***Vulnerability Scanning with Nessus***

Description:

This repository provides a guide for conducting vulnerability scanning using Nessus within a Kali Linux environment. Nessus is a powerful vulnerability scanner that aids in identifying security weaknesses across networks, systems, and applications.

Requirements:

- Kali Linux operating system

- Docker program with the Nessus image

- Internet connection

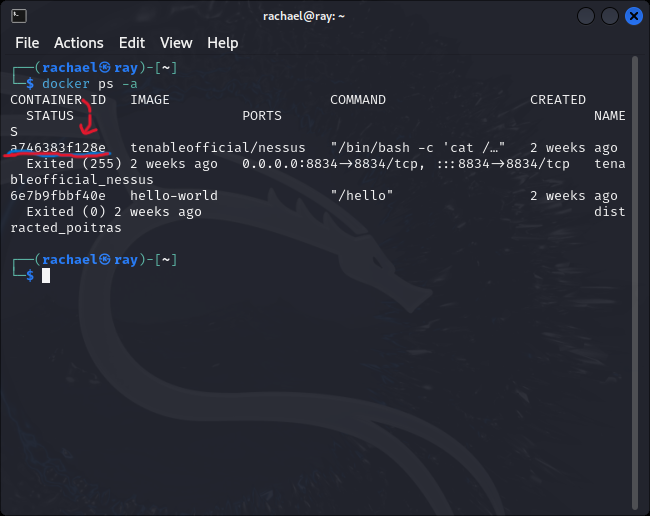
Instructions:

Ensure the Docker program is installed on your Kali Linux system.

1. To start and run the Nessus image, first, copy the container ID for the desired Nessus image using the following command:

> docker ps -a

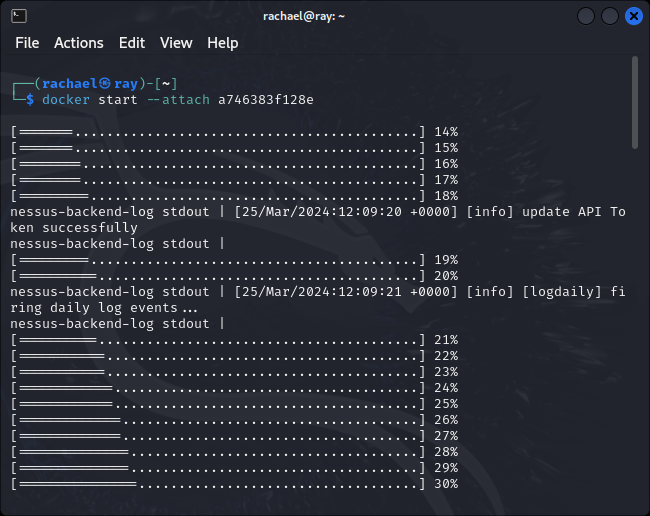
This command will display a list of all Docker containers along with their respective container IDs. Locate the container ID associated with the Nessus image you wish to start and run.



2. Once you have copied the container ID, execute the following command to start and attach to the Nessus container:

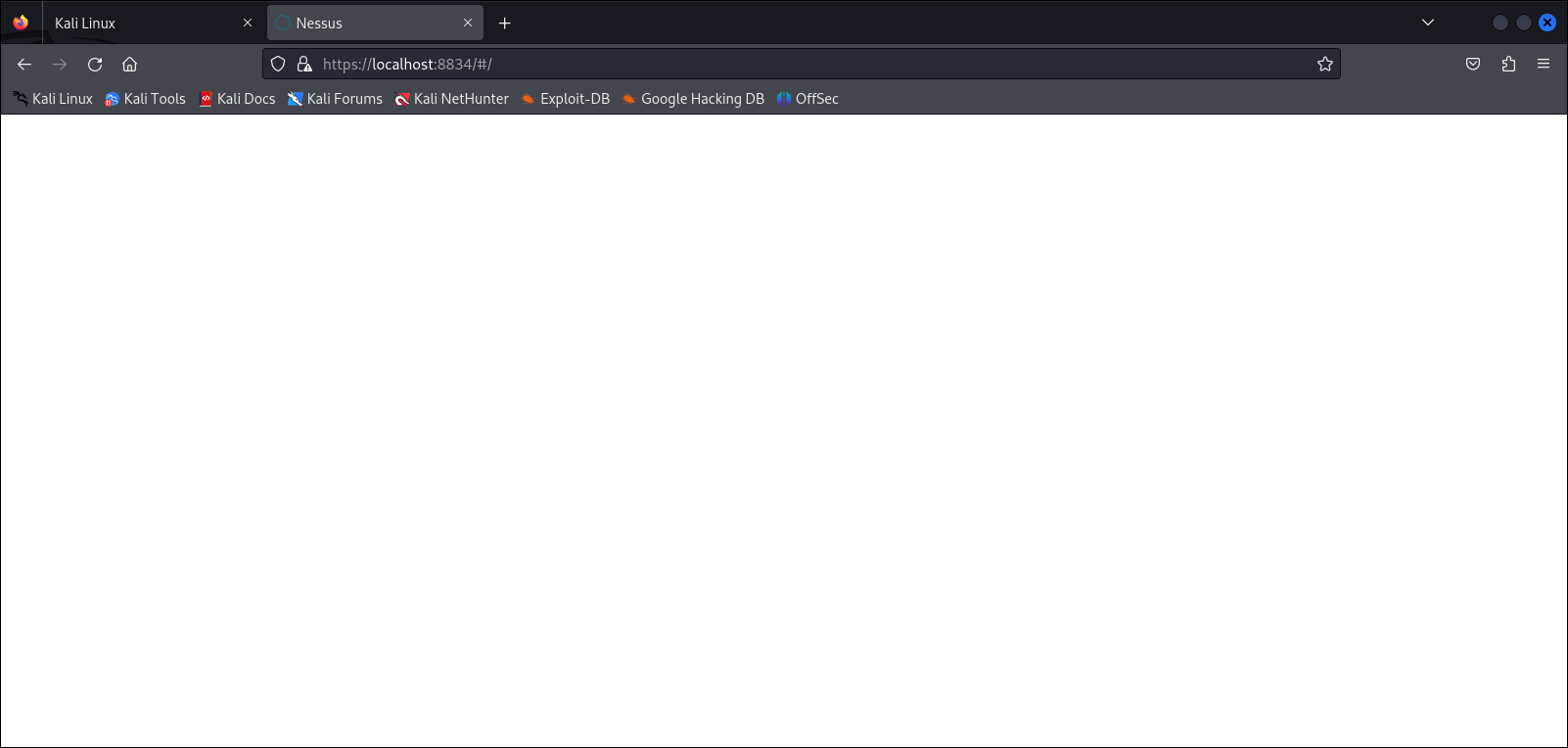
> docker start --attach <container ID>

This command will initiate the Nessus container and attach your terminal to its console, allowing you to interact with the Nessus instance.

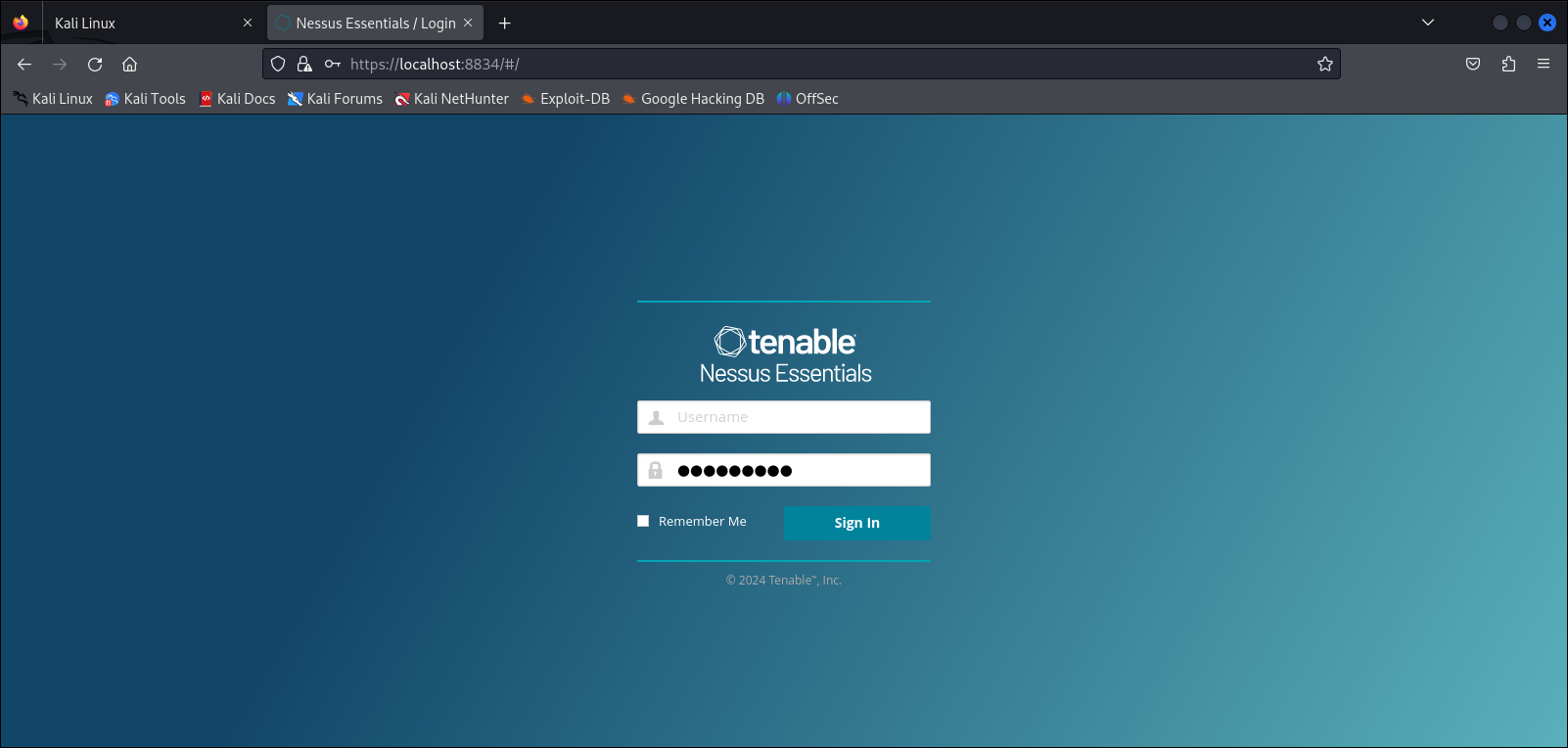


3. Now, you can launch Firefox and access the web interface for Nessus using the following URL: https://localhost:8834

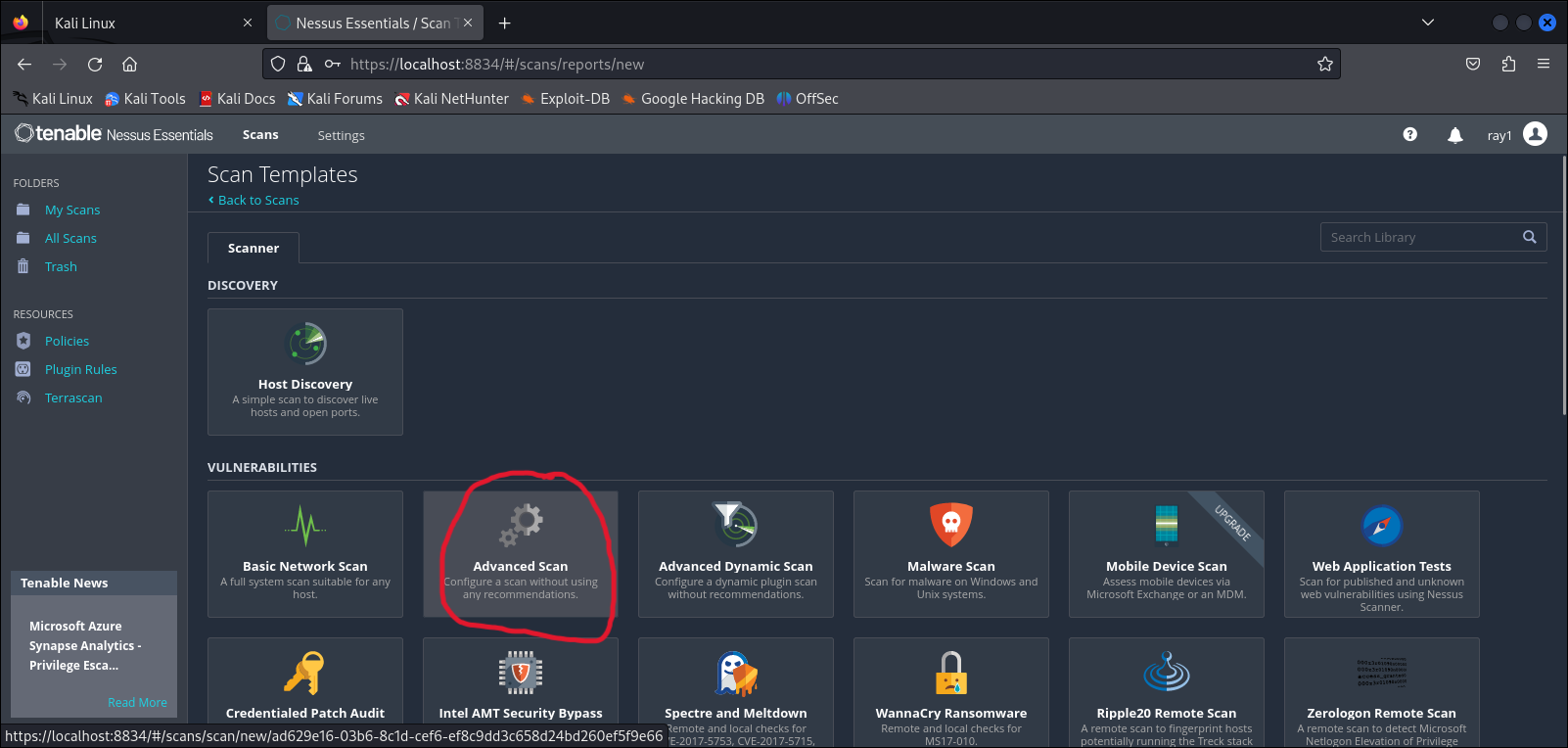
Simply enter the URL in the address bar of your Firefox browser and press Enter. This will direct you to the Nessus web interface, where you can begin configuring and utilizing Nessus for vulnerability scanning and management.



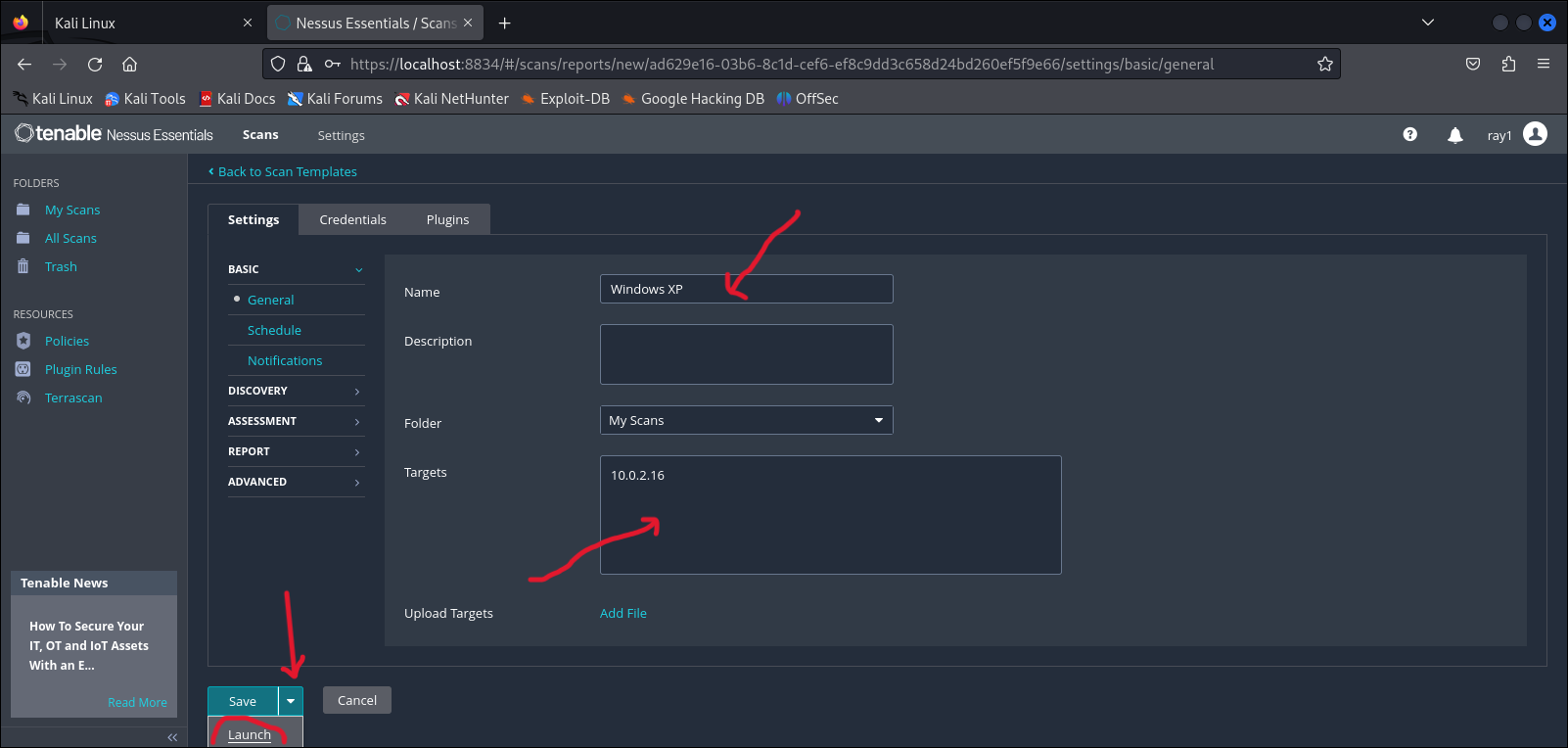
4. Login to Nessus Essentials with your credentials. If you haven't set up your credentials yet, you will need to do so during the initial setup process. Once logged in, you'll gain access to the full capabilities of Nessus Essentials for vulnerability scanning and analysis.



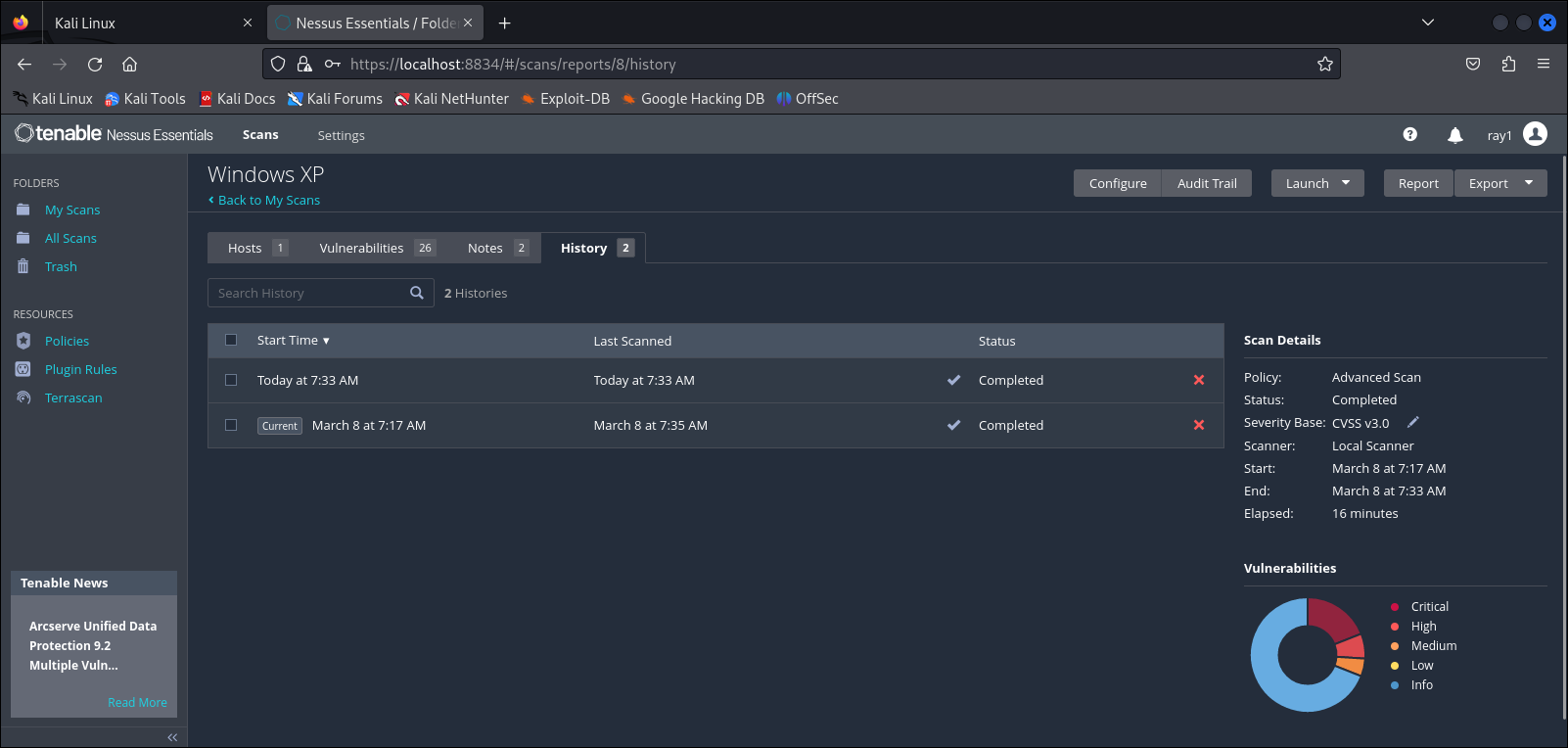
5. Navigate to the "New Scan" option located at the top right corner of the interface. Select "Advanced Scan" for this example. This will allow you to configure and customize the scan parameters according to your specific requirements and preferences.



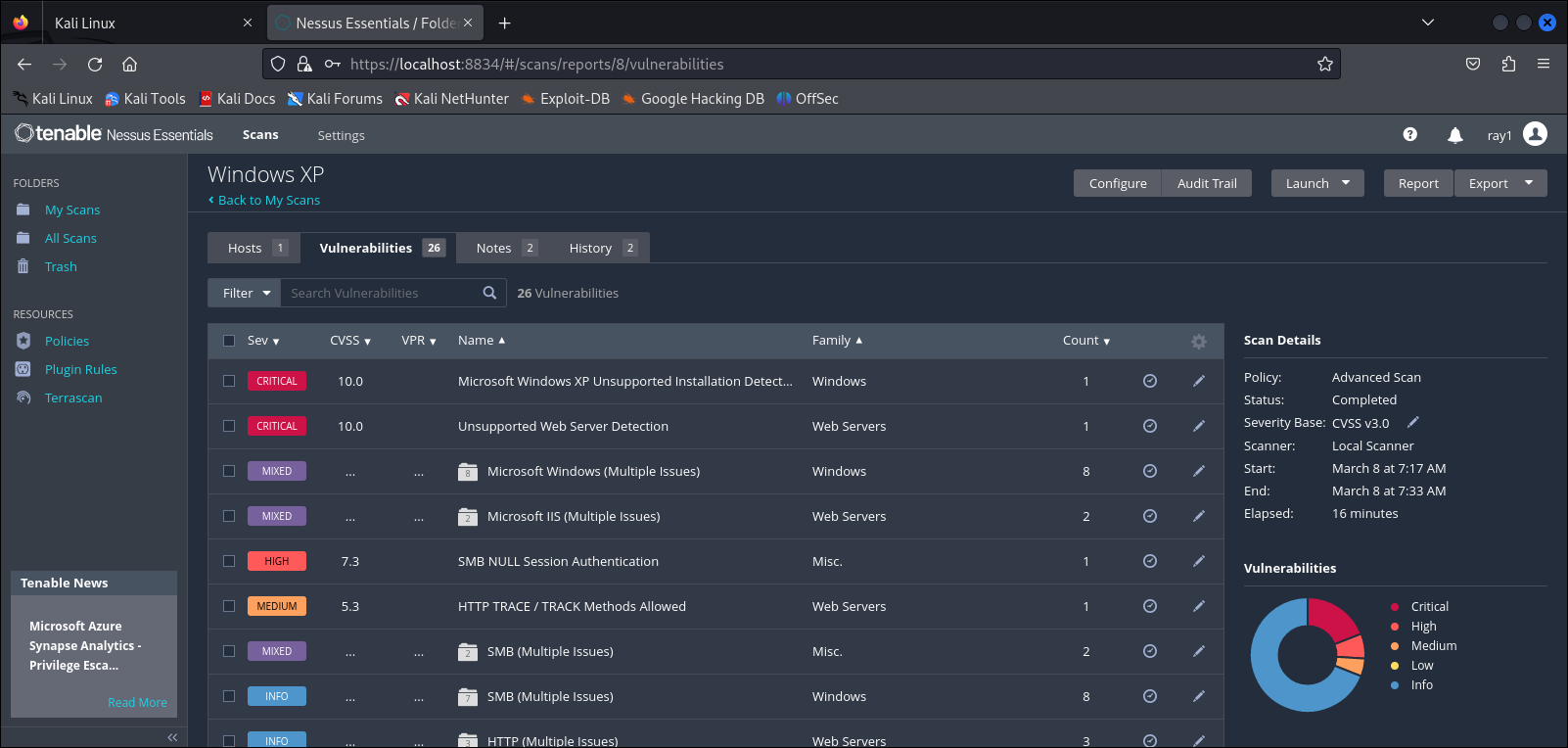
6. Fill in the required information including the scan name and the IP address of the target machine. Once you've entered the necessary details, navigate to the left side and click the downward arrow next to "Save." Then, click on "Launch" to initiate your scan. This will start the vulnerability scanning process on the specified target machine, allowing Nessus to identify and analyze potential security vulnerabilities.

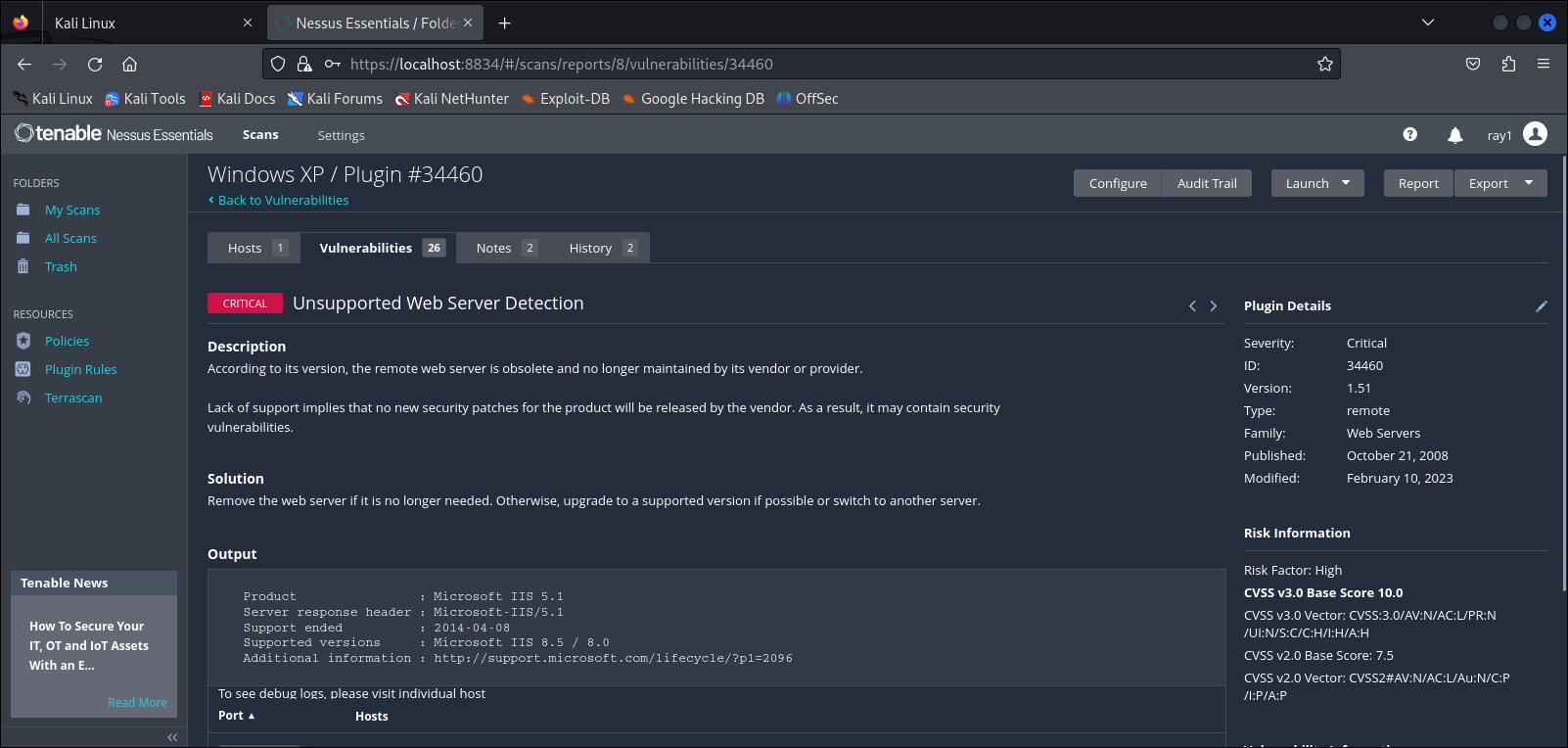


7. After the scan completes, navigate to "My Scans" in the left window pane to monitor the scan process in the right window pane. While the scan is in progress, you'll see green arrows circling next to the scan name, indicating ongoing activity. Keep an eye on this section to track the progress and status of your scans.



8. To obtain detailed information about any listed vulnerability, simply click on the vulnerability entry. This action will provide you with a comprehensive explanation of the vulnerability, including its severity, impact, affected systems, and potential remediation steps. Utilize this information to understand the nature of the vulnerability and to plan and implement appropriate mitigation measures.





9. What you can do with the scan results:

* Identify Vulnerabilities
* Assess Risk
* Validate Vulnerabilities
* Develop Exploits
* Recommend Remediation
* Provide Insights for Security Improvement

10. Conclusion:

Conclusion: After reviewing your scan results in Nessus, it's essential to further investigate potential vulnerabilities by leveraging additional resources like Searchsploit and other vulnerability databases. By cross-referencing the identified vulnerabilities with known attack vectors, CVEs, or Microsoft security bulletin numbers, you can validate their existence and assess the associated risks more accurately. Additionally, Nessus may provide actual exploits or enough information to facilitate further research. Consider conducting a second vulnerability scan to verify the findings and ensure there are no false positives or negatives. This comprehensive approach enhances the effectiveness of your vulnerability management strategy and strengthens your overall cybersecurity posture.