JGi JAIN DEEMED-TO-BE UNIVERSITY | SCHOOL OF COMPUTER SCIENCE AND IT

Department of
**Bachelor of Computer Applications**

# Ethical Hacking Fundamentals

Lab File – CA 10

**Subject Code:** 19BCA4C02L
**Class:** II$^{nd}$ Year II$^{nd}$ Semester

Prepared By:
Suman Garai
20BCAR0246

## Aim :

Perform vulnerability scan on target system using Nessus in Kali Linux

## Requirements :

- Virtualisation Software
- Kali Linux 2022.1
- Basics of Nessus
- Internet Connection

## Objectives :

To Run Basic Network Scan, and Analyse the results obatined.

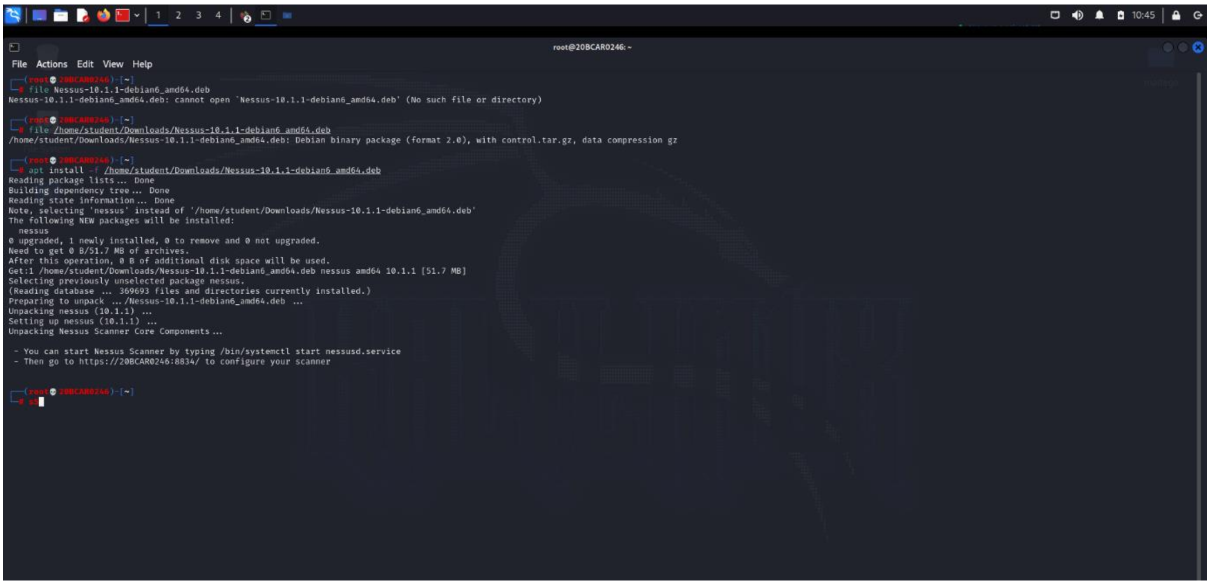
## Procedure :

Basics

For installation, we are going to do the following:

1> Open https://www.tenable.com/downloads/nessus?loginAttempted=true, and download the `Nessus-10.1.1-debian6_amd64.deb` package.

2> Thereafter, we are going to use the command `apt install -f <installation package location>`



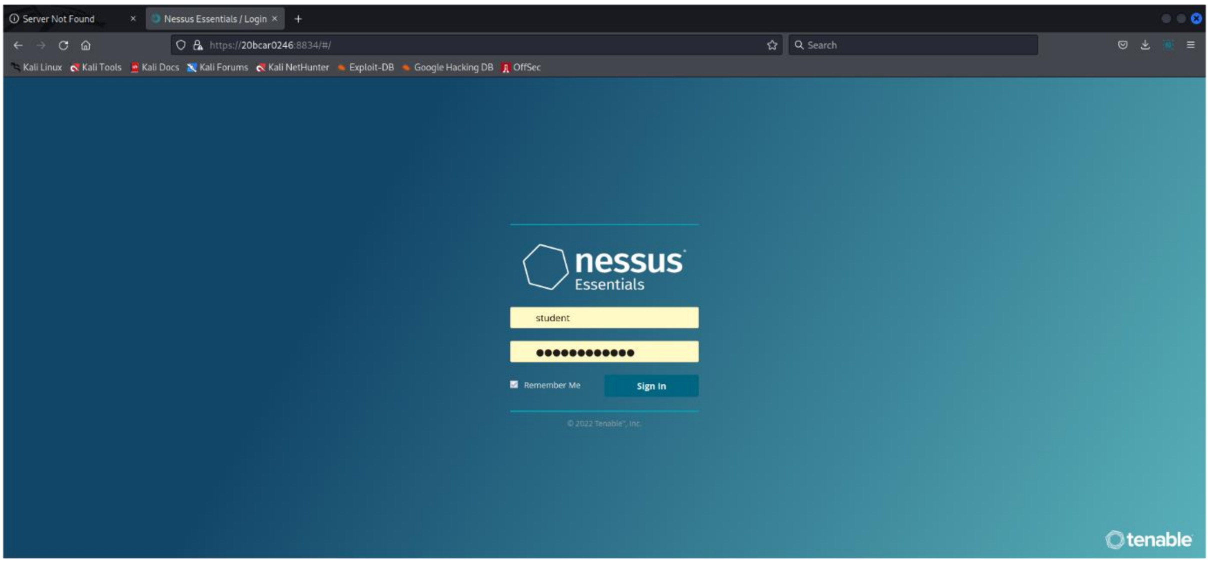
```
┌──(root💀20BCAR0246)-[~]
└─# file Nessus-10.1.1-debian6_amd64.deb
Nessus-10.1.1-debian6_amd64.deb: cannot open `Nessus-10.1.1-debian6_amd64.deb' (No such file or directory)

┌──(root💀20BCAR0246)-[~]
└─# file /home/student/Downloads/Nessus-10.1.1-debian6_amd64.deb
/home/student/Downloads/Nessus-10.1.1-debian6_amd64.deb: Debian binary package (format 2.0), with control.tar.gz, data compression gz

┌──(root💀20BCAR0246)-[~]
└─# apt install -f /home/student/Downloads/Nessus-10.1.1-debian6_amd64.deb
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Note, selecting 'nessus' instead of '/home/student/Downloads/Nessus-10.1.1-debian6_amd64.deb'
The following NEW packages will be installed:
  nessus
0 upgraded, 1 newly installed, 0 to remove and 0 not upgraded.
Need to get 0 B/51.7 MB of archives.
After this operation, 0 B of additional disk space will be used.
Get:1 /home/student/Downloads/Nessus-10.1.1-debian6_amd64.deb nessus amd64 10.1.1 [51.7 MB]
Selecting previously unselected package nessus.
(Reading database ... 369693 files and directories currently installed.)
Preparing to unpack .../Nessus-10.1.1-debian6_amd64.deb ...
Unpacking nessus (10.1.1) ...
Setting up nessus (10.1.1) ...
Unpacking Nessus Scanner Core Components...

 - You can start Nessus Scanner by typing /bin/systemctl start nessusd.service
 - Then go to https://20BCAR0246:8834/ to configure your scanner


┌──(root💀20BCAR0246)-[~]
└─# s5
```

The window appears like this. There are further instructions provided at the ending to get Nessus running. Do as instructed.

NOTE: To use Nessus, account is needed to be created and activation key is required.

## Procedure

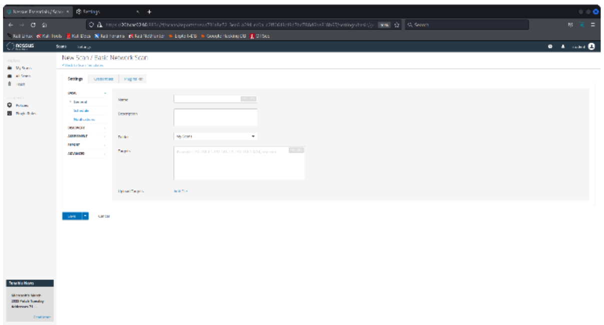
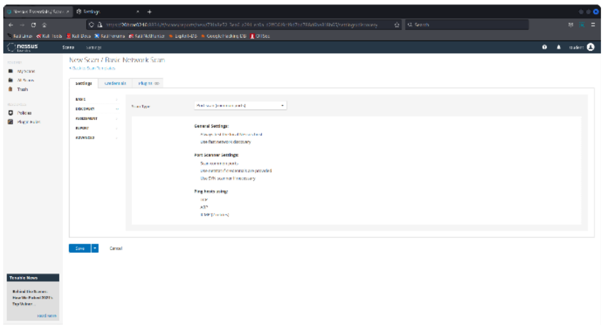
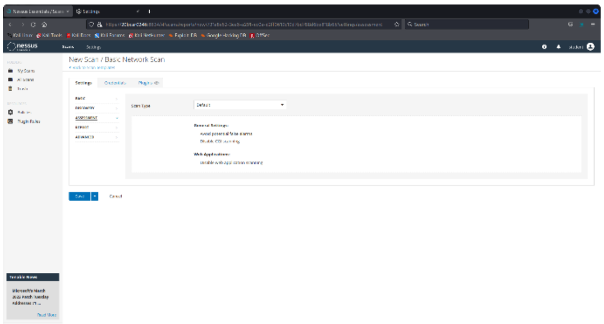
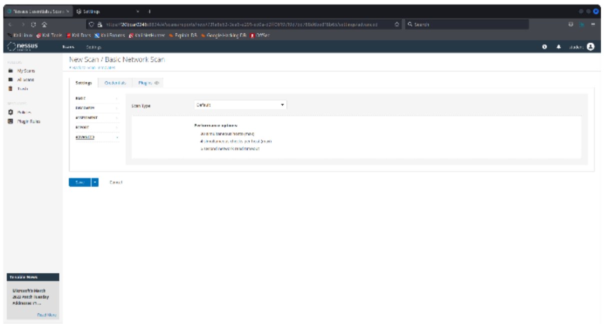
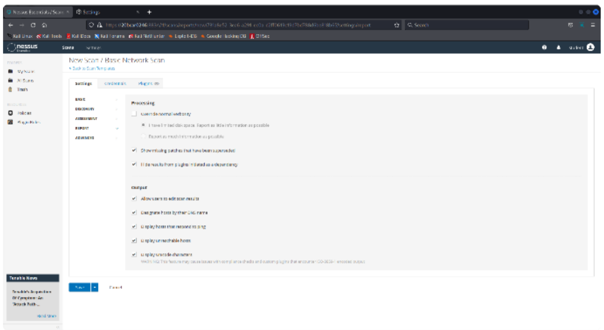
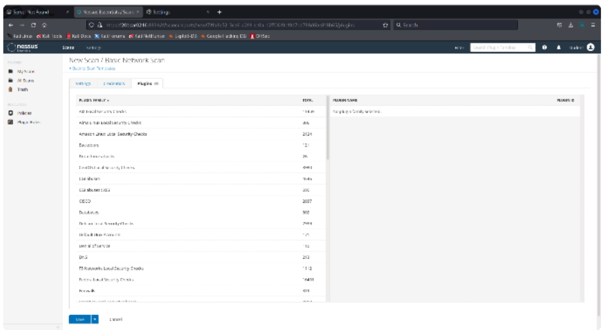
1> Login to Nessus, using the browser, to the My Scans Page.



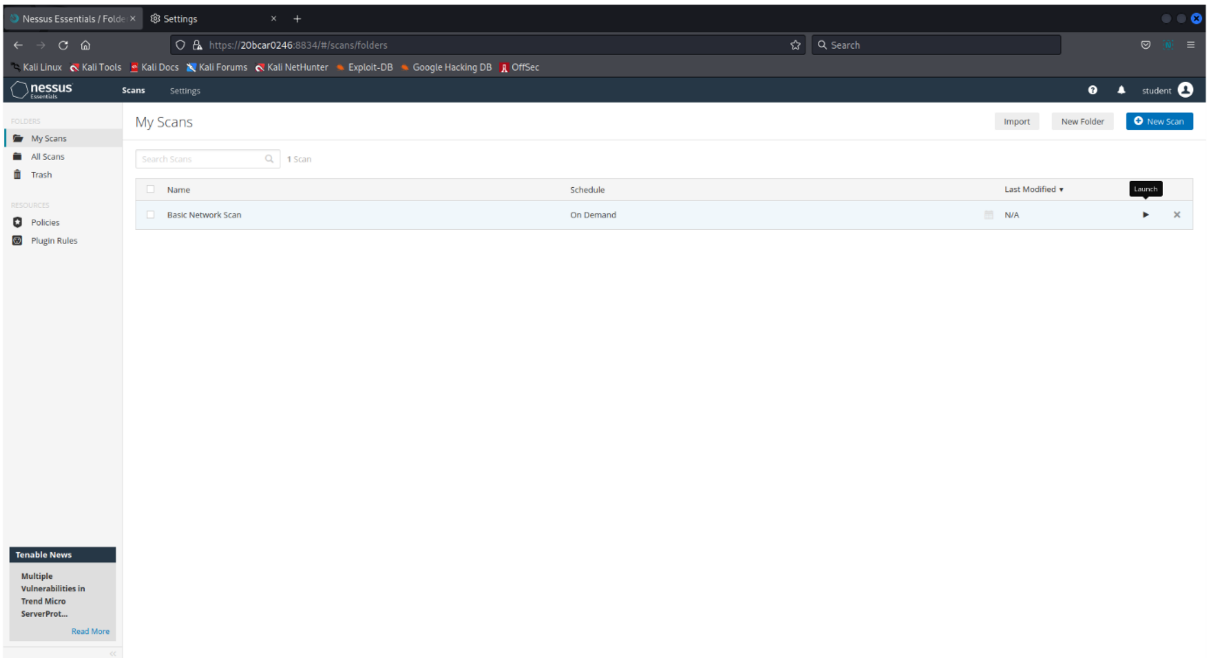
student

☑ Remember Me

2> Create a New Scan by customizing it accordingly.

3> Launch the Scan from My Scans Page.



My Scans

1 Scan

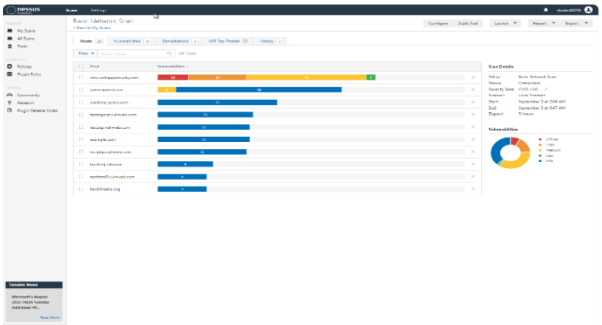
| ☐ | Name | Schedule | Last Modified ▾ |
|---|---|---|---|
| ☐ | Basic Network Scan | On Demand | N/A |

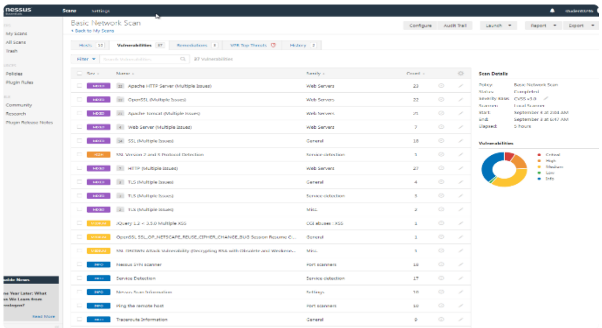
Tenable News

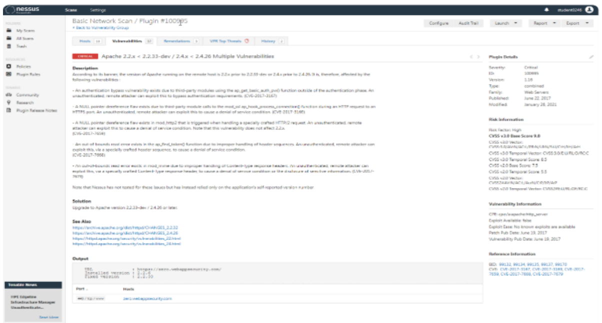
Multiple Vulnerabilities in Trend Micro ServerProt...

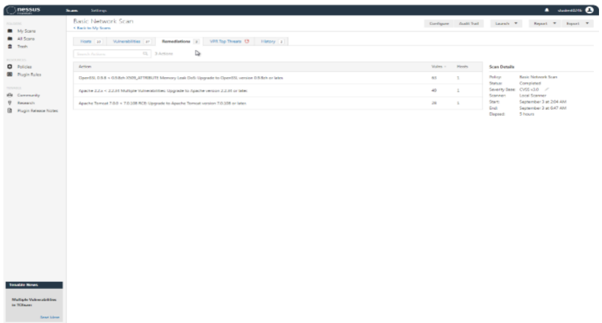
Read More

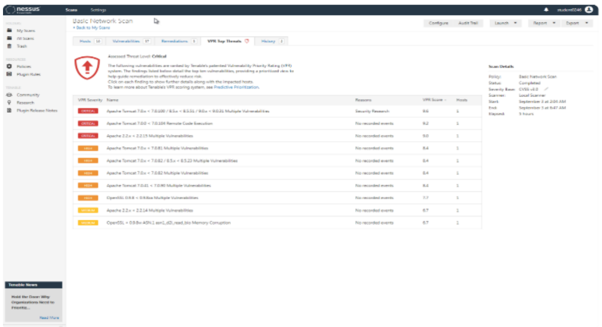
4> After the scan gets completed, results following, can be obtained:

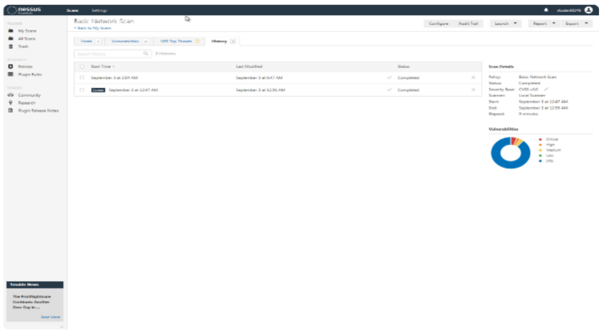




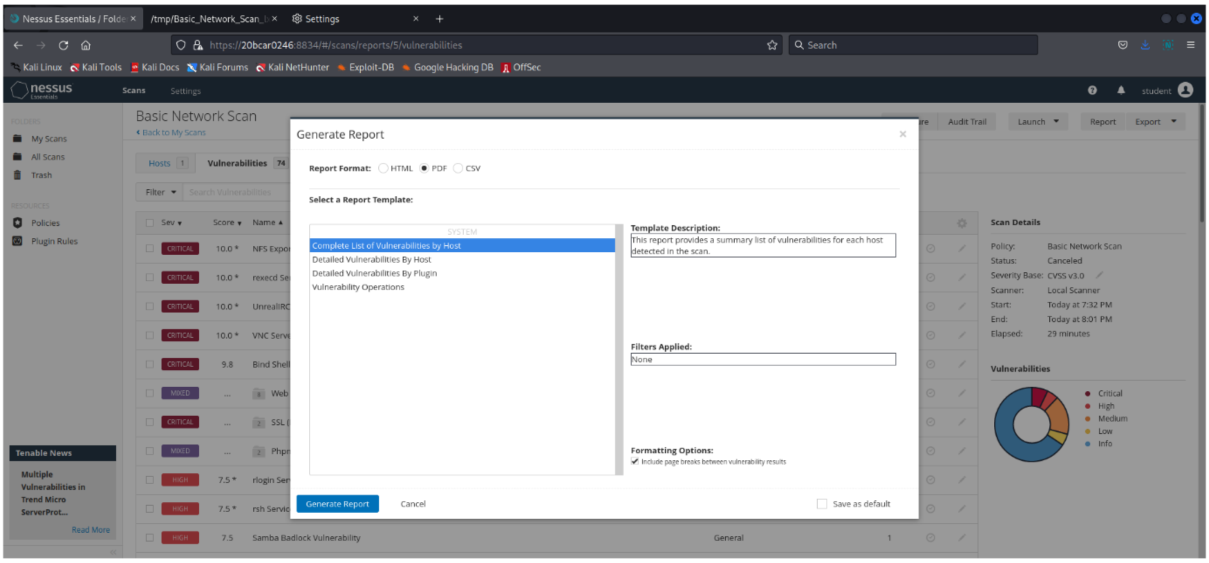








5> The obtained results, thereafter, can be exported by generating reports in different formats:



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

Generate Report  Cancel  □ Save as default

Scan Details

Policy: Basic Network Scan
Status: Canceled
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 7:32 PM
End: Today at 8:01 PM
Elapsed: 29 minutes

NOTE: For more details regarding the information obtained, head over to: https://drive.google.com/file/d/1KLaePWtaOooBYSdkxT76AWDGXnnoBTNX/view?usp=sharing

## Conclusion :

Nessus is a proprietary vulnerability scanner developed by Tenable, Inc. Tenable.io is a subscription-based service. Nessus is an open-source network vulnerability scanner that uses the Common Vulnerabilities and Exposures architecture for easy cross-linking between compliant security tools. In fact, Nessus is one of the many vulnerability scanners used during vulnerability assessments and penetration testing engagements, including malicious attacks. Nessus is a tool that checks computers to find vulnerabilities that hackers COULD exploit.

Nessus works by testing each port on a computer, determining what service it is running, and then testing this service to make sure there are no vulnerabilities in it that could be used by a hacker to carry out a malicious attack. Nessus performs its scans by utilizing plugins, which run against each host on the network in order to identify vulnerabilities.