

Department of

Bachelor of Computer Applications

**Ethical Hacking Fundamentals**

Lab File – CA 10

**Subject Code:** 19BCA4C02L

**Class:** IInd Year IInd 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 :**

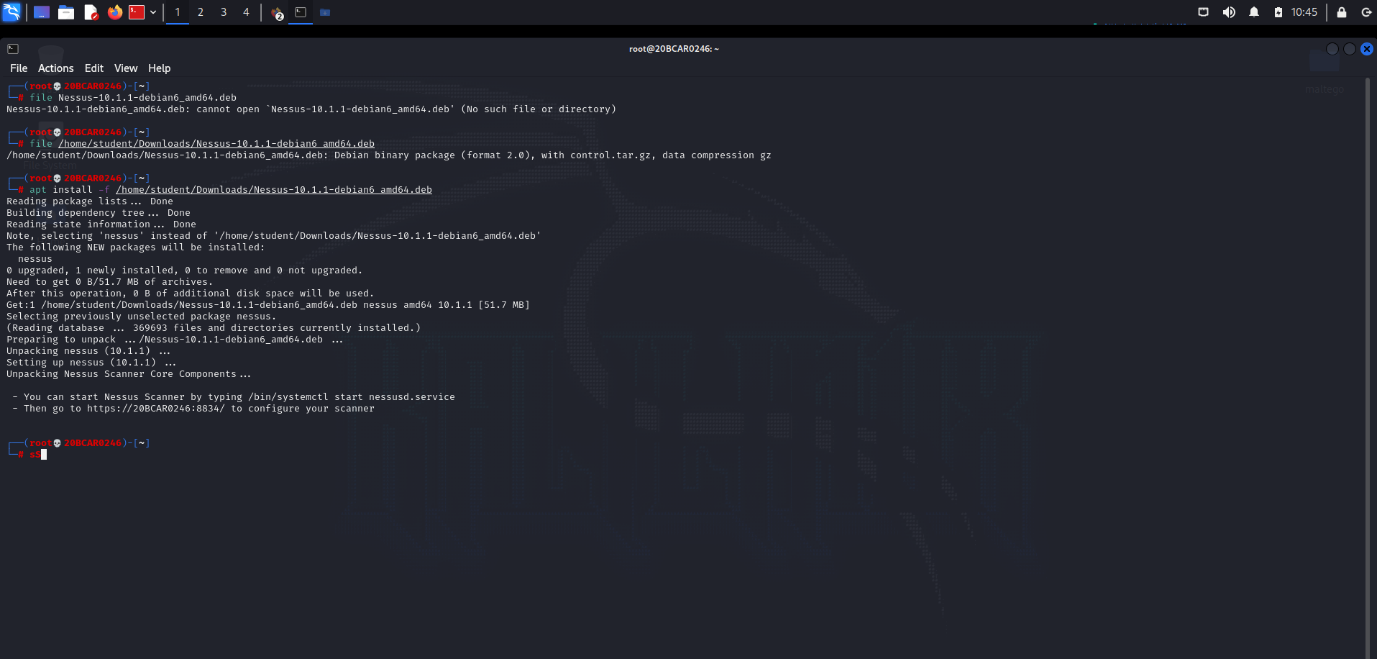
To Run Basic Network Scan, and Analyse the results obatined.

**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>

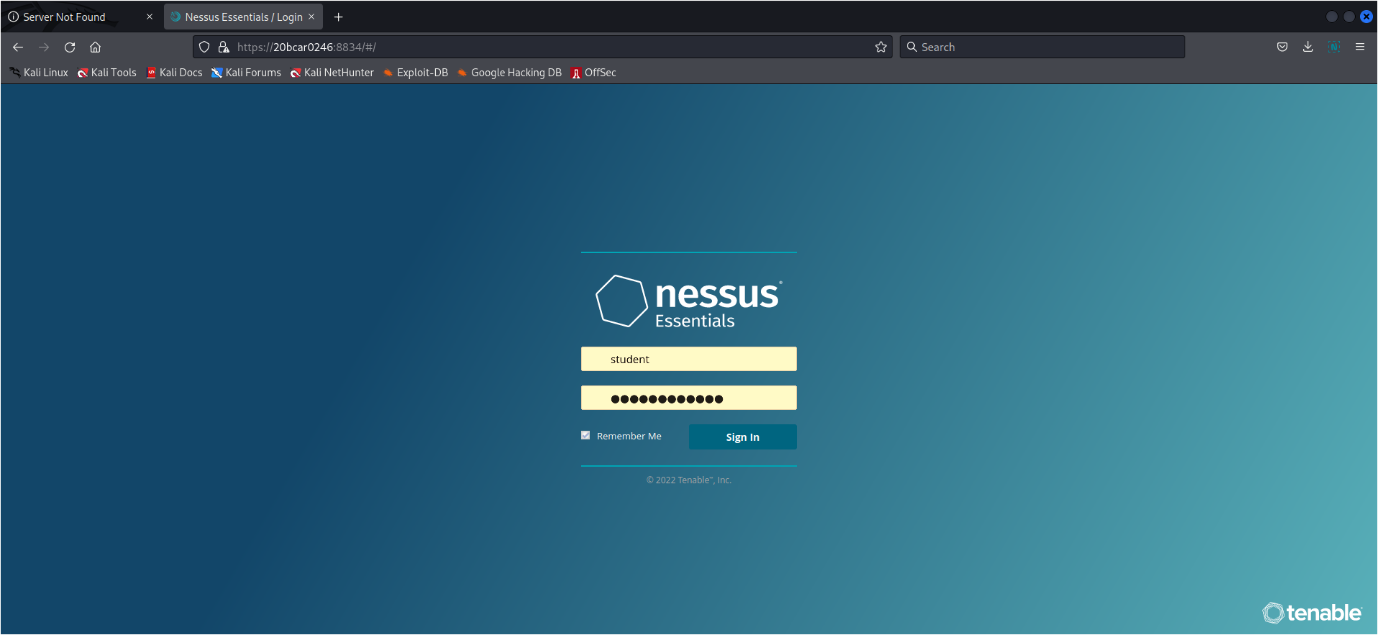


The window appears like this. There are further instructions provided at the ending to get Nessus running. Do as instructed.

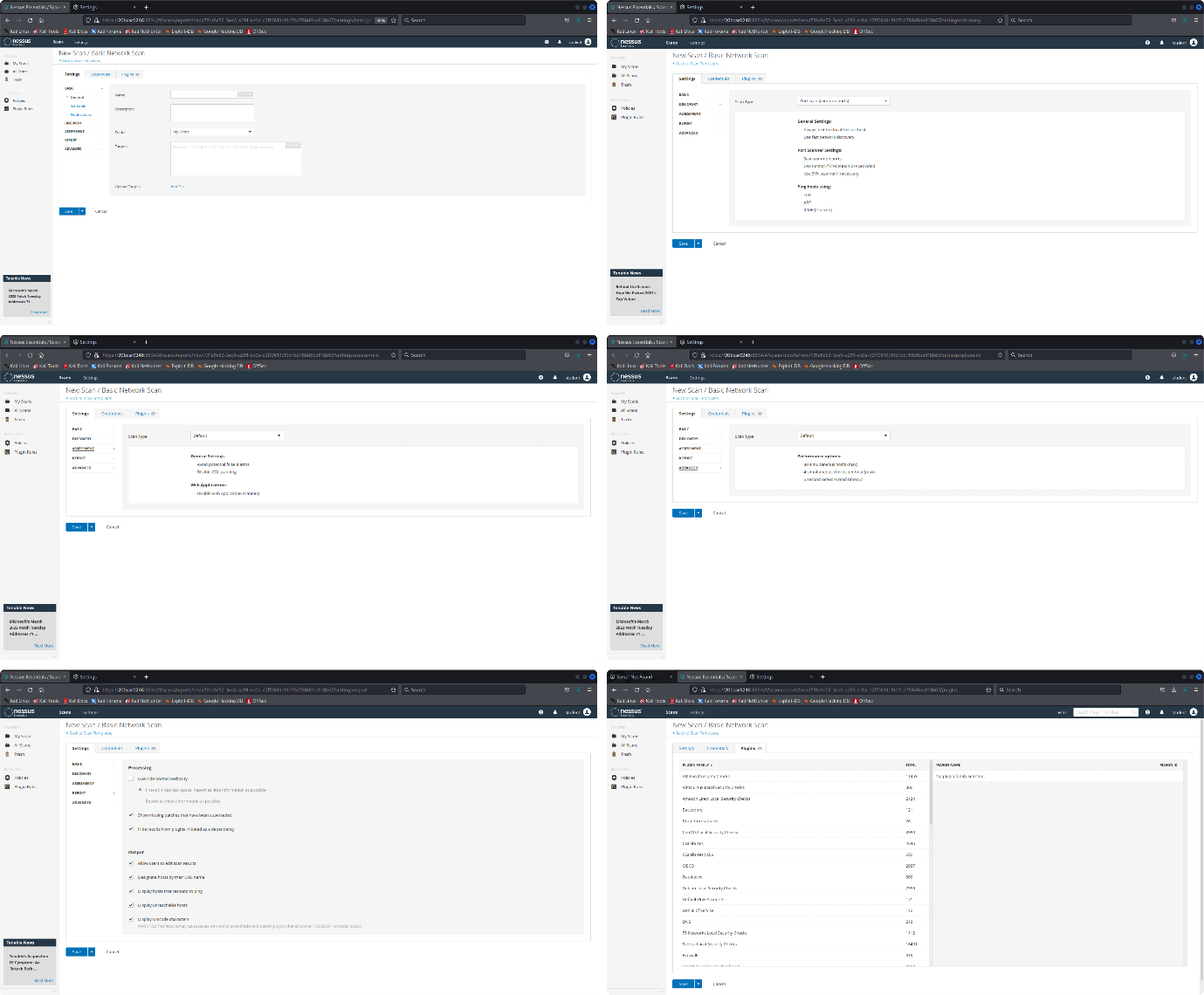
NOTE: To use Nessus, account is needed to be created and activation key is required.

Procedure

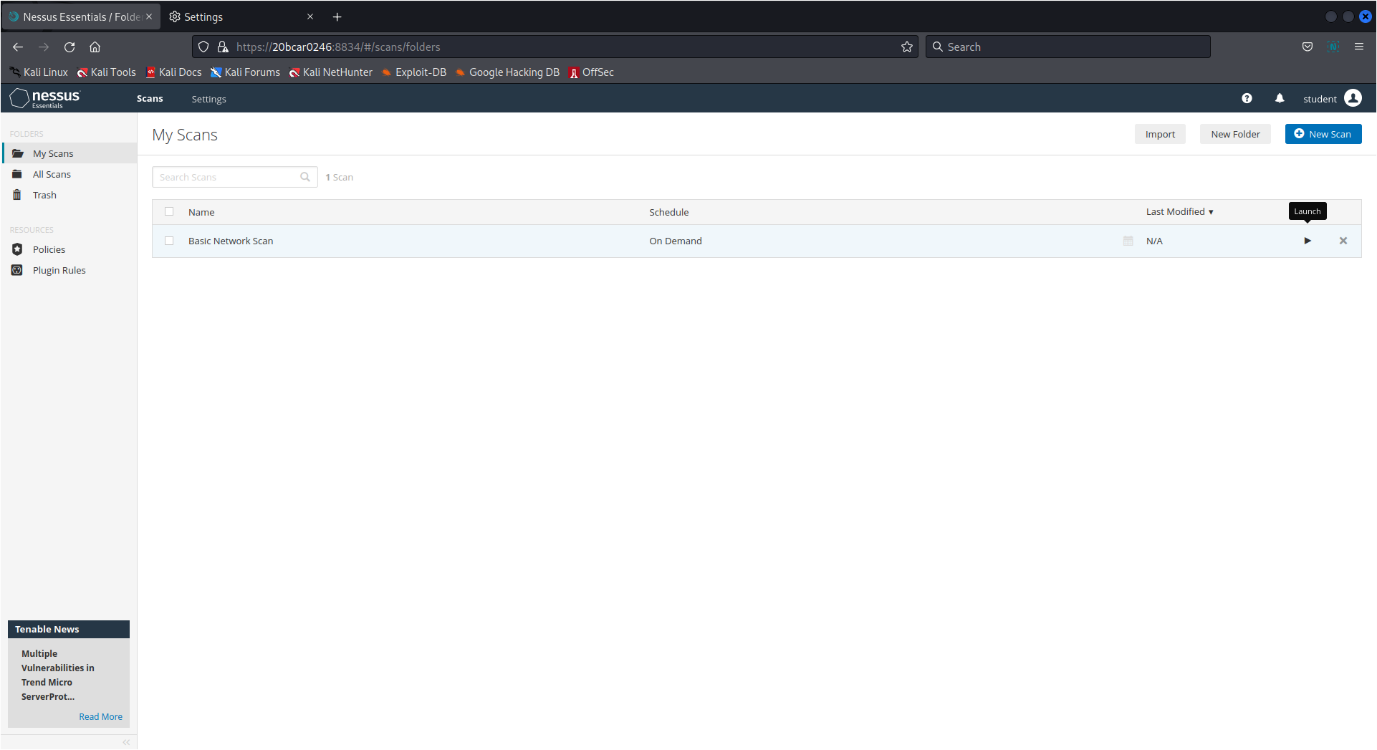
1. Login to Nessus, using the browser, to the My Scans Page.



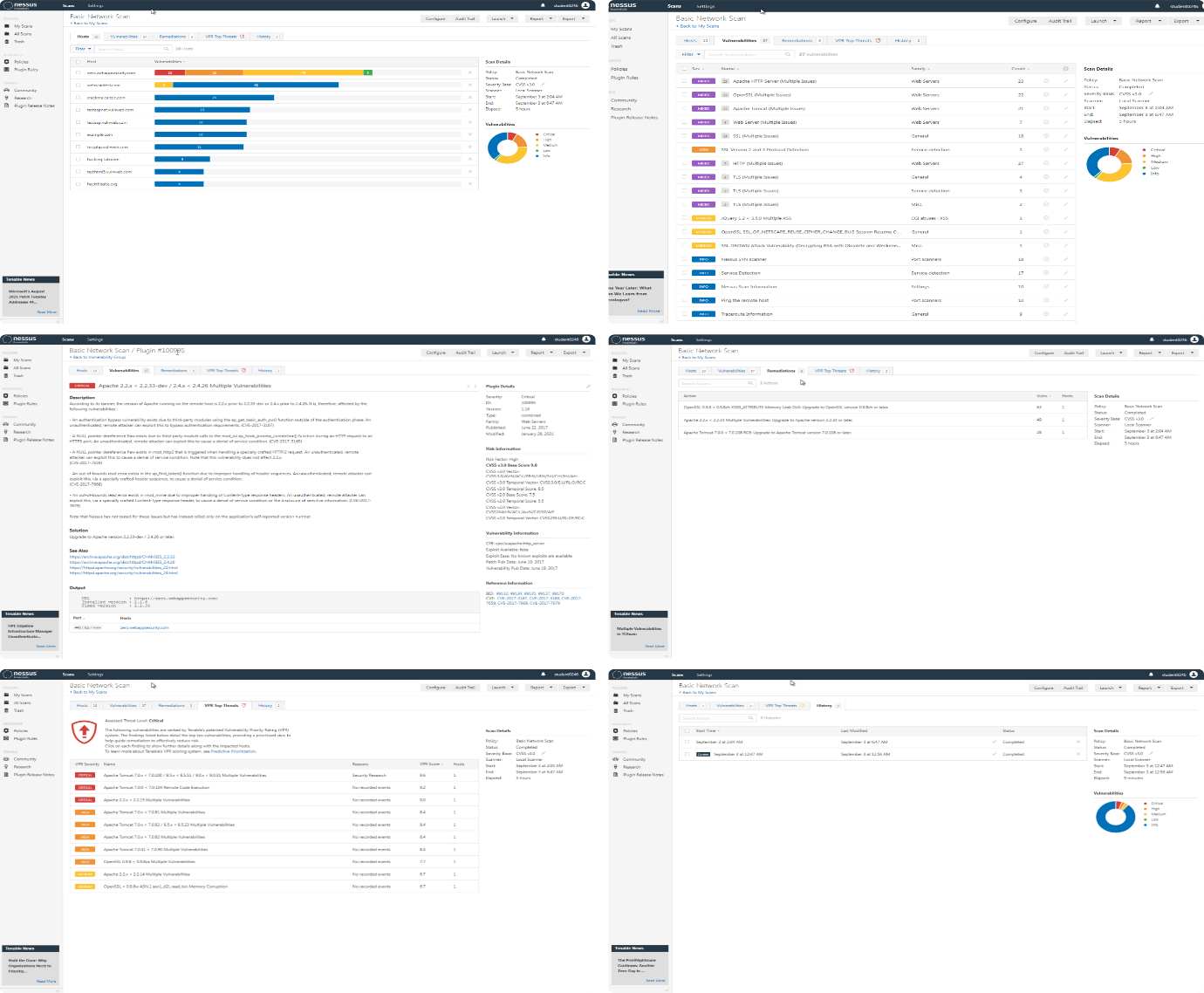
1. Create a New Scan by customizing it accordingly.



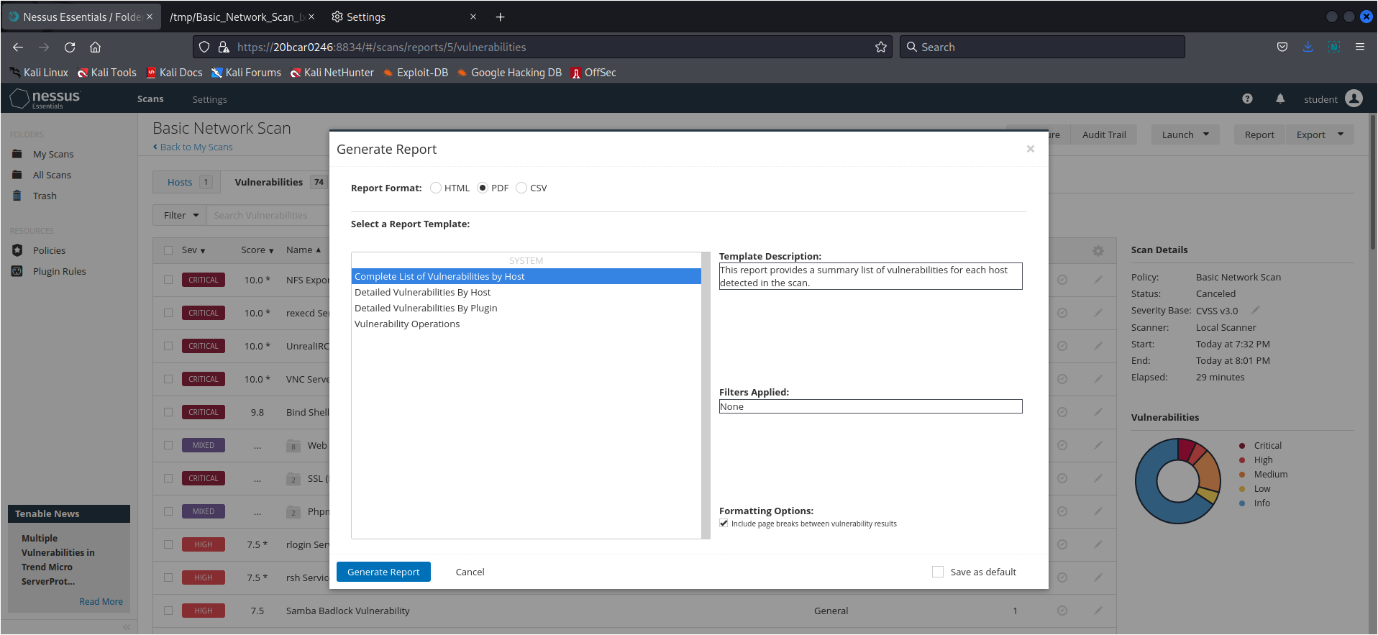
1. Launch the Scan from My Scans Page.



1. After the scan gets completed, results following, can be obtained:



1. The obtained results, thereafter, can be exported by generating reports in different formats:



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](https://www.itperfection.com/network-security/network-monitoring/what-is-network-vulnerability-scanning/) developed by [Tenable, Inc](https://www.tenable.com/). 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](https://www.itperfection.com/network-security/network-monitoring/vulnerability-scanning-tools-solarwinds-msp-openvas-nikto-nexpose-community-edition-manageengine-vulnerability-manager-plus-immuniweb/) 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.