**CY2004**

**Cyber Security**

**PROJECT**

**Understanding Nessus: A Fundamental Tool in the Cybersecurity Defense Arena**

**Submitted by:** Fatima Naeem , Sarita Sangrez

**Roll number:** 23I-2046 , 23I-2088

**Date:** 12th November 2024

**Table of Contents**

[Overview 3](#_Toc182341124)

[**Offensive Tools** 3](#_Toc182341125)

[**Defensive tools** 3](#_Toc182341126)

[Introduction 3](#_Toc182341127)

[Purpose of the Tool 3](#_Toc182341128)

[Cyber Security Domain 4](#_Toc182341129)

[Step-by-Step Installation and Configuration Manual for Nessus 4](#_Toc182341130)

[**Prerequisites** 4](#_Toc182341131)

[**Process** 4](#_Toc182341132)

[**Summary** 12](#_Toc182341133)

[Scenario for Tool Usage 12](#_Toc182341134)

[Conclusions 13](#_Toc182341135)

[References 13](#_Toc182341136)

**Understanding Nessus: A Fundamental Tool in the Cybersecurity Defense Arena**

## Overview

*Security is not a product, but a process." — Bruce Schneier*

In cybersecurity, tools are divided into two primary categories:

* offensive
* defensive.

**Offensive Tools** are designed to simulate attacks and identify weaknesses in systems, allowing security professionals to understand potential vulnerabilities from an attacker’s perspective. Examples include penetration testing frameworks, exploitation tools, and social engineering kits.

**Defensive tools**, on the other hand, focus on protecting systems from attacks, identifying vulnerabilities, and ensuring compliance with security standards. These include firewalls, intrusion detection systems, antivirus software, and vulnerability assessment tools.

## **Introduction**

**Nessus** is a **vulnerability assessment** defensive cybersecurity tool developed

by Tenable, Inc. It enables organizations to **identify**, **assess**, and **remediate** vulnerabilities within their IT infrastructure. Since its launch in 1998, Nessus has become a critical component of many security programs, providing comprehensive scanning capabilities across a wide range of platforms, including operating systems, network devices, databases, and web applications. By utilizing Nessus, organizations can proactively strengthen their security posture and mitigate risks before they can be exploited by malicious actors.

## Purpose of the Tool

The primary purpose of Nessus is to conduct thorough vulnerability assessments to identify security weaknesses in systems and networks. Key functionalities include:

1. **Vulnerability Scanning**: Nessus scans systems to detect known vulnerabilities based on a regularly updated database of Common Vulnerabilities and Exposures (CVEs).
2. **Configuration Auditing**: The tool evaluates system configurations against best practices and compliance standards to ensure secure settings.
3. **Malware Detection**: Nessus can identify potential malware on systems, aiding in the prevention of data breaches.
4. **Reporting and Visualization**: It offers detailed reports and dashboards that summarize findings, making it easier for security teams to understand vulnerabilities and prioritize remediation efforts.
5. **Integration Capabilities**: Nessus can integrate with various security information and event management (SIEM) platforms and ticketing systems, streamlining security workflows.

## Cyber Security Domain

Nessus primarily operates within the defensive cybersecurity domain. Its capabilities are focused on identifying vulnerabilities and weaknesses before they can be exploited by malicious actors. By conducting proactive assessments, organizations can strengthen their defenses and reduce the risk of security incidents. While Nessus itself is not an offensive tool like penetration testing frameworks, it plays a critical role in the overall security strategy by providing the necessary insights for defensive measures and remediation efforts.

## Step-by-Step Installation and Configuration Manual for Nessus

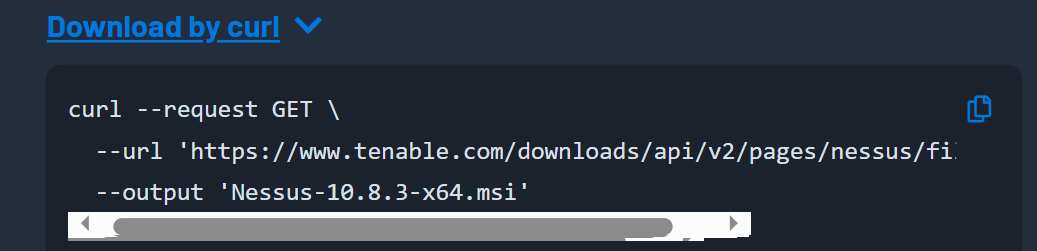
### **Prerequisites**

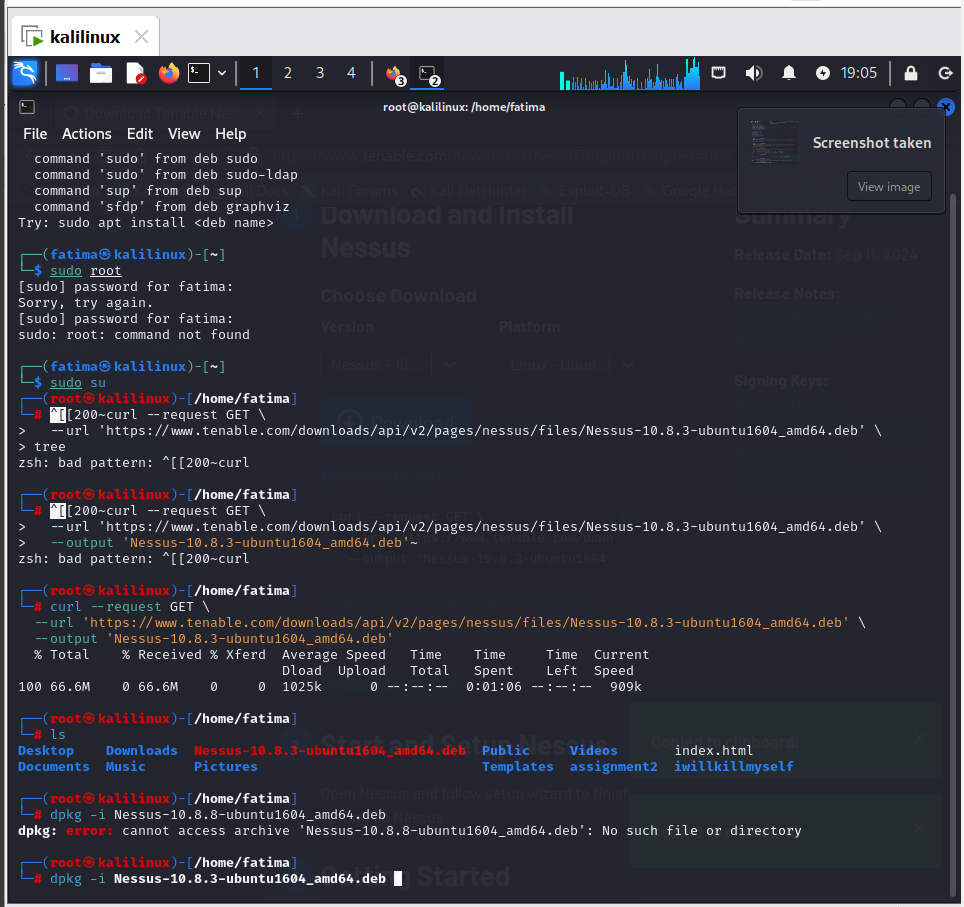
Before installing Nessus, ensure that your system meets the following requirements:

* **Operating System:** Nessus supports Windows, Linux (various distributions), and macOS.  Hardware Requirements
  + Processor\*: 1 GHz or higher
  + RAM\*: Minimum 2 GB (4 GB recommended)
  + Disk Space\*: Minimum 20 GB of free disk space
* Software Dependencies: For Linux, you may need to install additional packages depending on the distribution (e.g., libc6, libstdc++, etc.).

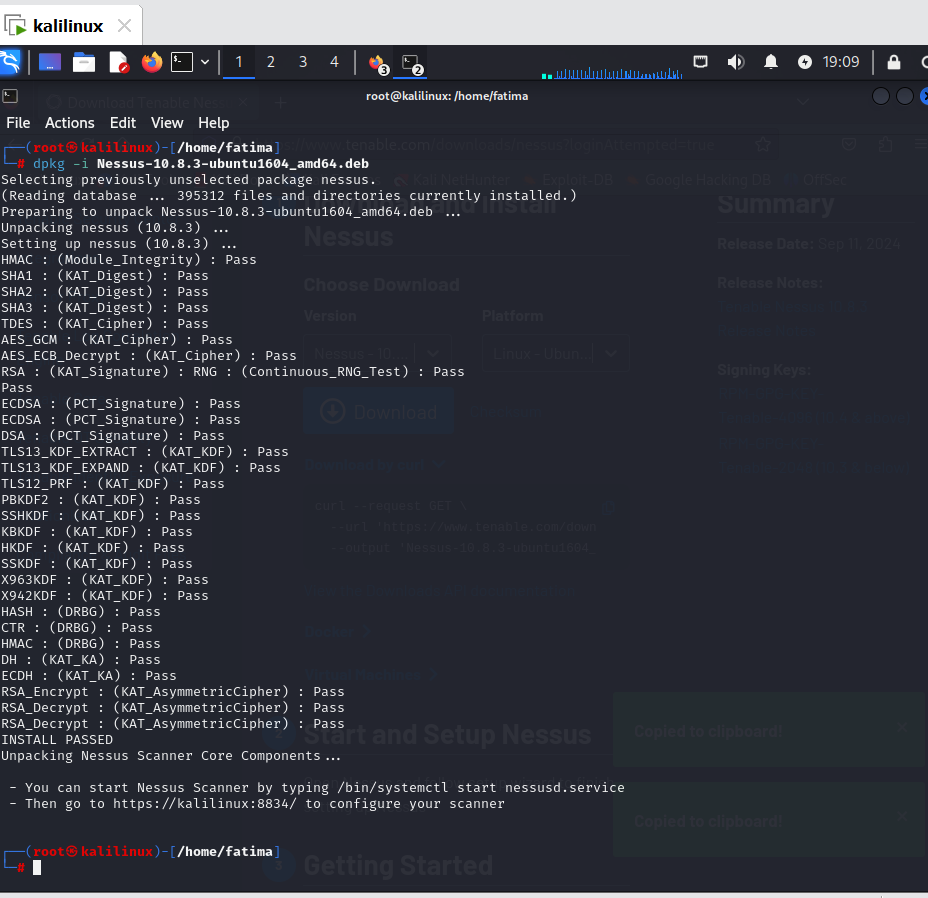
### **Process**

1. Official Website: [https://www.tenable.com.](https://www.tenable.com./)
2. In "Products" and select "Nessus."
3. Choose the Version: Select the version you want (Nessus Essentials, Nessus Professional, etc.).
4. Then copy the curl command onto your terminal and press enter .



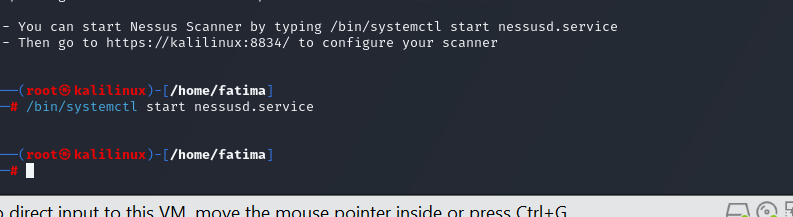
 Here we used the ls command to see if it downloaded.

1. Now using the dpkg command we will install the Nessus onto our system.



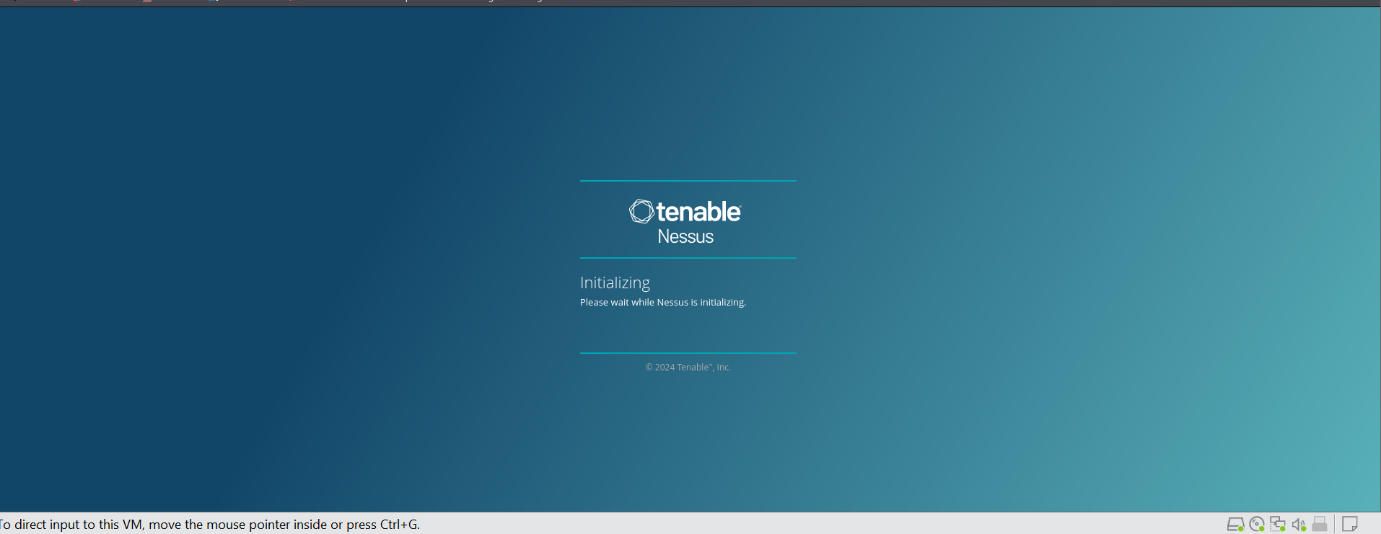
* **dpkg -i**: The -i option tells dpkg to install the specified .deb package.
* **Nessus-10.8.3-ubuntu1604\_amd64.deb**: This is the package file for Nessus version 10.8.3, specifically built for 64-bit Ubuntu 16.04.

1. Now we will start the Nessus service **(nessusd.service**) on your system by running the following command.

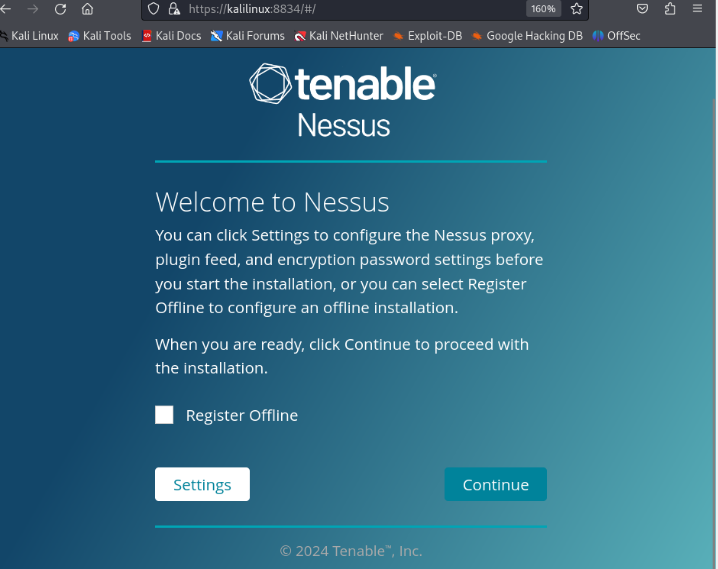


1. To see if the installation has actually started we go to the link that we get through the dpkg command. The instruction are given in it.

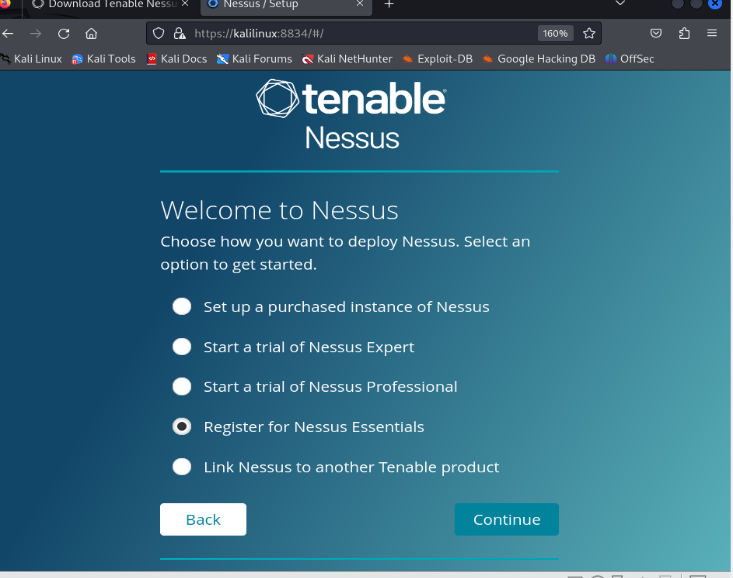
Here we can the installation has started.



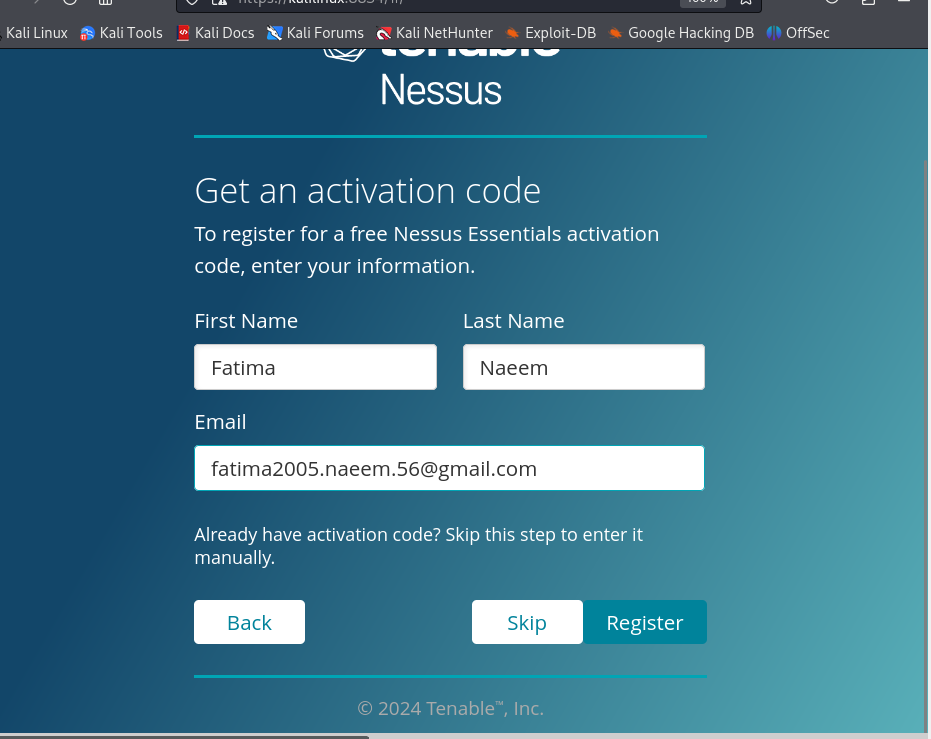
1. After installation you will come across this interface. Click **Continue**.



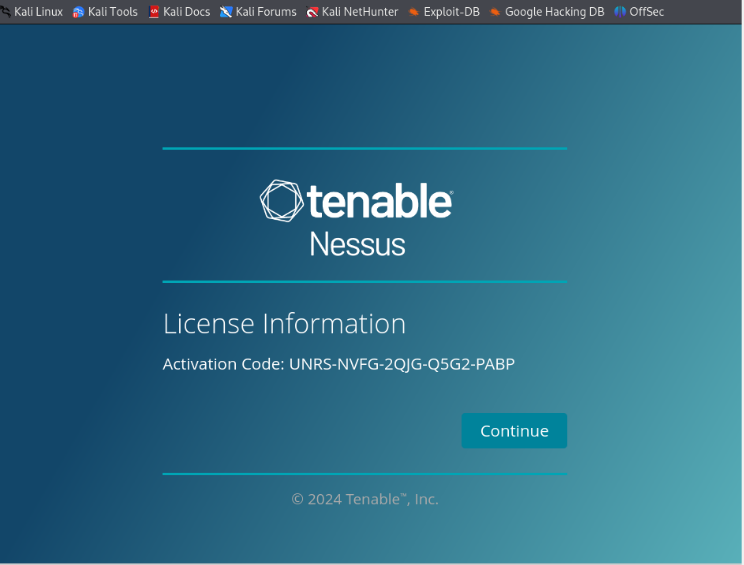
1. Select **Register for Nessus Essentials** and click **Continue**.



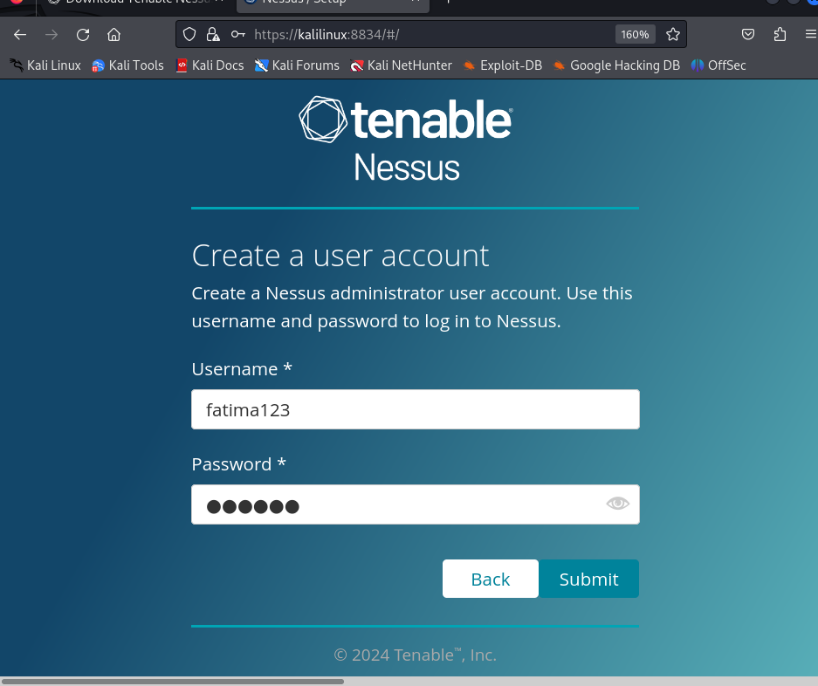
1. Enter your **First** **Name**, **Last Name**, **Email** and click **Register**.



1. You will be provided with an **Activation Code** save this code in a safe place for later use. Click **Continue**.



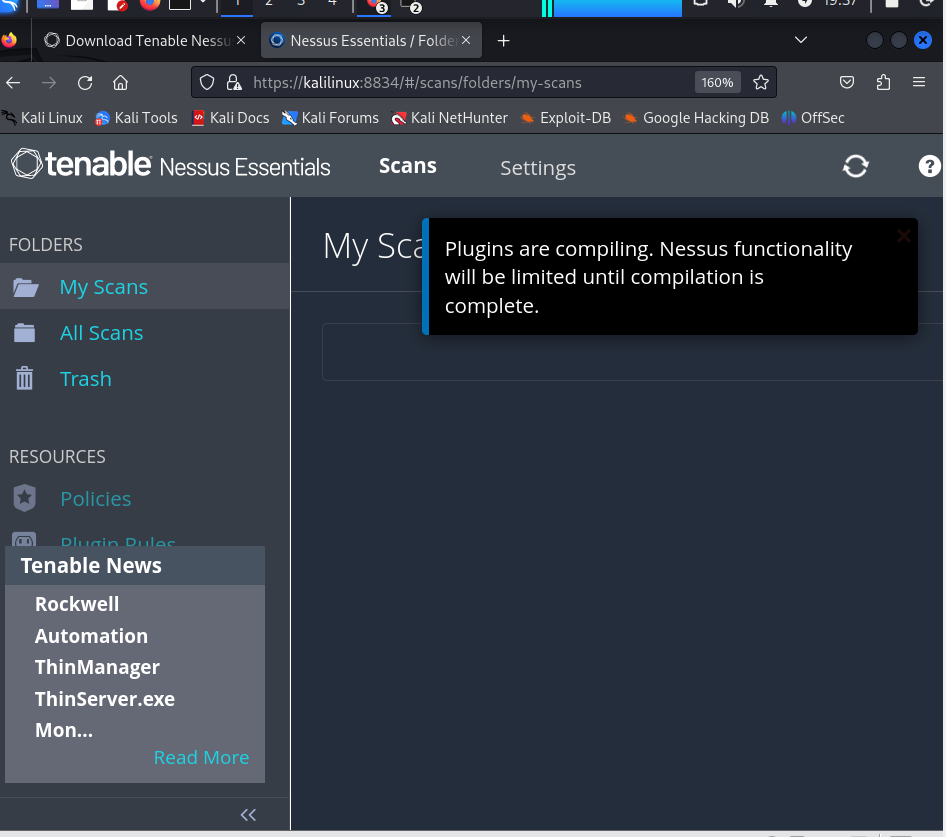
1. Create your account by choosing your **username** and **password** and then click **Submit**.



1. Wait for it to **initialize**. The time depend on your internet speed.

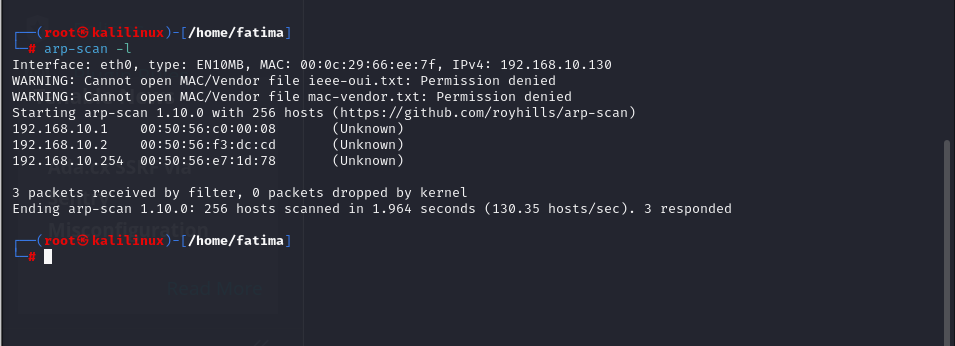


1. After initializing you will be directed to the following page. Wait for the **Plugins** to completely compile , this may take a while.

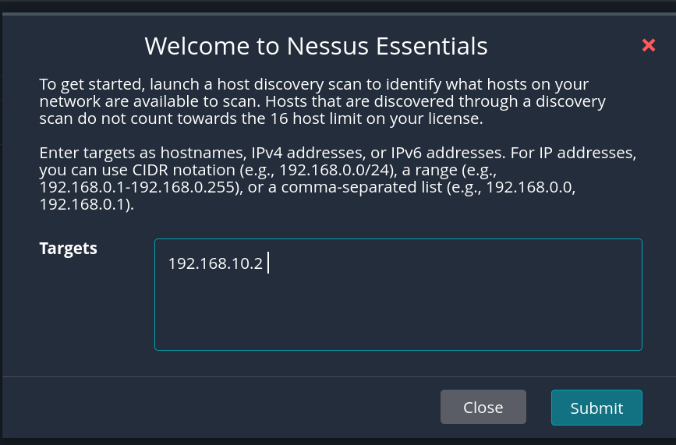
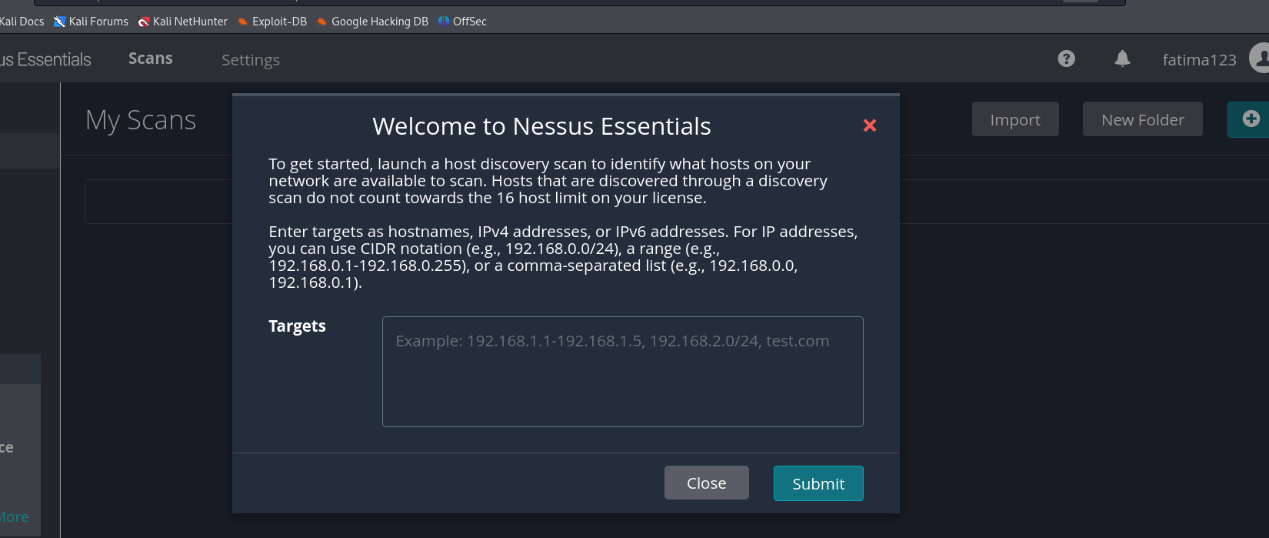


1. Going back to the terminal we are going to run the following command.

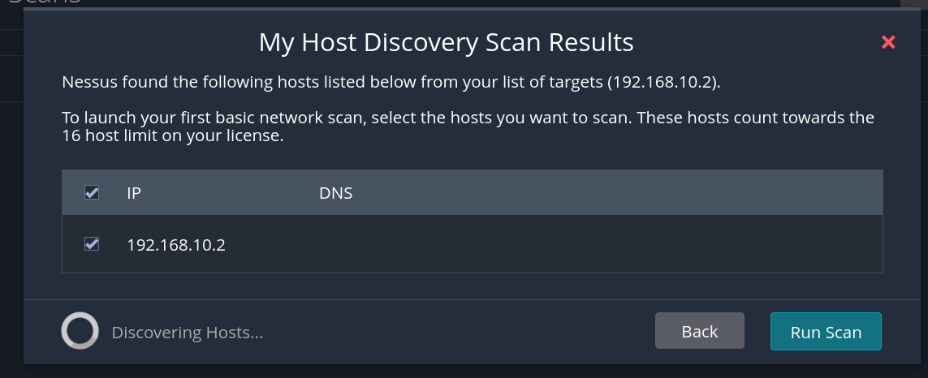
The **arp-scan -l** command is used to scan the local network and discover all devices connected to it .



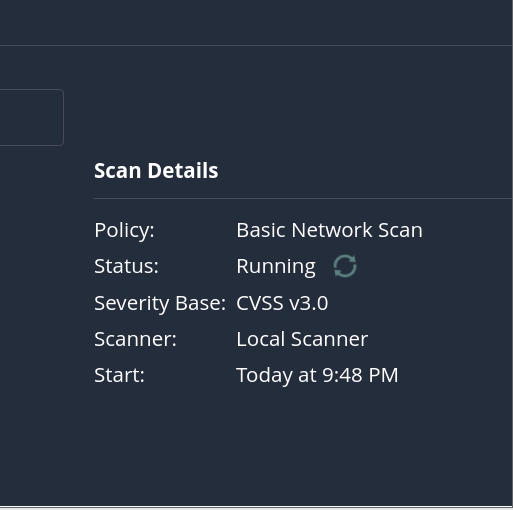
1. After your Plugins are done you will meet will the following interface. Here we will enter any **IP address** that we discovered from the last step to check it for any vulnerabilities.



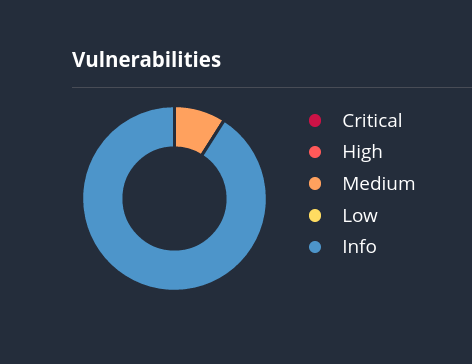
1. Select your **IP** and click **Run** **scan**.



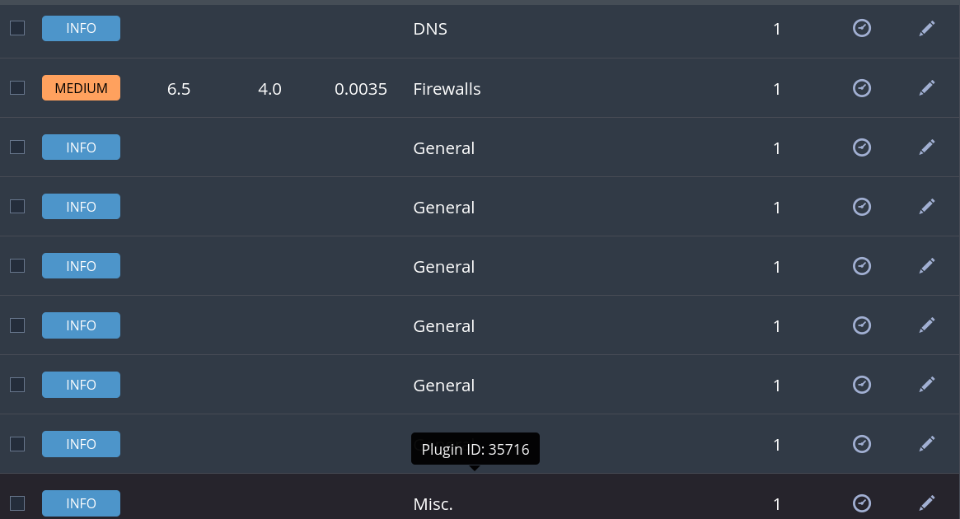
1. On the right bottom corner you can see your **Scan Details**.



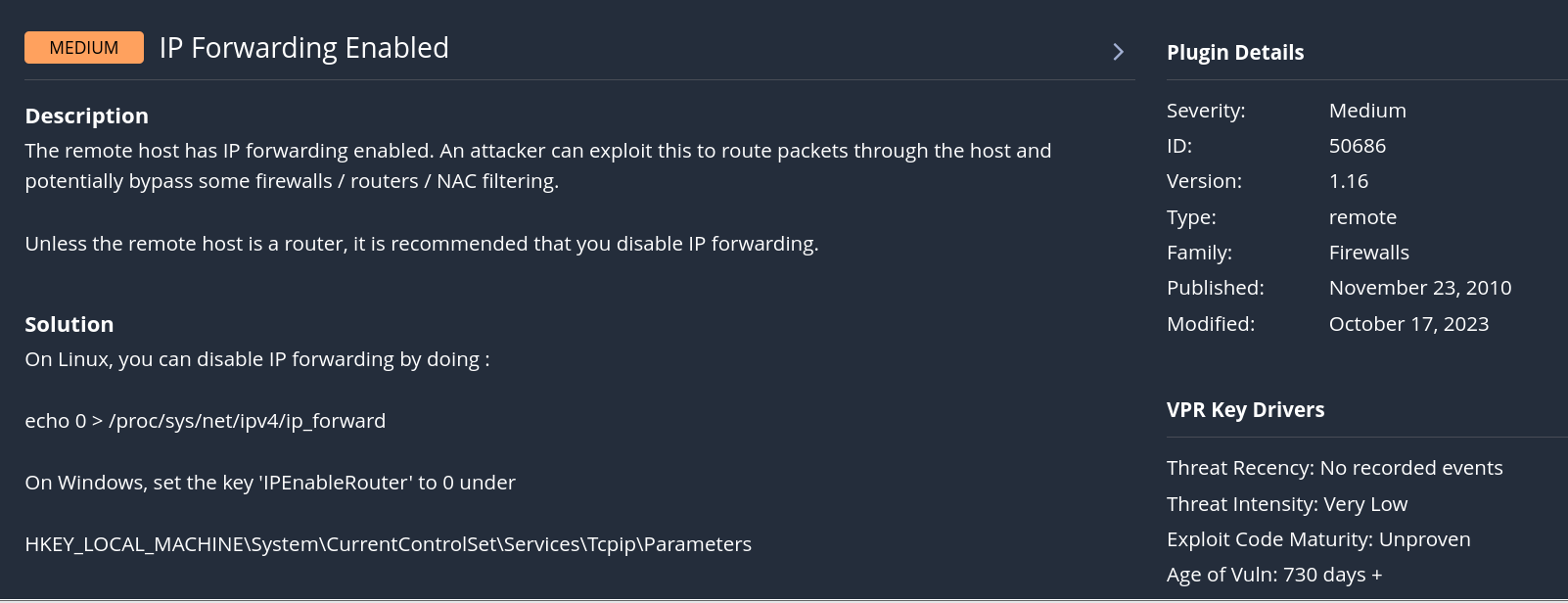
1. After your scan is completed you can if any **vulnerabilities** are found and if yes what is their **severity** and this is indicated by different **colours.** A detailed report is generated listing all vulnerabilities along with their solutions.



1. Click on your scan and you will be given more details regarding your IP. Here I can see that I have middle severity vulnerablity indicated by the orange colour. Click on it.



1. Now the best thing about Nessus is it also provides you will solution for your Vulnerabilities. Here it is providing me with descriptions of my issue and solution along with it.



This way you can do more scans in your MY SCAN window to launch more scans. The history of your scans is also maintained to track Vulnerability trends.

### **Summary**

To initiate a vulnerability assessment, navigate to the “Scans” section and click on “New Scan.” Here, you will be presented with various scan templates. Choose a template that aligns with your assessment requirements. For instance, if you are conducting a broad evaluation of your network, the Basic Network Scan template may be suitable. Conversely, if you are specifically targeting a web application, opt for the Web Application Test template.

Input the target IP addresses or ranges you wish to assess. It’s essential to include all relevant systems, such as servers, network devices, and endpoints. You can also configure additional settings, such as the scan schedule, to automate regular assessments, and notification preferences, so that the appropriate team members are alerted upon scan completion.

Once you have finalized the scan configuration, save your settings and click "Launch" to start the vulnerability scan. Nessus will begin scanning the specified targets, comparing them against its extensive database of known vulnerabilities and configuration issues.

After the scan is complete, you can review the results in the dashboard. Nessus categorizes vulnerabilities based on severity levels—critical, high, medium, and low—and provides detailed descriptions and remediation recommendations for each identified issue. This categorization helps prioritize your response efforts, allowing you to focus on the most critical vulnerabilities first.

## Scenario for Tool Usage

Imagine a financial institution that has recently integrated a new online banking system with its existing infrastructure. Given the sensitive nature of financial data, the organization’s cybersecurity team recognizes the need for a thorough vulnerability assessment to identify potential weaknesses in both their legacy systems and the new online platform.

To begin, the cybersecurity team uses Nessus to create a comprehensive scan that includes all critical components of the IT environment, including on premises servers, network devices, and the cloud infrastructure supporting the online banking application. They select the appropriate scan templates tailored for both network and web application assessments, ensuring that they cover all potential attack vectors.

Once the scan is launched, Nessus diligently analyzes each component, identifying vulnerabilities such as outdated software versions on legacy systems and misconfigured security settings on the new online banking platform. The team receives a detailed report summarizing the vulnerabilities found, complete with severity ratings and actionable remediation steps.

Upon reviewing the findings, the cybersecurity team prioritizes the remediation efforts based on the criticality of the vulnerabilities. They work closely with IT staff to patch outdated software, strengthen access controls, and adjust configurations to mitigate identified risks. This proactive approach not only enhances the security posture of the organization but also ensures compliance with stringent regulatory requirements governing financial institutions.

## Conclusions

Nessus is a vital vulnerability assessment tool that helps organizations identify and remediate various weaknesses in their IT infrastructure, including outdated software, misconfigurations, weak passwords, and unpatched systems. By providing comprehensive scanning, configuration auditing, and detailed reporting, it enables security teams to prioritize vulnerabilities effectively. Its use in assessing environments, such as a financial institution's online banking system, highlights its role in enhancing security posture and ensuring compliance, ultimately strengthening an organization's overall cybersecurity strategy.

## References

1. Tenable, Inc. - Nessus Product Page <https://www.tenable.com/products/nessus>
2. Nessus User Guide <https://docs.tenable.com/nessus/Content/GettingStarted.htm>
3. Common Vulnerabilities and Exposures (CVE)

[https://cve.mitre.org/](https://cve.mitre.org/](https://cve.mitre.org/%5D(https:/cve.mitre.org/)

1. Nessus Essentials: Free Vulnerability Scanning <https://www.tenable.com/products/nessus/essentials>5. Vulnerability Management Best Practices <https://www.tenable.com/blog/vulnerability-management-best-practices>
2. Nessus vs. Other Vulnerability Scanners <https://www.securitymetrics.com/blog/nessus-vs-other-vulnerability-scanners>
3. Understanding Vulnerability Scanning [https://www.csoonline.com/article/3531346/understanding-vulnerabilityscanning.html](https://www.csoonline.com/article/3531346/understanding-vulnerability-scanning.html)
4. The Importance of Vulnerability Assessments [https://www.cyber.gov.au/acsc/view-all-content/publications/importancevulnerability-assessments](https://www.cyber.gov.au/acsc/view-all-content/publications/importance-vulnerability-assessments)
5. 9. Nessus Security Center <https://www.tenable.com/products/tenable.io>

10. \*Cybersecurity Frameworks and Standards <https://www.nist.gov/cyberframework>