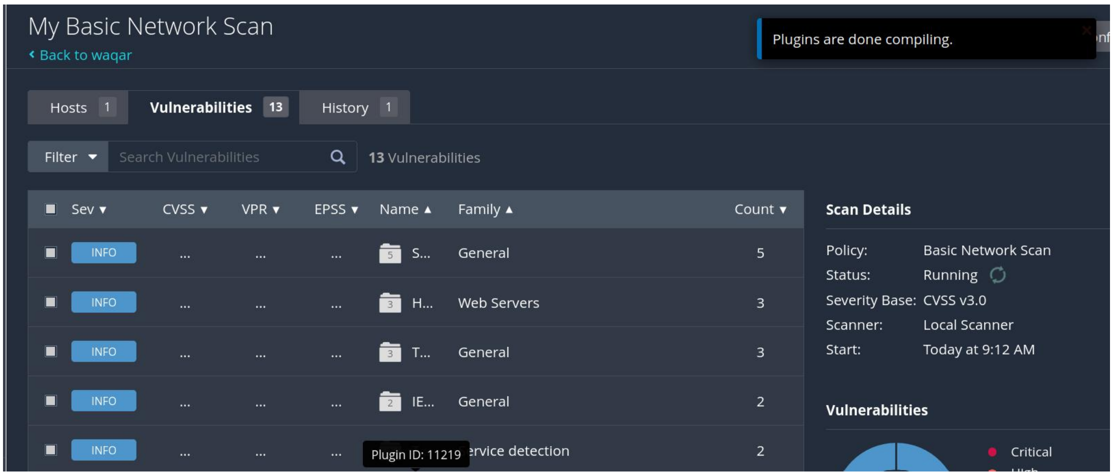
Plugins are done compiling.

Welcome to Nessus Essentials

To get started, launch a host discovery scan to identify what hosts on your network are available to scan. Hosts that are discovered through a discovery scan do not count towards the 16 host limit on your license.

Enter targets as hostnames, IPv4 addresses, or IPv6 addresses. For IP addresses, you can use CIDR notation (e.g., 192.168.0.0/24), a range (e.g., 192.168.0.1-192.168.0.255), or a comma-separated list (e.g., 192.168.0.0, 192.168.0.1).

Targets: 23.206.96.189



My Basic Network Scan

‹ Back to waqar

Plugins are done compiling.

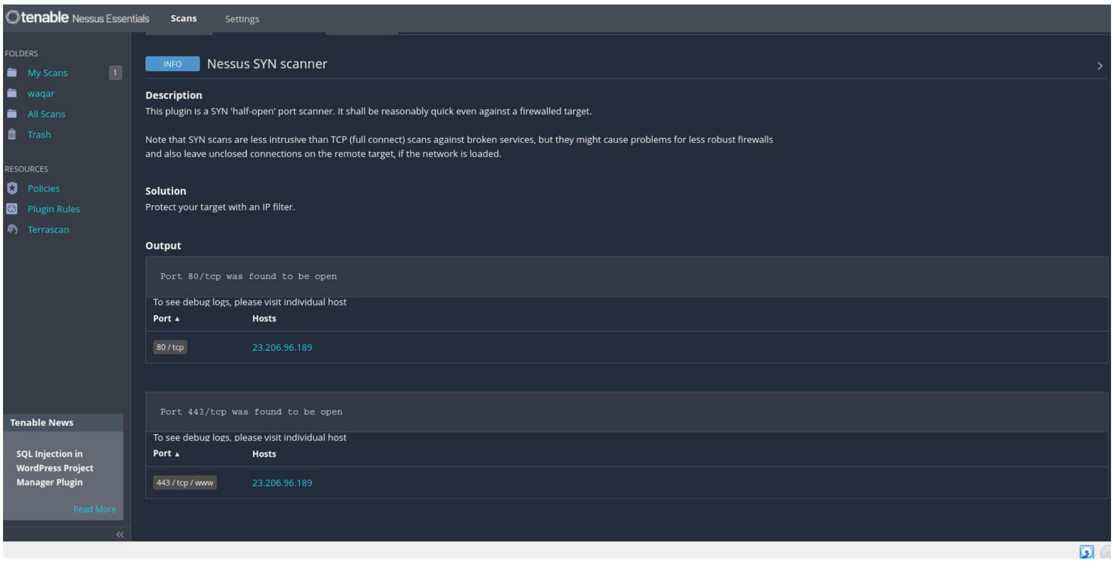
13 Vulnerabilities

□	Sev ▾	CVSS ▾	VPR ▾	EPSS ▾	Name ▴	Family ▴	Count ▾
□	INFO	...	...	...	5 S...	General	5
□	INFO	...	...	...	3 H...	Web Servers	3
□	INFO	...	...	...	3 T...	General	3
□	INFO	...	...	...	2 IE...	General	2
□	INFO	...	...	...	Plugin ID: 11219	ervice detection	2

Scan Details

Policy:	Basic Network Scan
Status:	Running
Severity Base:	CVSS v3.0
Scanner:	Local Scanner
Start:	Today at 9:12 AM

Vulnerabilities



INFO Nessus SYN scanner

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Output

```
Port 80/tcp was found to be open
```

To see debug logs, please visit individual host

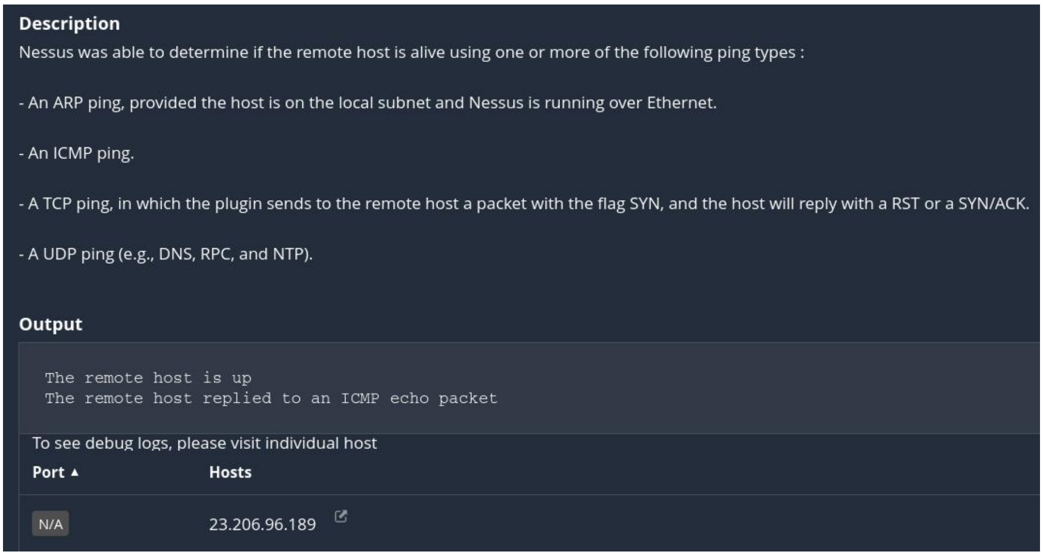
Port ▴	Hosts
80 / tcp	23.206.96.189

```
Port 443/tcp was found to be open
```

To see debug logs, please visit individual host

Port ▴	Hosts
443 / tcp / www	23.206.96.189

Basic Vulnerabilty reporting



Description

Nessus was able to determine if the remote host is alive using one or more of the following ping types :

- An ARP ping, provided the host is on the local subnet and Nessus is running over Ethernet.

- An ICMP ping.

- A TCP ping, in which the plugin sends to the remote host a packet with the flag SYN, and the host will reply with a RST or a SYN/ACK.

- A UDP ping (e.g., DNS, RPC, and NTP).

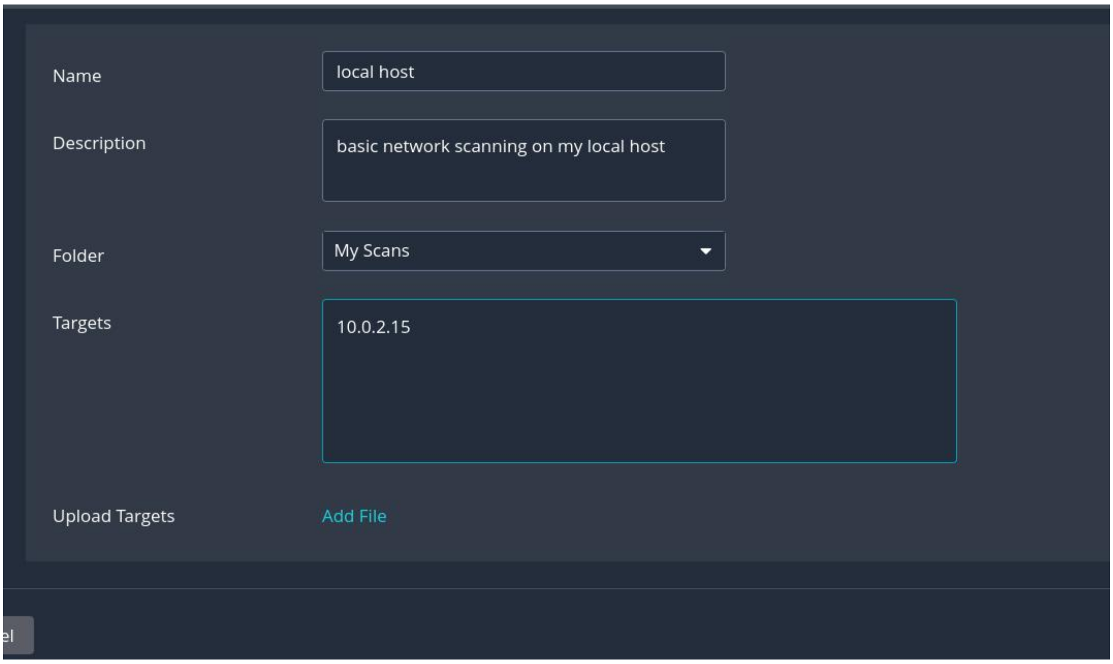
Output

```
The remote host is up
The remote host replied to an ICMP echo packet
```

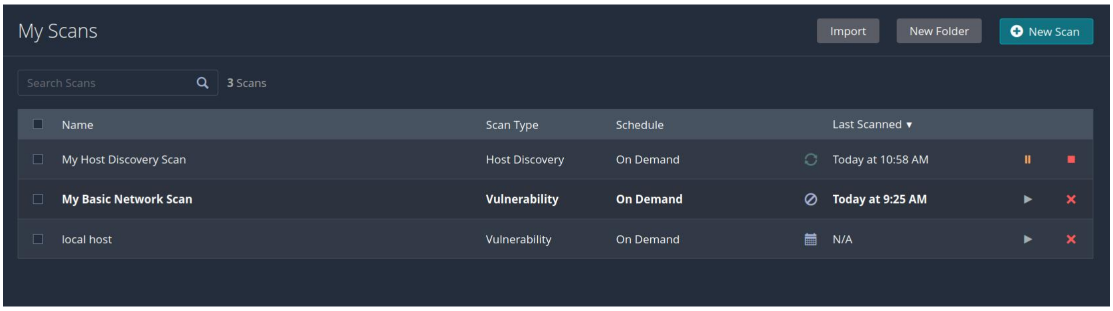
To see debug logs, please visit individual host

Port ▴	Hosts
N/A	23.206.96.189

Localhost scanning

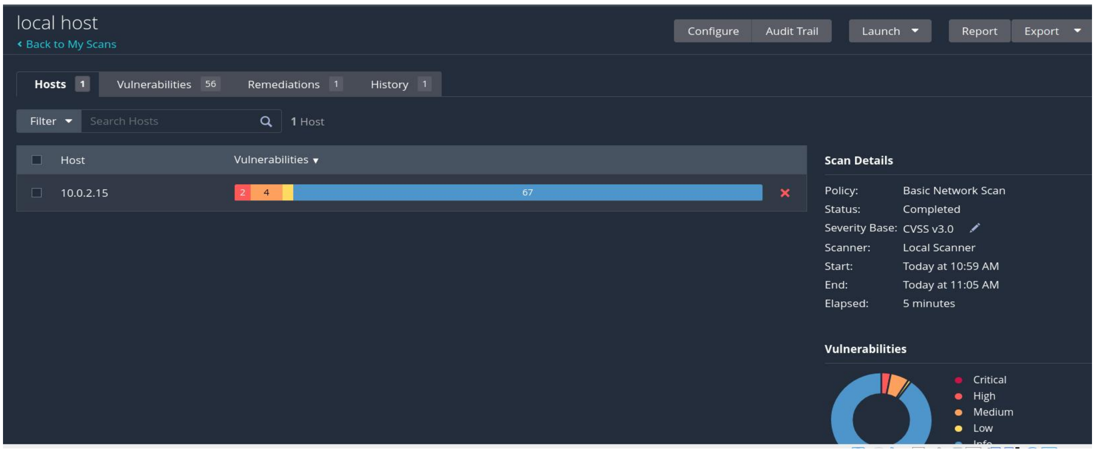


Name	local host
Description	basic network scanning on my local host
Folder	My Scans
Targets	10.0.2.15
Upload Targets	Add File



3 Scans

Name	Scan Type	Schedule	Last Scanned ▾
My Host Discovery Scan	Host Discovery	On Demand	Today at 10:58 AM
My Basic Network Scan	**Vulnerability**	**On Demand**	**Today at 9:25 AM**
local host	Vulnerability	On Demand	N/A



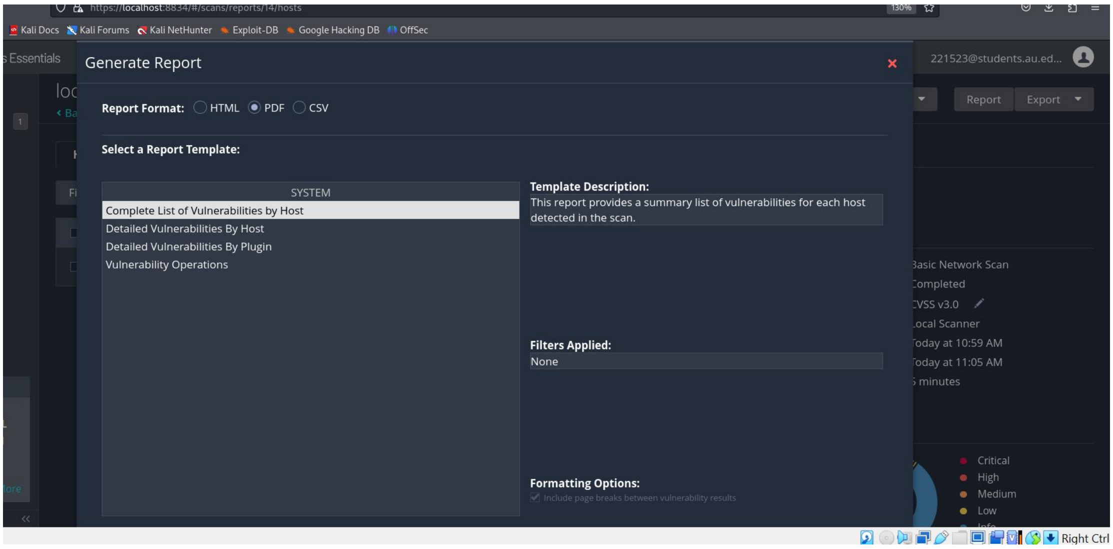
1 Host

Host	Vulnerabilities ▾
10.0.2.15	2 4 67

Scan Details

Policy:	Basic Network Scan
Status:	Completed
Severity Base:	CVSS v3.0
Scanner:	Local Scanner
Start:	Today at 10:59 AM
End:	Today at 11:05 AM
Elapsed:	5 minutes

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

Limitations

1. No Exploitation Capabilities

- Nessus only identifies vulnerabilities; it does not exploit them to verify their impact. For penetration testing, tools like Metasploit or manual testing are required.

2. False Positives & False Negatives

- Nessus may sometimes report vulnerabilities that are not actually exploitable (false positives) or fail to detect some vulnerabilities (false negatives), requiring manual verification.

3. Limited Web Application Scanning

- While Nessus can identify some web-based vulnerabilities, it is not a full-fledged web application scanner like Burp Suite or OWASP ZAP. It lacks advanced testing for SQL Injection, XSS, and authentication-based flaws.

4. Resource-Intensive Scanning

- Nessus scans can consume high CPU and network resources, potentially impacting system performance, especially on production environments.

5. Limited Zero-Day Detection

- Nessus relies on known vulnerability databases (CVE, plugins). It does not detect zero-day vulnerabilities or custom application security flaws.

…………………………………………………………………