

# PRACTICAL – 6

**AIM:** Implementation to identify web vulnerabilities, using OWASP project Tools: OWASP ZAP Proxy (windows and kali)

## Description:

**Introducing ZAP:-**

Zed Attack Proxy (ZAP) is a free, open-source penetration testing tool being maintained under the umbrella of the Open Web Application Security Project (OWASP). ZAP is designed specifically for testing web applications and is both flexible and extensible. At its core, ZAP is what is known as a “man-in-the-middle proxy.” It stands between the tester’s browser and the web application so that it can intercept and inspect messages sent between browser and web application, modify the contents if needed, and then forward those packets on to the destination. It can be used as a stand-alone application, and as a daemon process.



If there is another network proxy already in use, as in many corporate environments, ZAP can be configured to connect to that proxy.



ZAP provides functionality for a range of skill levels – from developers to testers new to security testing, to security testing specialists. ZAP has versions for each major OS and Docker, so you are not tied to a single OS. Additional functionality is freely available from a variety of add-ons in the ZAP Marketplace, accessible from within the ZAP client. Because ZAP is open source, the source code can be examined to see exactly how the functionality is implemented. Anyone can

volunteer to work on ZAP, fix bugs, add features, create pull requests to pull fixes into the project, and author add-ons to support specialized situations.

**Install and Configure ZAP**

ZAP has installers for Windows, Linux, and Mac OS/X. There are also Docker images available on the download site listed below.

Install ZAP The first thing to do is install ZAP on the system you intend to perform pen testing on. Download the appropriate installer from ZAP’s download location at https://[www.zaproxy.org/download/](http://www.zaproxy.org/download/) and execute the installer.

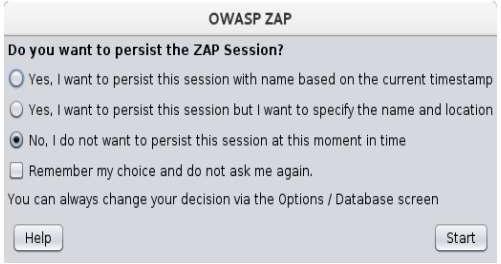
Note that ZAP requires Java 8+ in order to run. The Mac OS/X installer includes an appropriate version of Java but you must install Java 8+ separately for Windows, Linux, and Cross-Platform versions. The Docker versions do not require you to install Java.

Once the installation is complete, launch ZAP and read the license terms. Click Agree if you accept the terms, and ZAP will finish installing, then ZAP will automatically start.

Persisting a Session When you first start ZAP, you will be asked if you want to persist in the ZAP session. By default, ZAP sessions are always recorded to disk in a HSQLDB database with a default name and location.

If you do not persist in the session, those files are deleted when you exit ZAP.

If you choose to persist a session, the session information will be saved in the local database so you can access it later, and you will be able to provide custom names and locations for saving the files.





For now, select No, I do not want to persist this session at this moment in time, then click Start. The ZAP sessions will not be persisted for now.

**ZAP Desktop UI:**

The ZAP Desktop UI is composed of the following elements:

1. **Menu Bar –** Provides access to many of the automated and manual tools.
2. **Toolbar –** Includes buttons which provide easy access to most commonly used features.
3. **Tree Window –** Displays the Sites tree and the Scripts tree.
4. **Workspace Window –** Displays requests, responses, and scripts and allows you to edit them.
5. **Information Window –** Displays details of the automated and manual tools. **6. Footer –** Displays a summary of the alerts found and the status of the main automated tools.





## Running an Automated Scan

The easiest way to start using ZAP is via the Quick Start tab. Quick Start is a ZAP add-on

that is included automatically when you installed ZAP.

## To run a Quick Start Automated Scan :

1. Start ZAP and click the Quick Start tab of the Workspace Window.
2. Click the large Automated Scan button.
3. In the URL to attack text box, enter the full URL of the web application you want to attack.

## Click the Attack button.



* + ZAP will proceed to crawl the web application with its spider and passively scan each page it finds. Then ZAP will use the active scanner to attack all of the discovered pages, functionality, and parameters.
  + ZAP provides 2 spiders for crawling web applications, you can use either or both of them from this screen.



* + The traditional ZAP spider which discovers links by examining the HTML in responses from the web application. This spider is fast, but it is not always effective when exploring an AJAX web application that generates links using JavaScript.
  + For AJAX applications, ZAP’s AJAX spider is likely to be more effective. This spider explores the web application by invoking browsers which then follow the links that have been generated. The AJAX spider is slower than the traditional spider and requires additional configuration for use in a “headless” environment.
  + ZAP will passively scan all of the requests and responses proxied through it. So far ZAP has only carried out passive scans of your web application. Passive scanning does not change responses in any way and is considered safe. Scanning is also performed in a background thread to not slow down exploration.
  + Passive scanning is good at finding some vulnerabilities and as a way to get a feel for the basic security state of a web application and locate where more investigation may be warranted. Active scanning, however, attempts to find other vulnerabilities by using known attacks against the selected targets.
  + Active scanning is a real attack on those targets and can put the targets at risk, so do not use active scanning against targets you do not have permission to test.

## See Explored Pages

To examine a tree view of the explored pages, click the Sites tab in the Tree Window. You can expand the nodes to see the individual URLs accessed.

View Alerts and Alert Details

The left-hand side of the Footer contains a count of the Alerts found during your test, broken

out into risk categories. These risk categories are:





## To view the alerts created during your test:

1. Click the Alerts tab in the Information Window.
2. Click each alert displayed in that window to display the URL and the vulnerability

detected in the right side of the Information Window.

1. In the Workspace Windows, click the Response tab to see the contents of the header

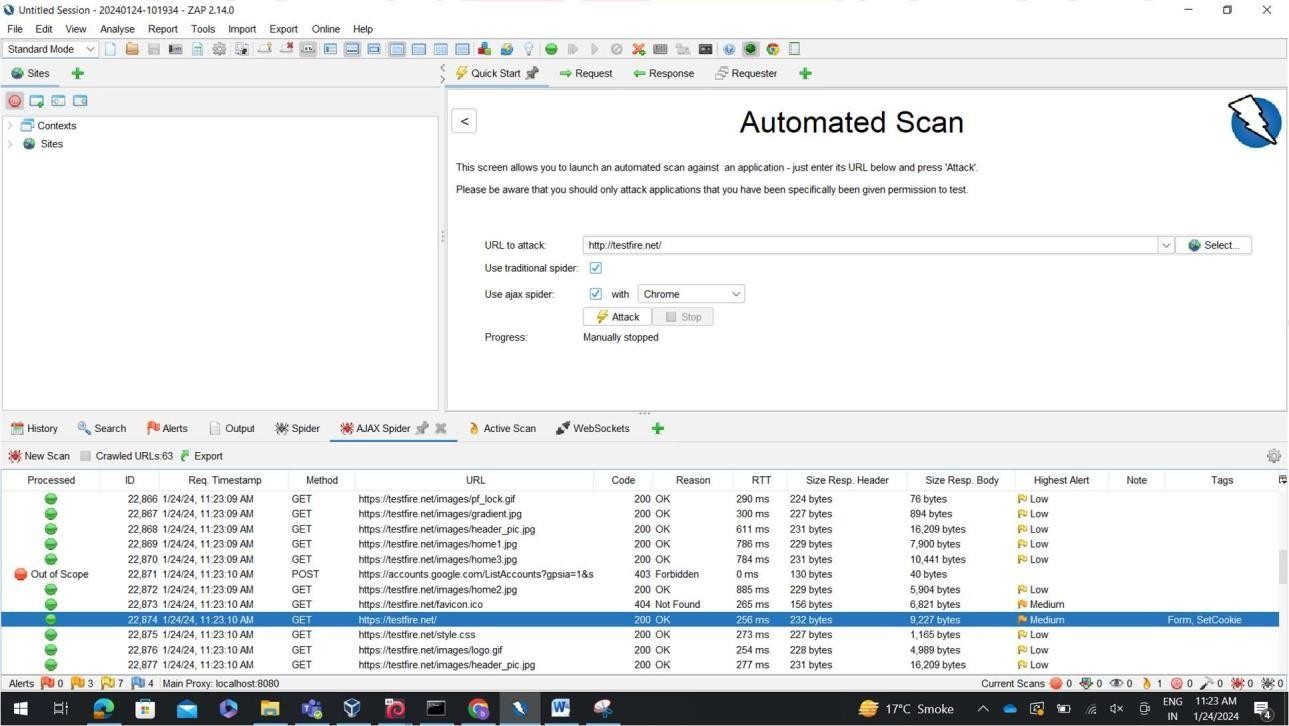
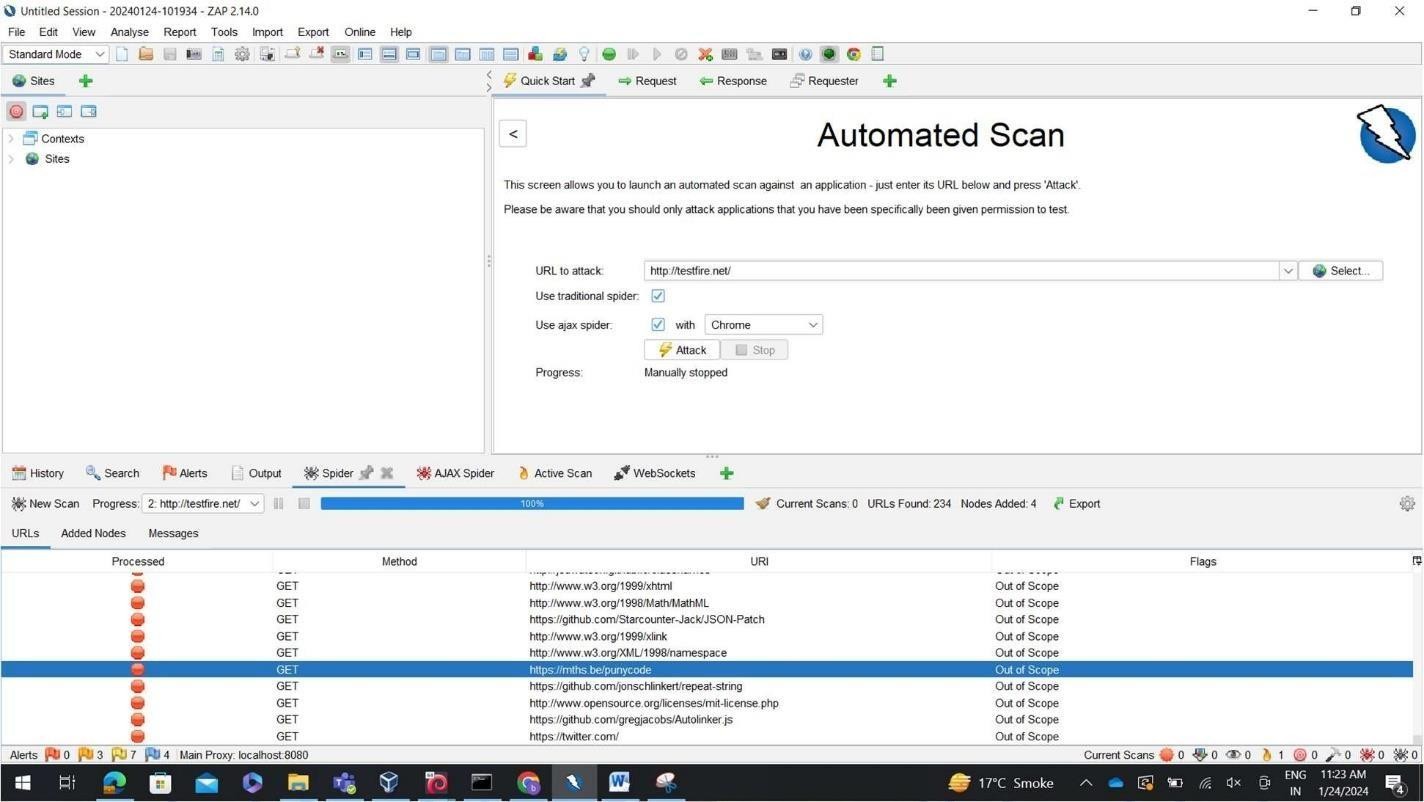
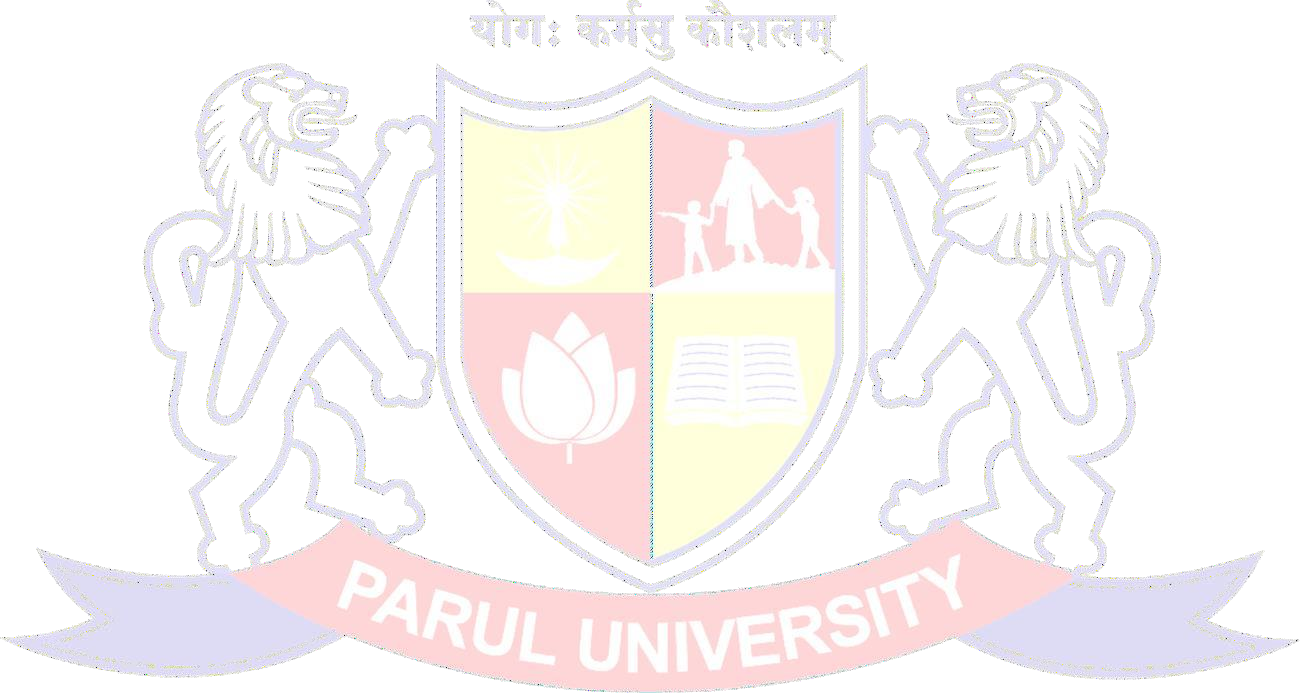
and body of the response. The part of the response that generated the alert will be highlighted.

## Here are the Outputs of a Sample bank website follow the images below step by step



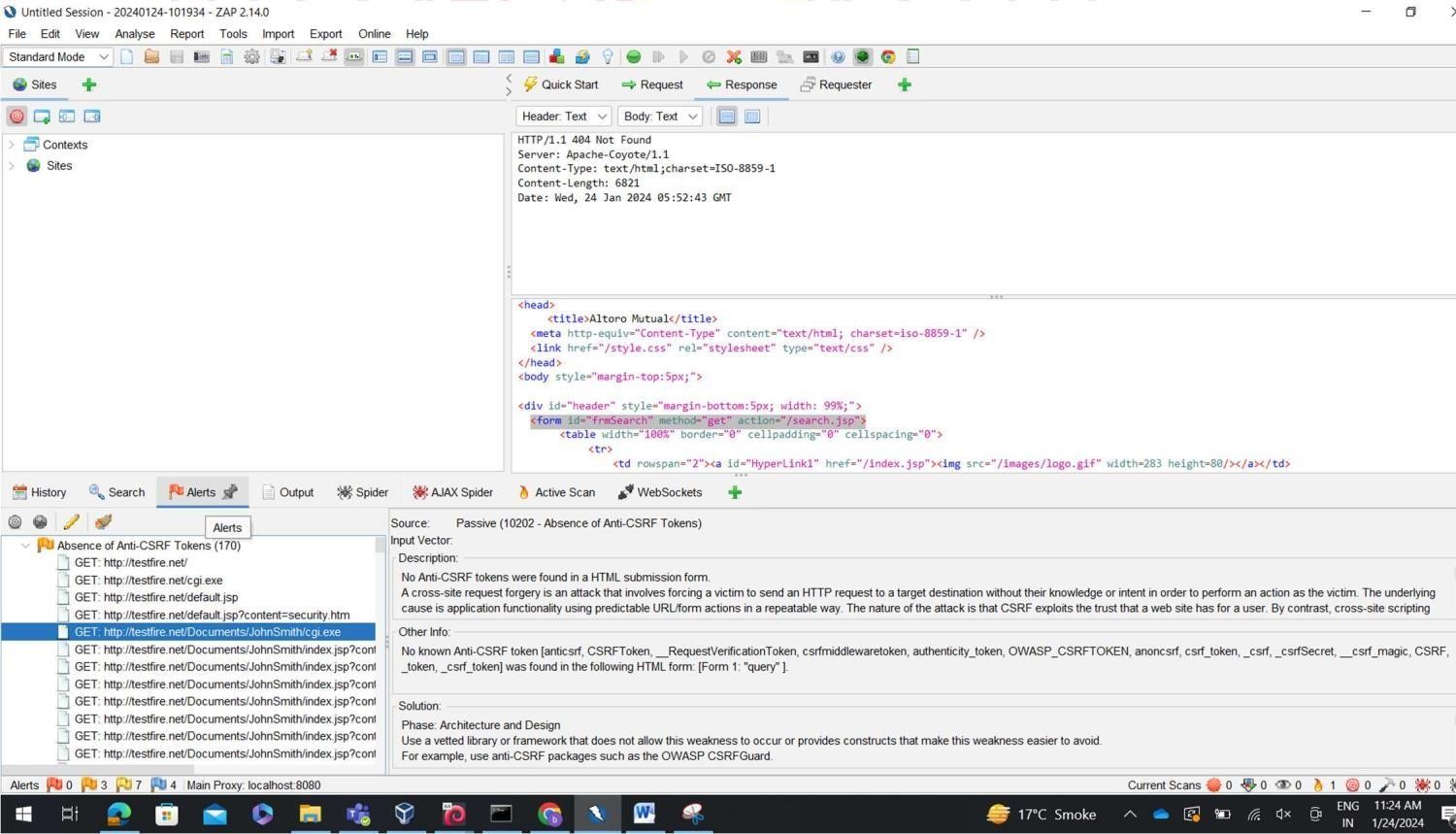
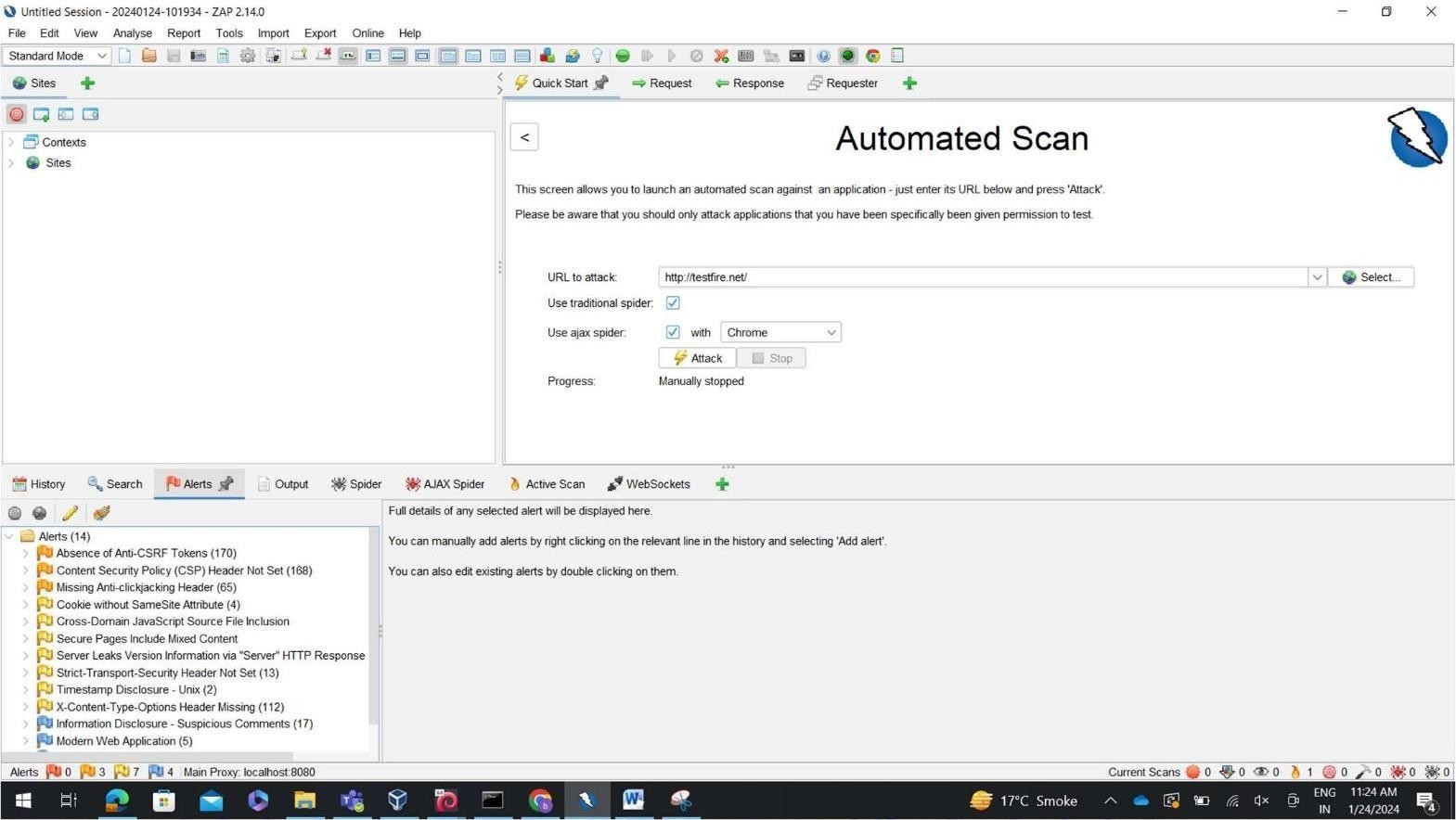
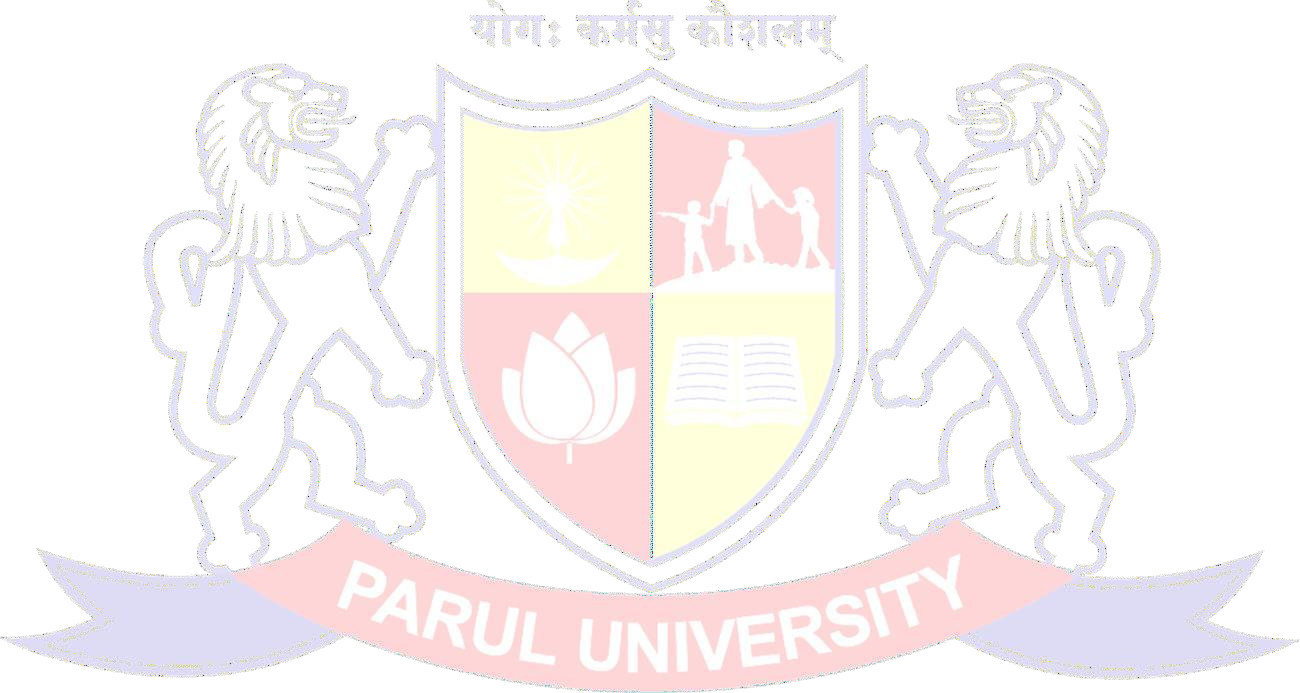


**CLICK ON ATTACK BUTTON**



## CHECK THE OUTPUT OF BELOW DASHBORD IN IMAGE

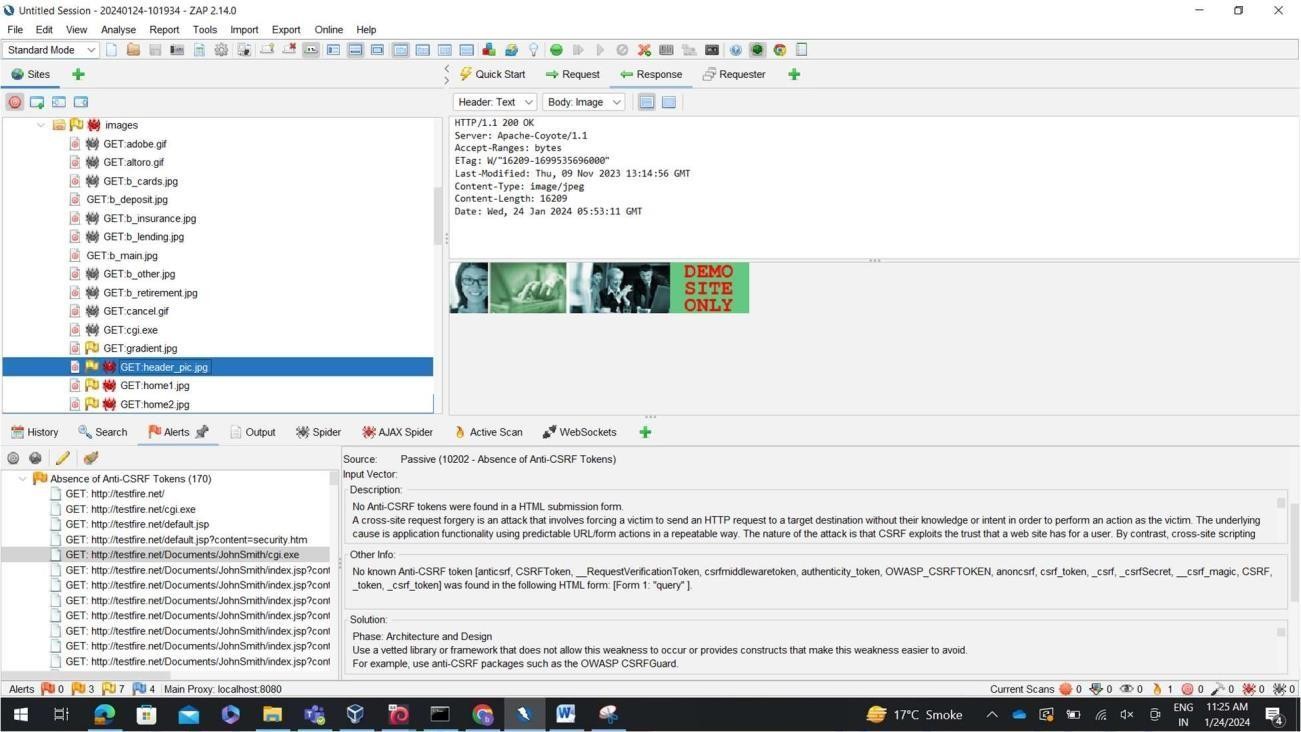




**CLICK ON ALERT OPTION TO CHECK VULNERABLITIES IN BELOW IMAGE**



**SELECT ANY LINK CHECK THAT DESCRIPTION ABOUT VULNERABILITY**





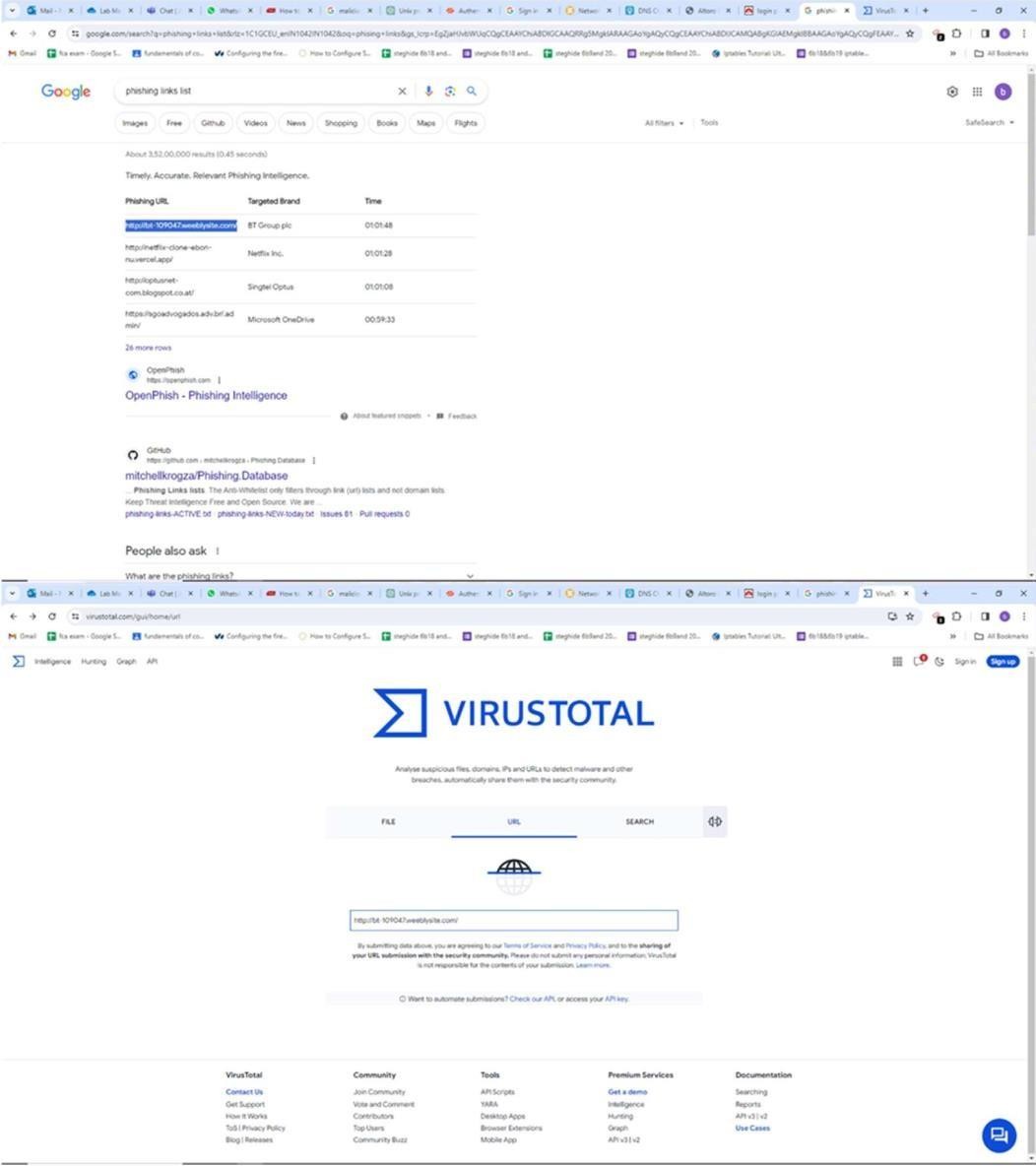
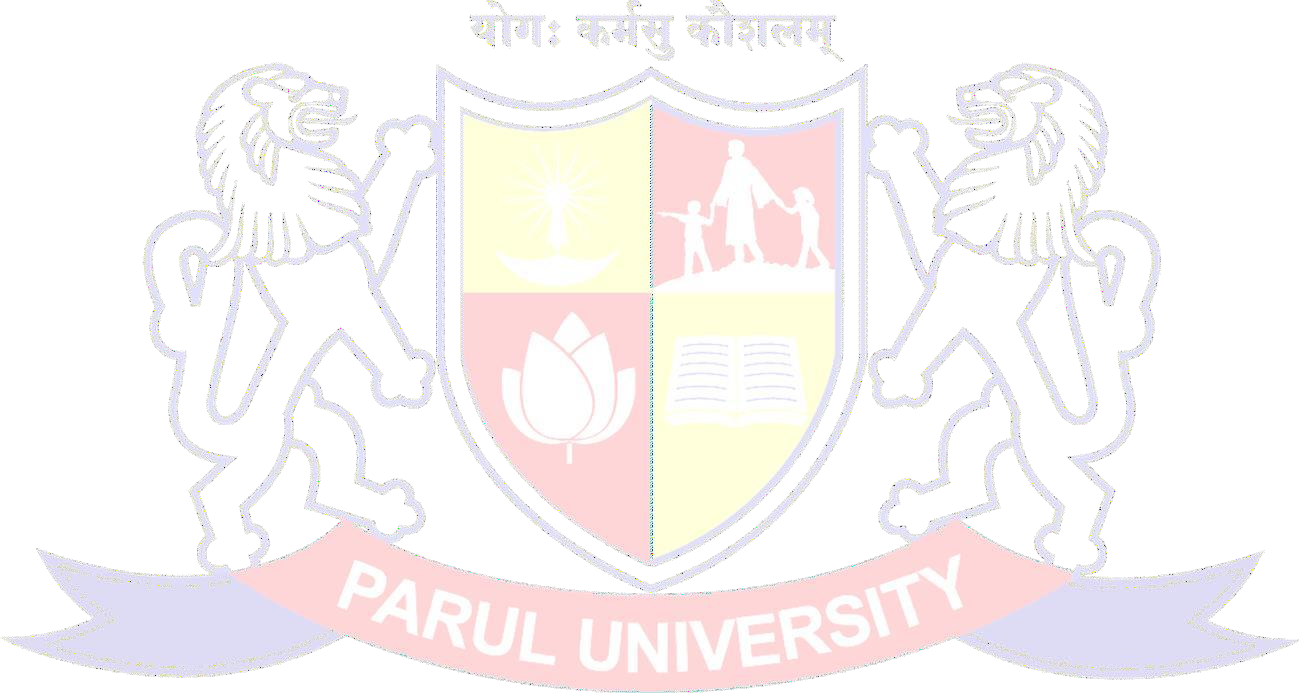
# PRACTICAL – 7

**Aim:** Mplementation of IT Audit, malware analysis and Vulnerability assessment and generate the report.

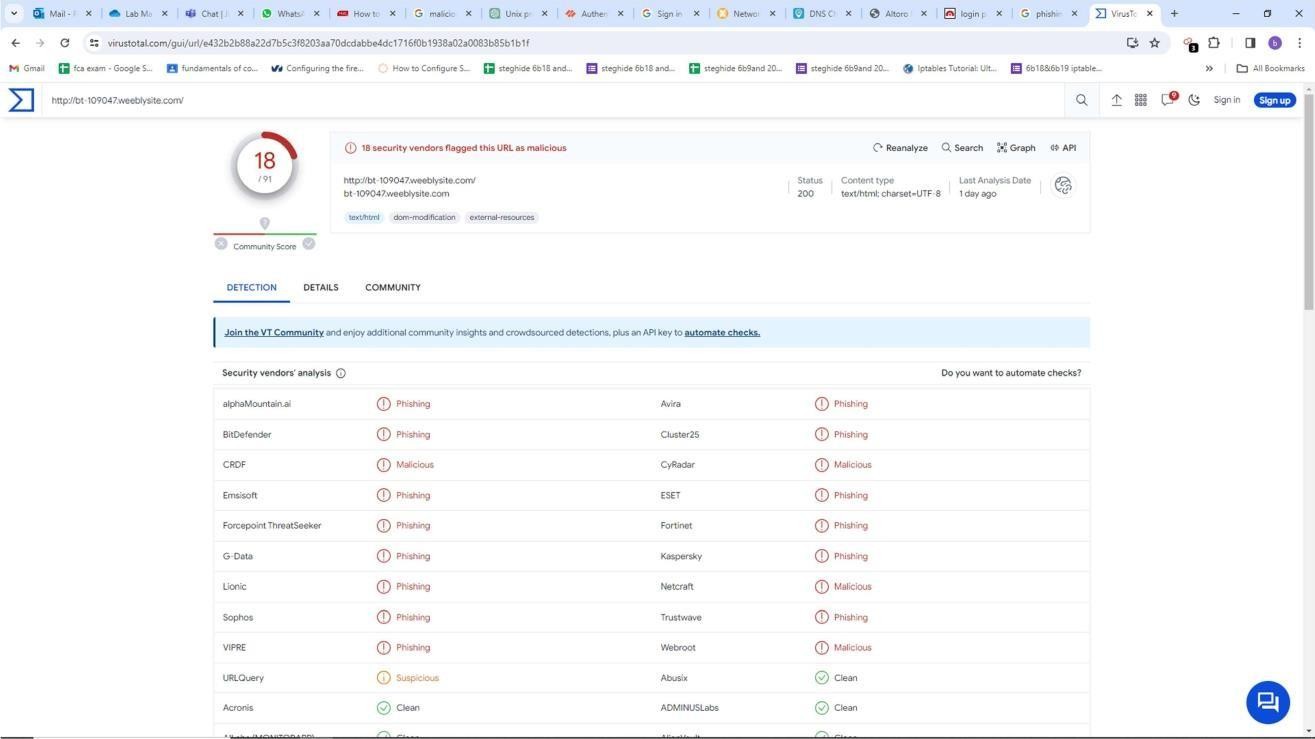
**Objective:** To know how to find vulnerabilities by using NESSUS

**Requirements:** Laptop, Kali linux, Nessusd pakage in kali

## Malware analysis







NESSUS:

Nessus, developed by Tenable Inc, is a widely-used open-source vulnerability scanner. It offers a paid subscription, Nessus Professional, as well as a free version, Nessus Essentials, which is limited to 16 IP addresses per scanner.

Nessus provides a range of services, including vulnerability assessments, network scans, web scans, asset discovery, and more, to aid security professionals, penetration testers, and other cybersecurity enthusiasts in proactively identifying and mitigating vulnerabilities in their networks.

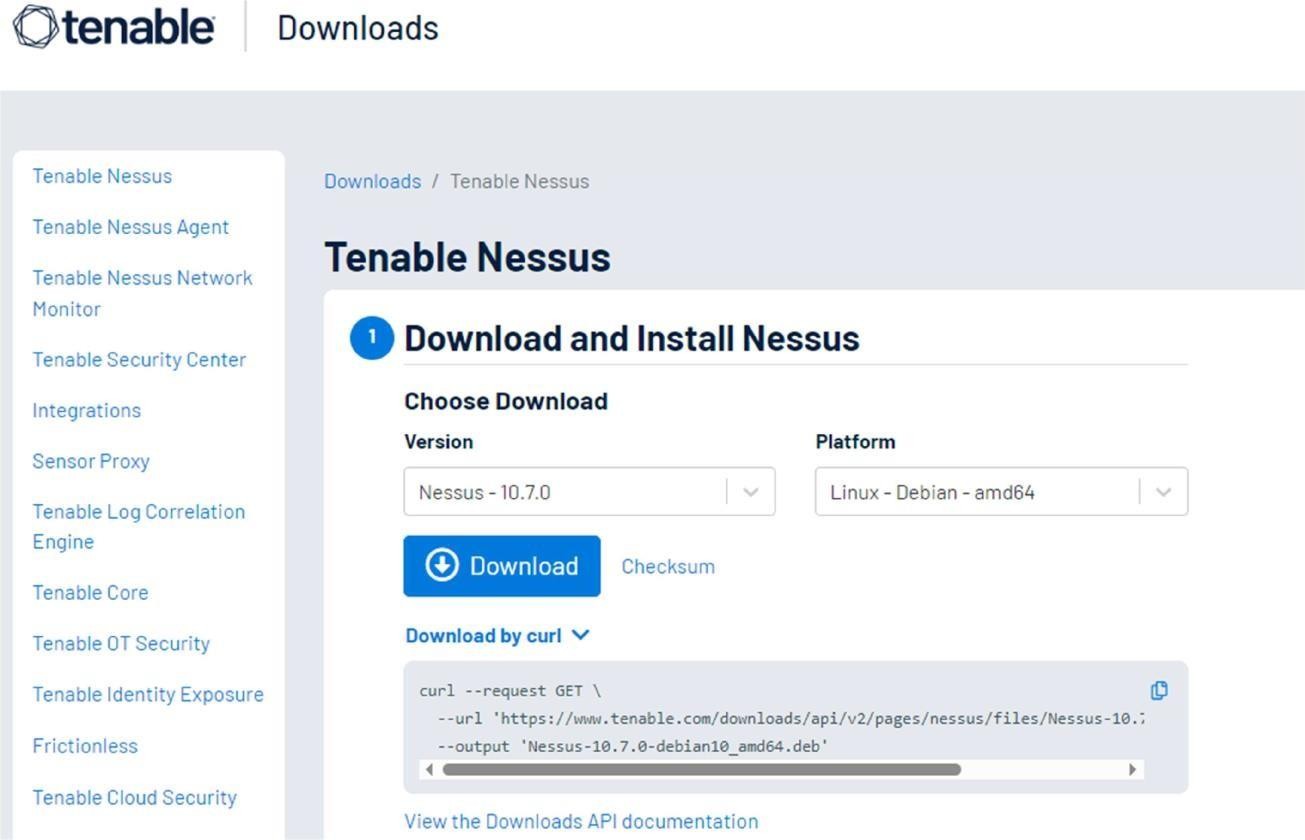
## How to install a Nessus in kali

Unlike many security tools, Nessus doesn't come installed on Kali Linux.

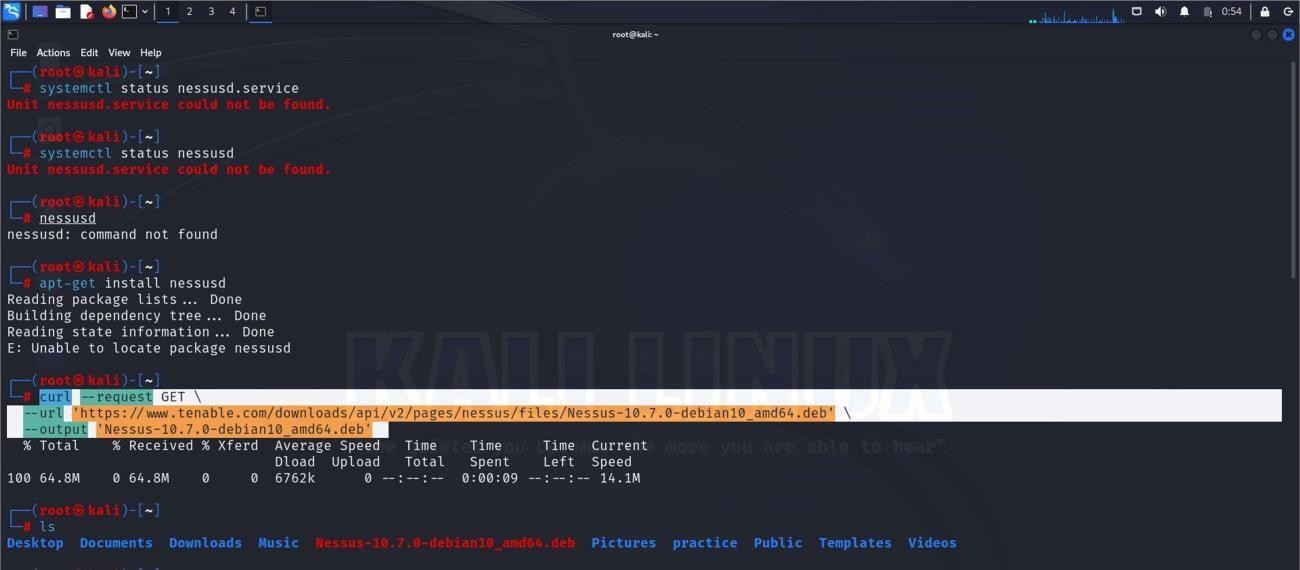
But it is very easy to download and install. Follow these steps to install Nessus on your Kali:

* 1. Download the Nessus package for Debian on the Nessus website and make sure you set the Platform to **Linux-Debian-amd64**.





* 1. When it's finished downloading, open your Linux terminal and navigate to the location you downloaded the Nessus file to.



Install Nessus using this command:



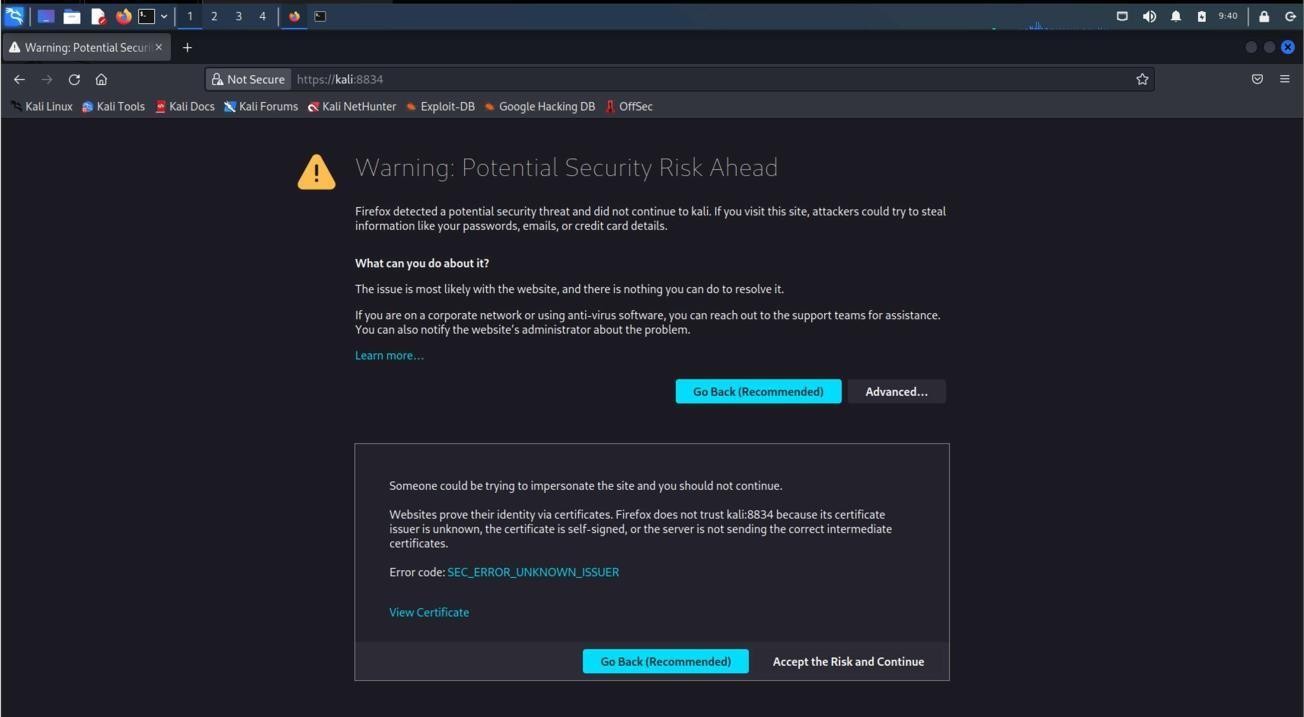


Start the Nessus service with this command:



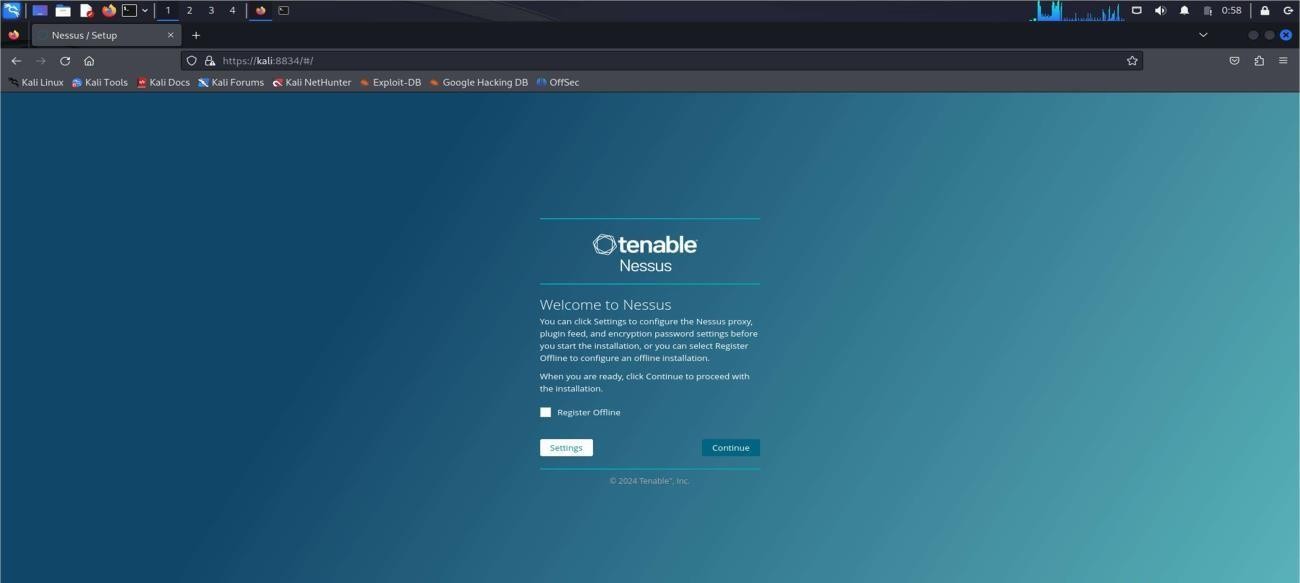
On your browser, go to **https://kali:8834/**. It would show a warning page



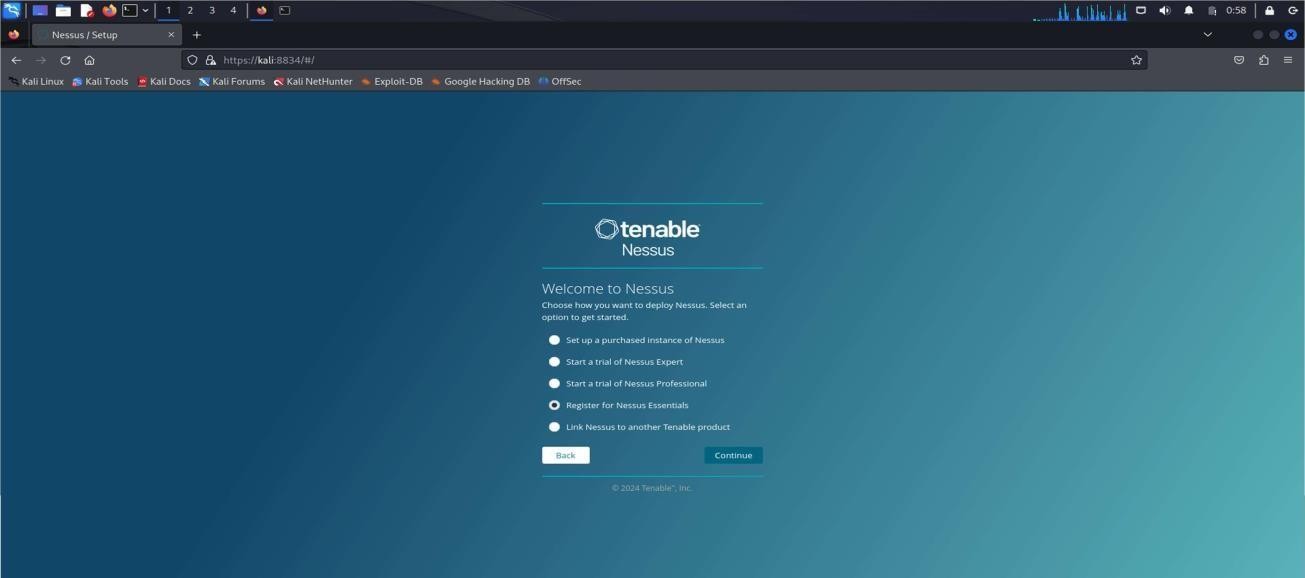


Click on Advanced. Then, click on Accept Risk and Continue.

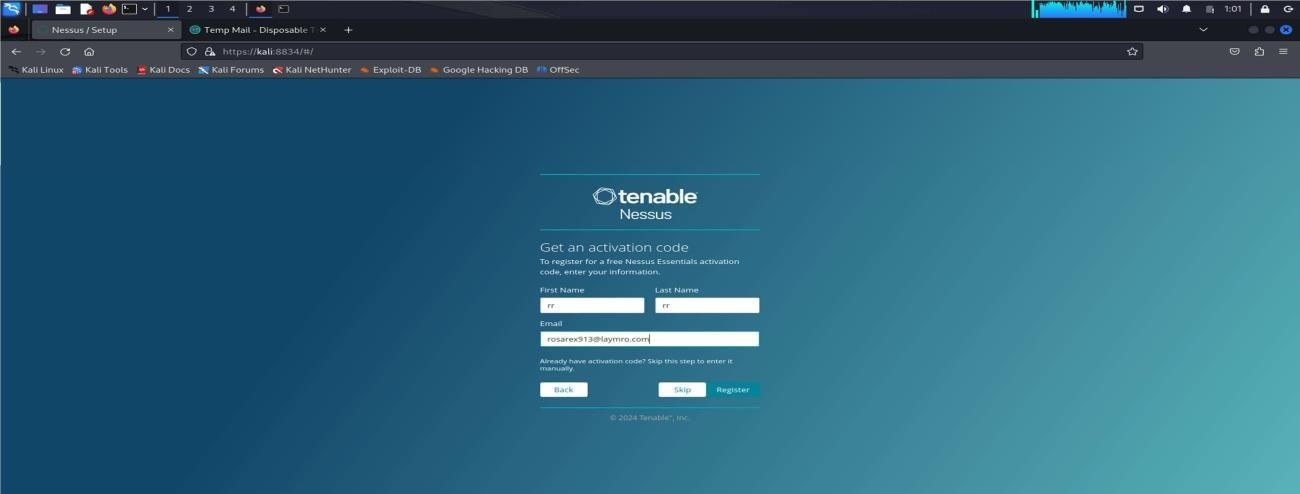
7. Choose the Nessus Product you prefer. If you want the free version of Nessus, click on **Register Nessus Essentials.**





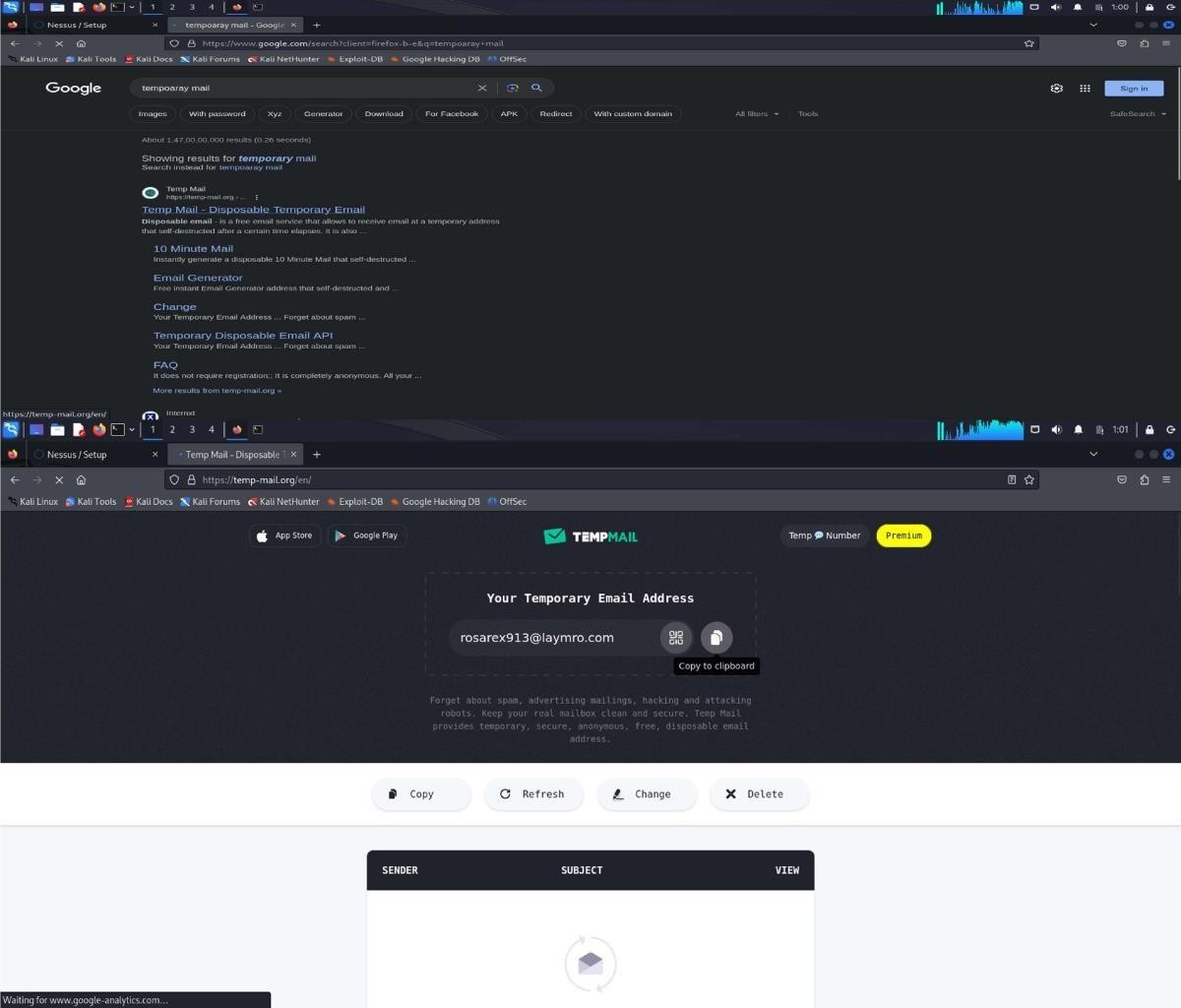
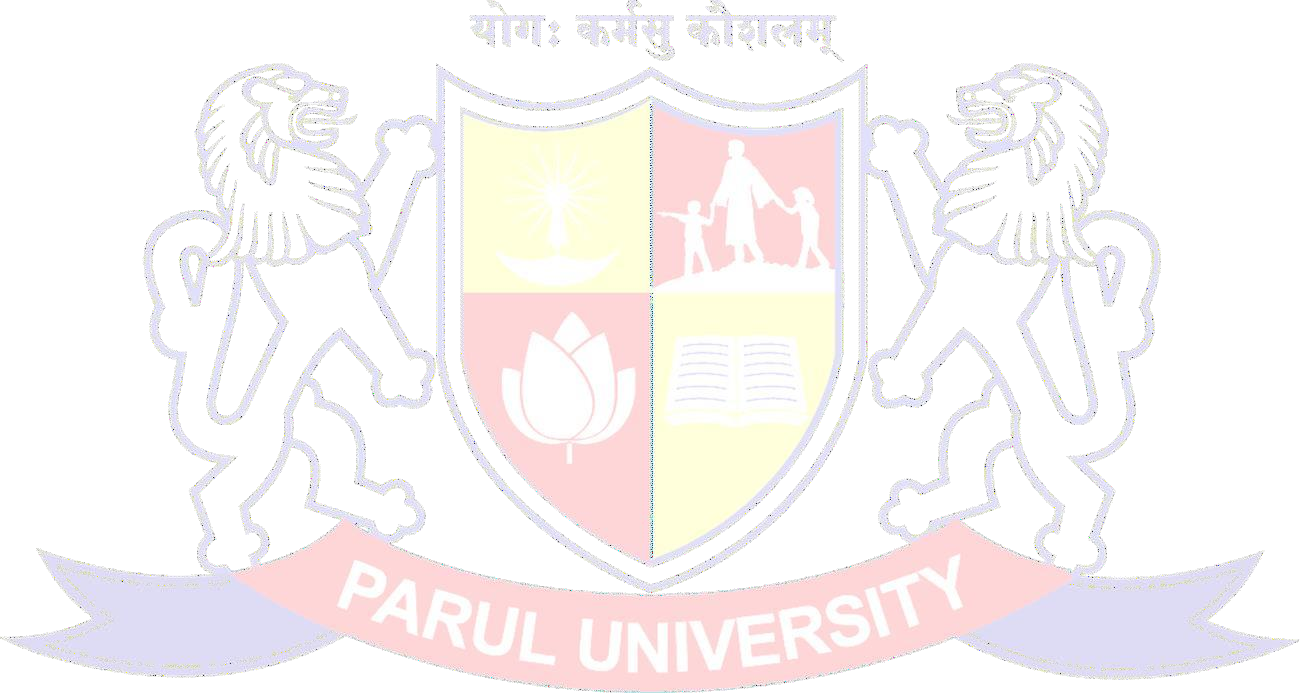


Enter your name and email address to receive an activation code by email. Paste the activation code into the space provided and choose a username and password.

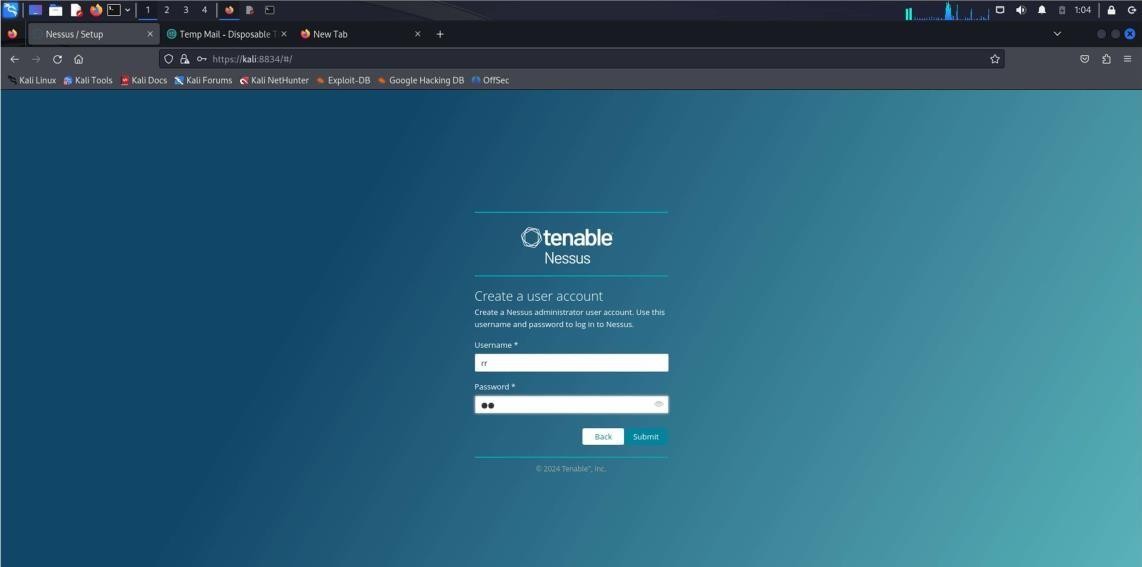
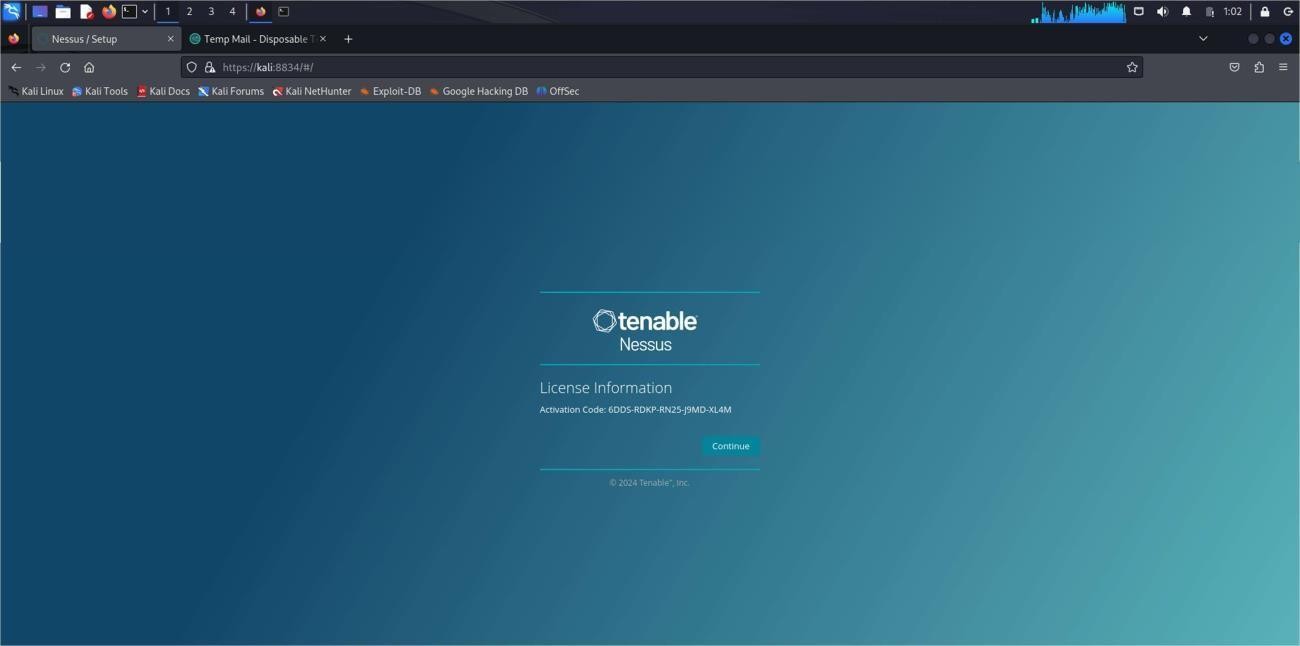




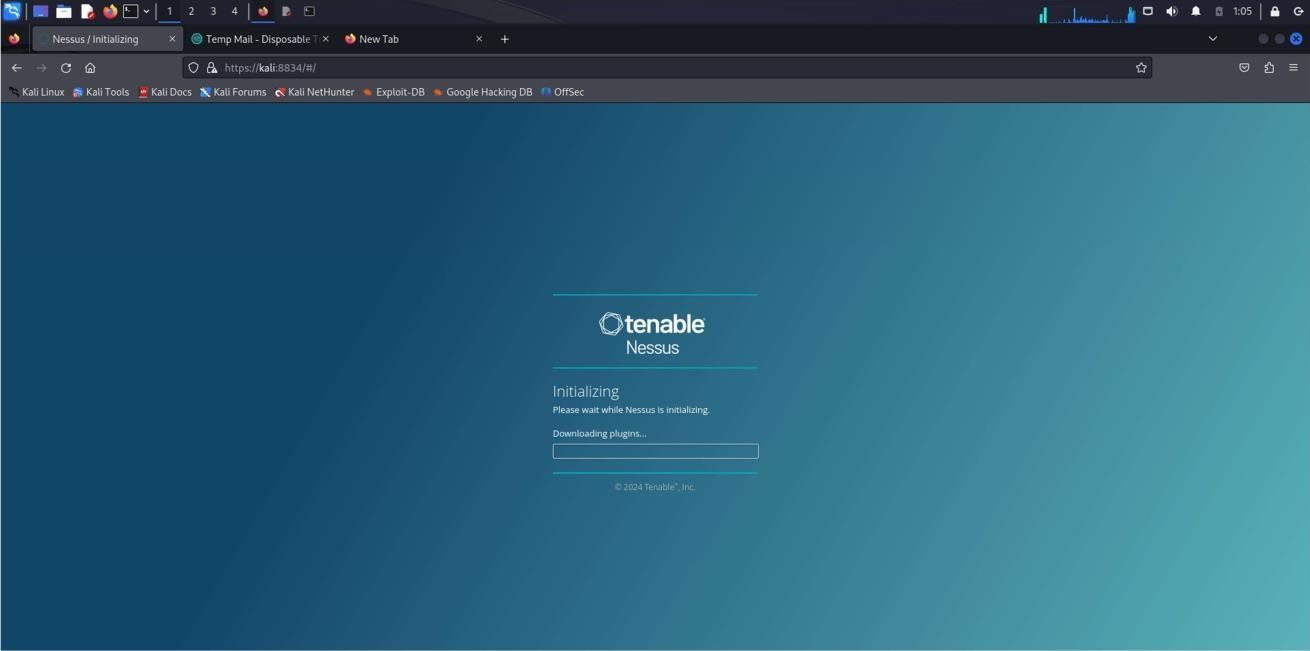
You can use emailaddress as temporary you can visit online temporary email address examples below

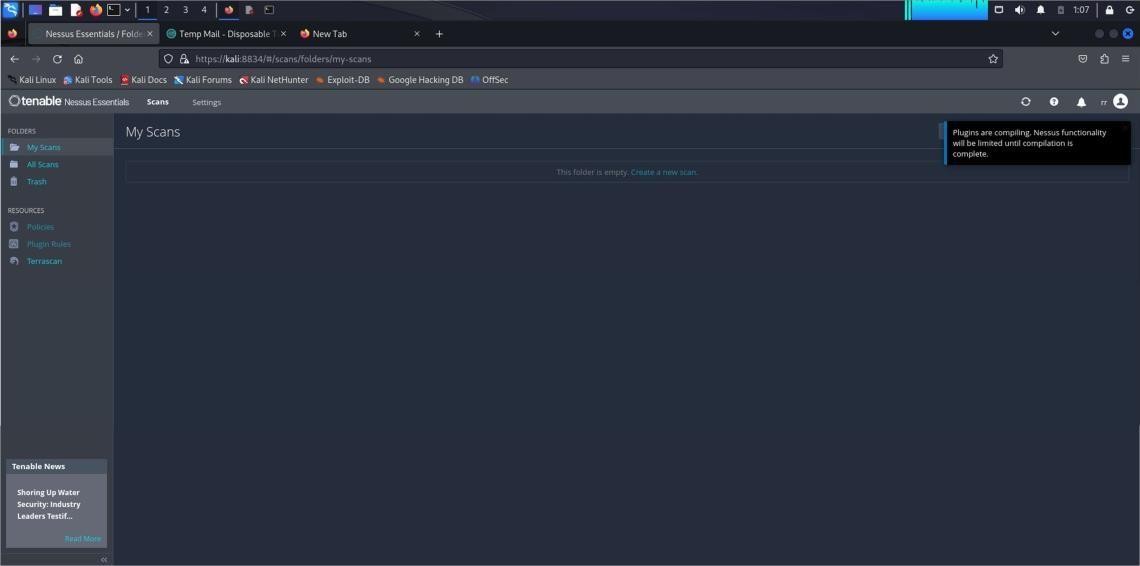




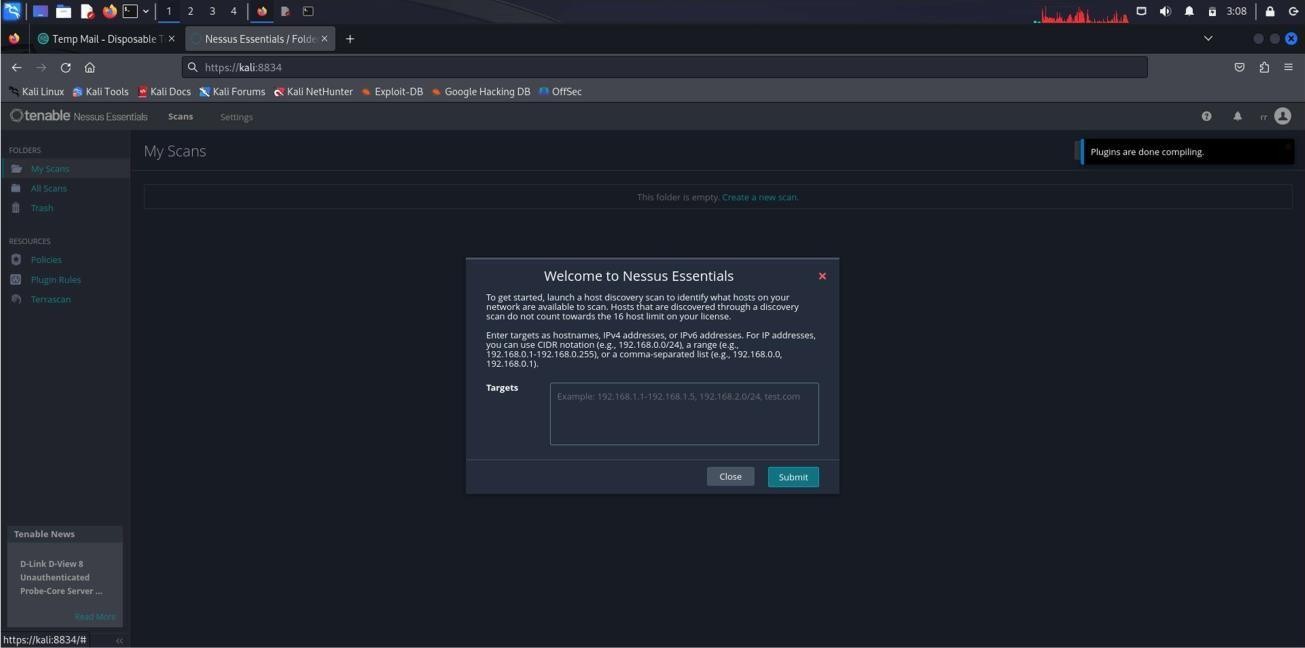
Allow Nessus to download the necessary plugins.

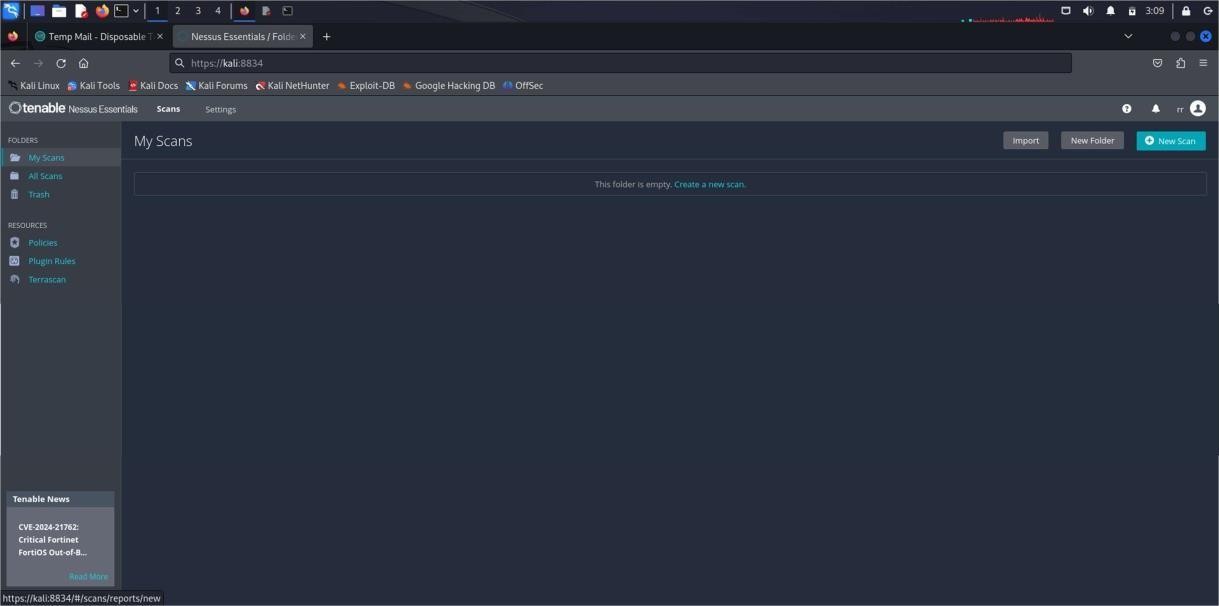






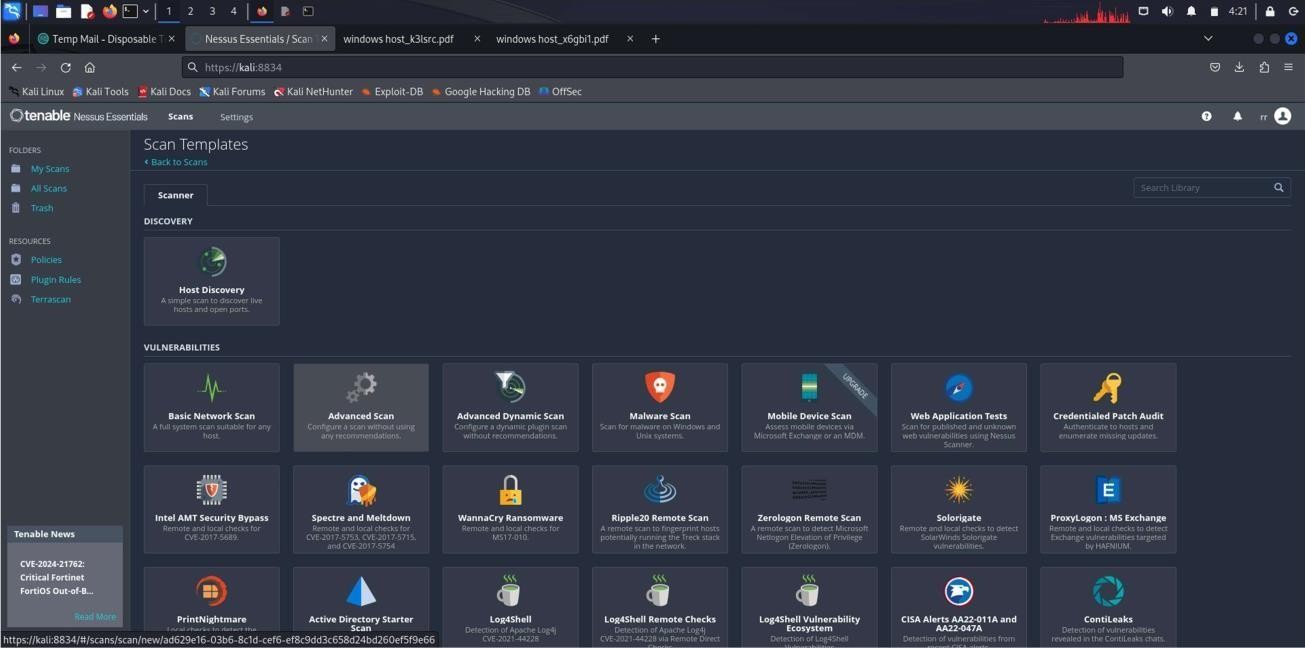




Click on **New Scan** to begin scanning for vulnerabilities

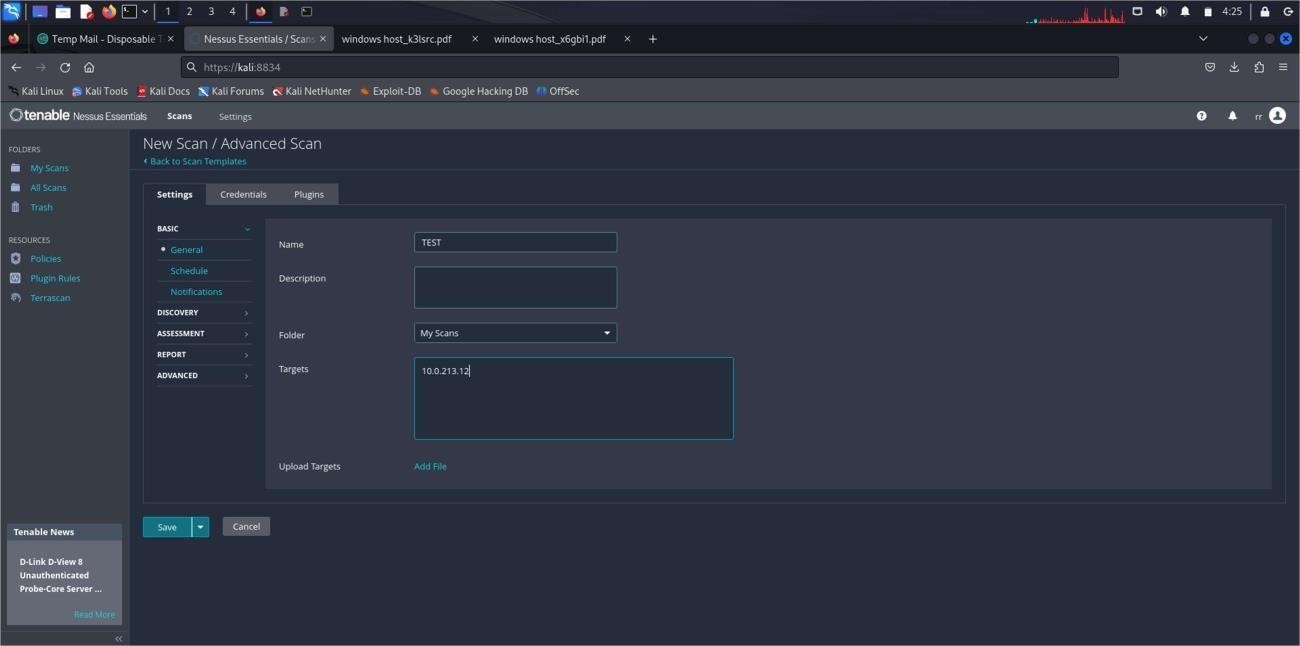


Click on Advance scan



Give name for scaning (e.g test,windows scan..etc)

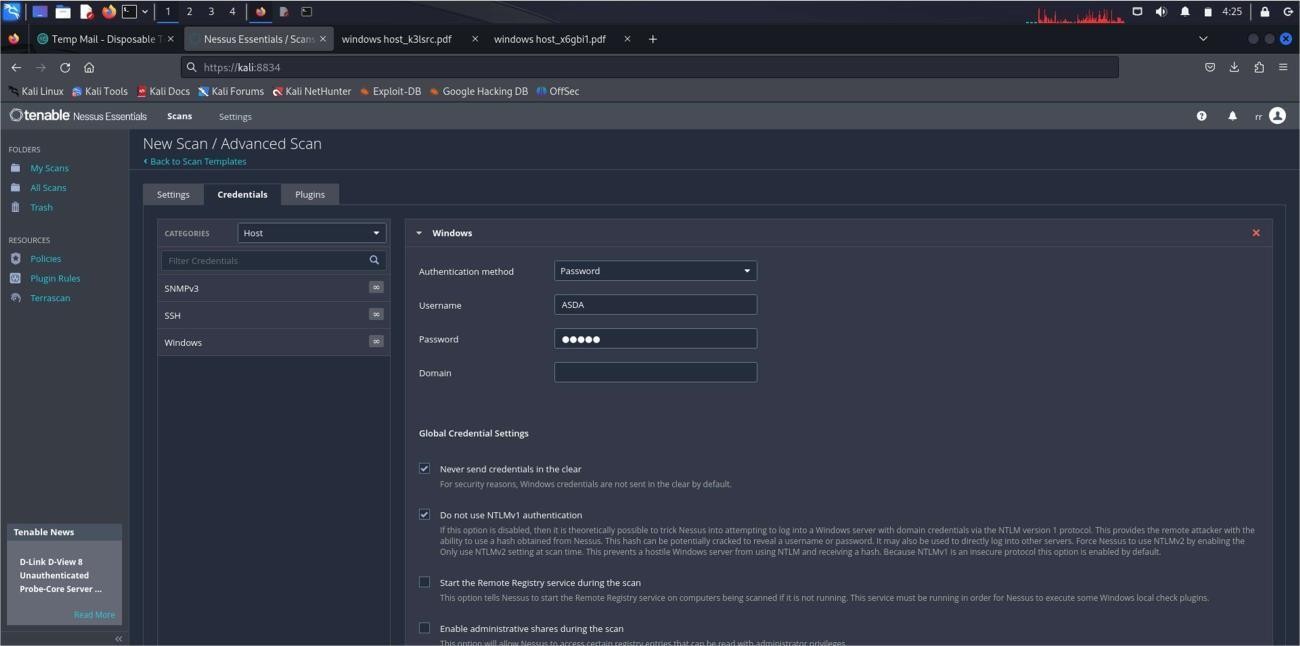
Give the ip address of your windows that you want to scan for vulnerabilities in Target box shown in the below



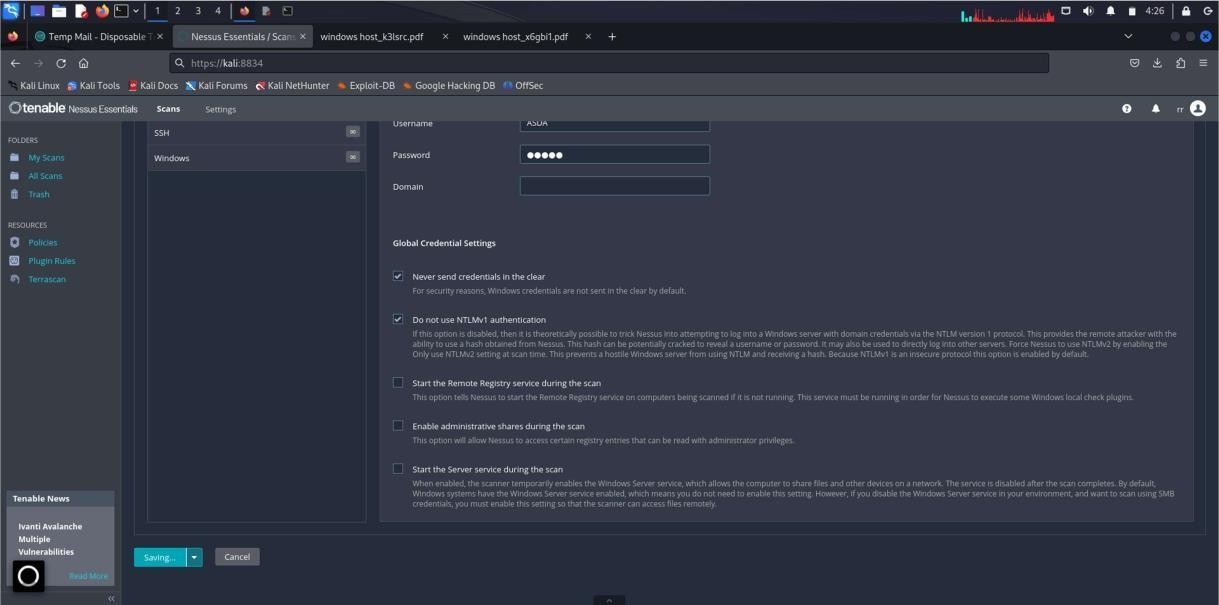
Give the credentials of your windows like username and password if you known (OPTIONAL).



## NOTE:- Use of giving credential it will help you scan more into your system

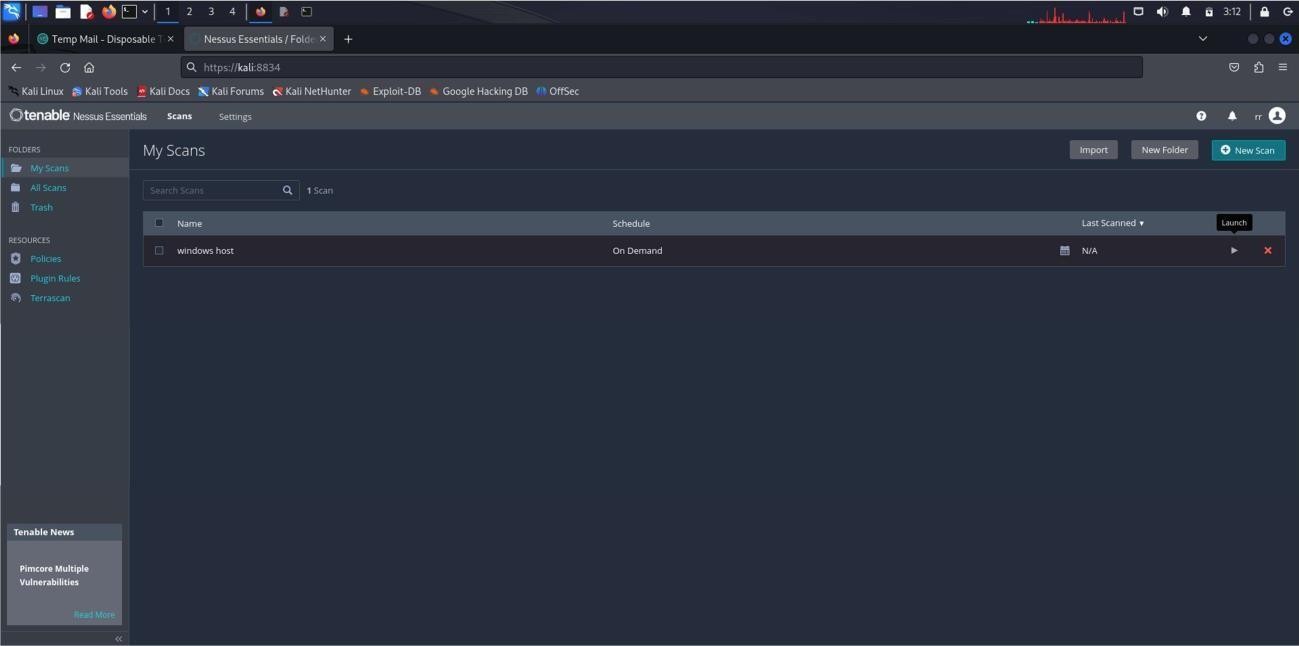


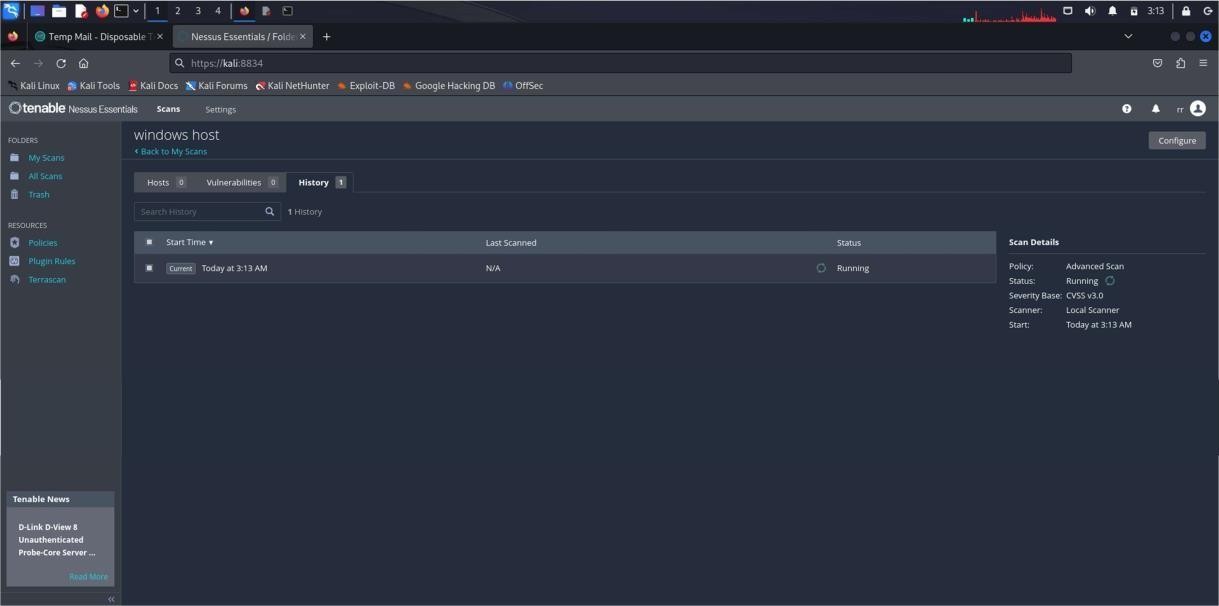
Go down and save the Progress





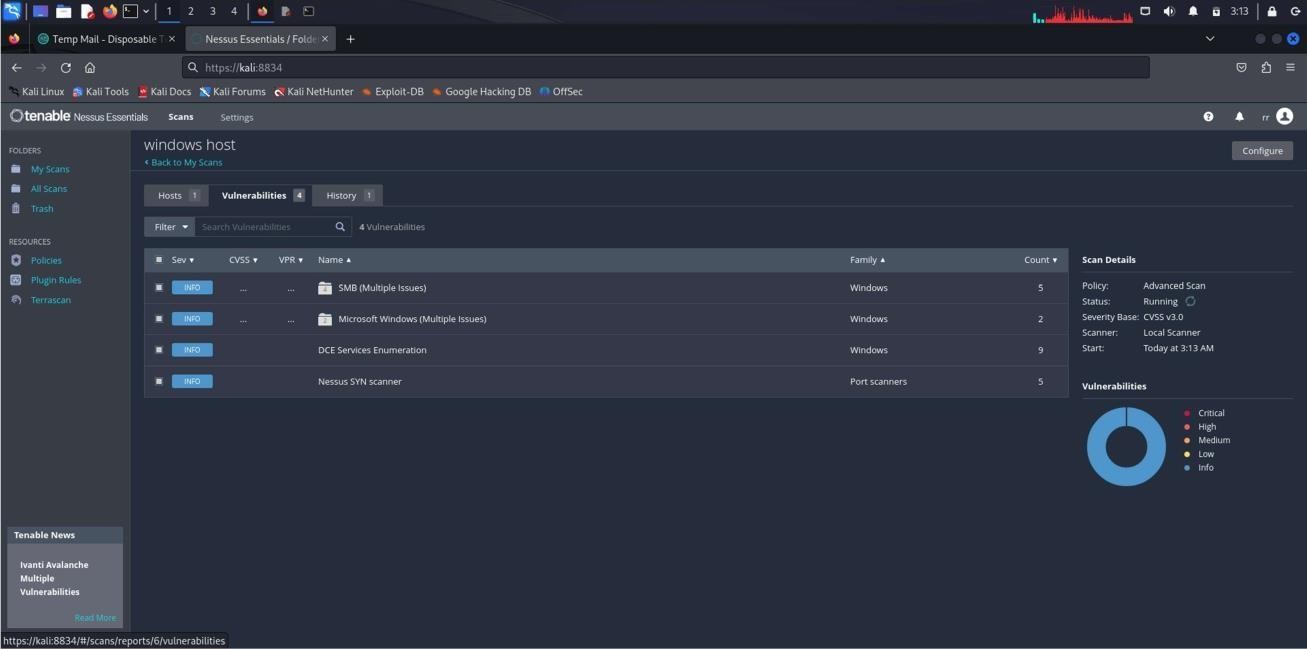
Click on launch

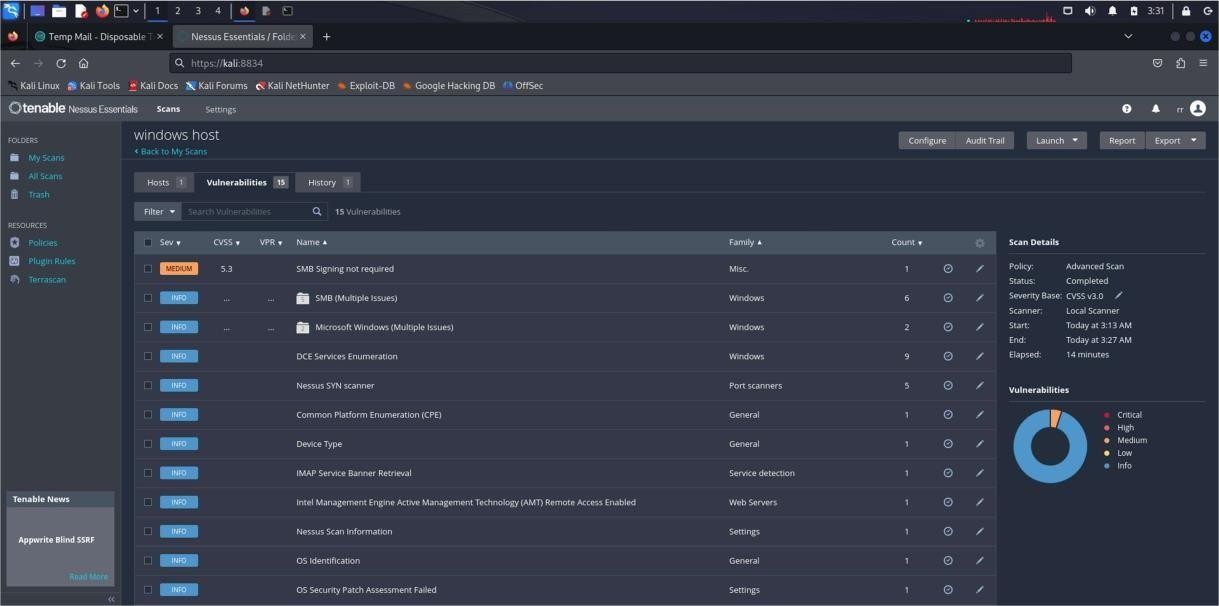






Wait for Some time to get the Output.







ON RIGHT SIDE CLICK ON REPORT TO GENERATE THE ENTIRE REPORT OF YOUR SYSTEM VULNERABILITY

