**Task 3 : Perform a Basic Vulnerability Scan on our PC**

* Objective: Use free tools to identify common vulnerabilities on your computer. Tools:
* OpenVAS Community Edition (free vulnerability scanner) or Nessus Essentials. Deliverables:
* Vulnerability scan report with identified issues.
* Hints/Mini Guide:

1.Install OpenVAS or Nessus Essentials.

2.Set up scan target as your local machine IP or localhost.

3.Start a full vulnerability scan.

4.Wait for scan to complete (may take 30-60 mins).

5.Review the report for vulnerabilities and severity.

6.Research simple fixes or mitigations for found vulnerabilities.

7.Document the most critical vulnerabilities.

8.Take screenshots of the scan results.

…………………………………………………………………………Output………………………………………………………………………

1.Install OpenVAS or Nessus Essentials.

=> Open kaliLinux and past the command for installing OpenVas

# apt install openvas

# gvm-setup

# apt update && install postgresql-17

# pg\_dropcluster –stop 17 main

# pg\_upgradecluster 15 main

# gvm-check-setup

#greenbone-feed-sync –type nvt

#greenbone-feed-sync –type cert

#greenbone-feed-sync –type scap

#runuser -u \_gvm –gvmd –create-user=admin2 –new-password=password

#gvm-start

#systemctl stop gvmd

#systemctl stop ospd-openvas

#systemctl stop gsad

#systemctl start ospd-openvas

#systemctl start gvmd

#systemctl start gsad

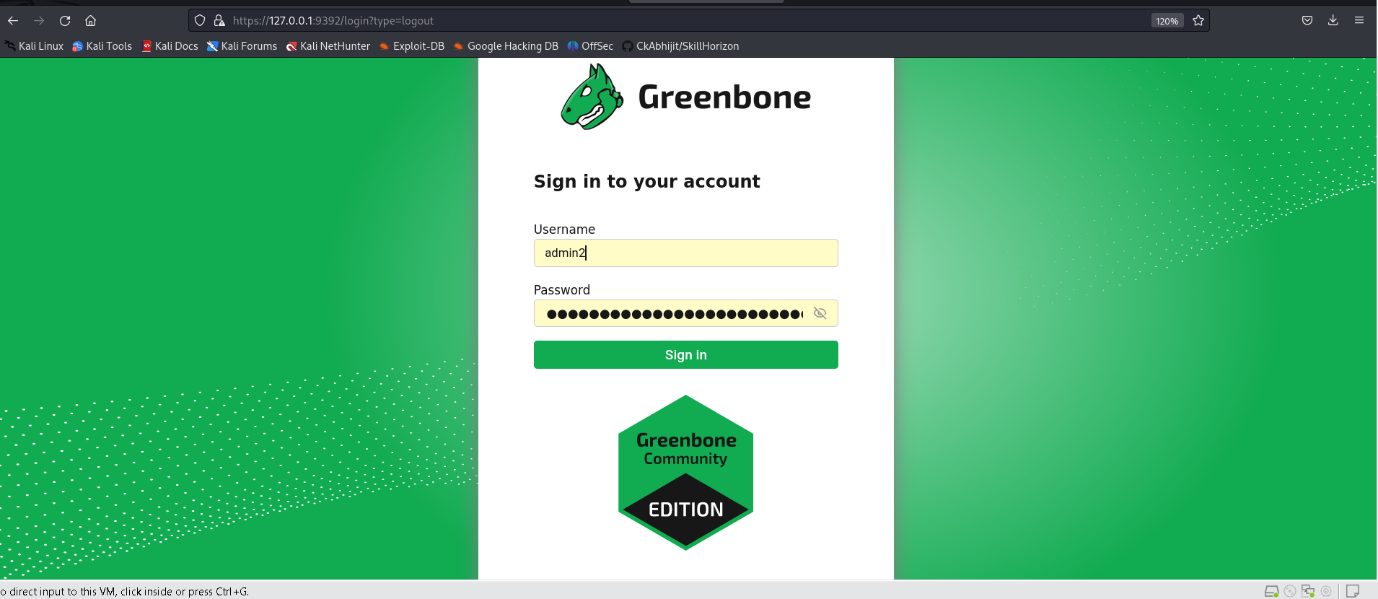
#greenbone-feed-sync –type scap

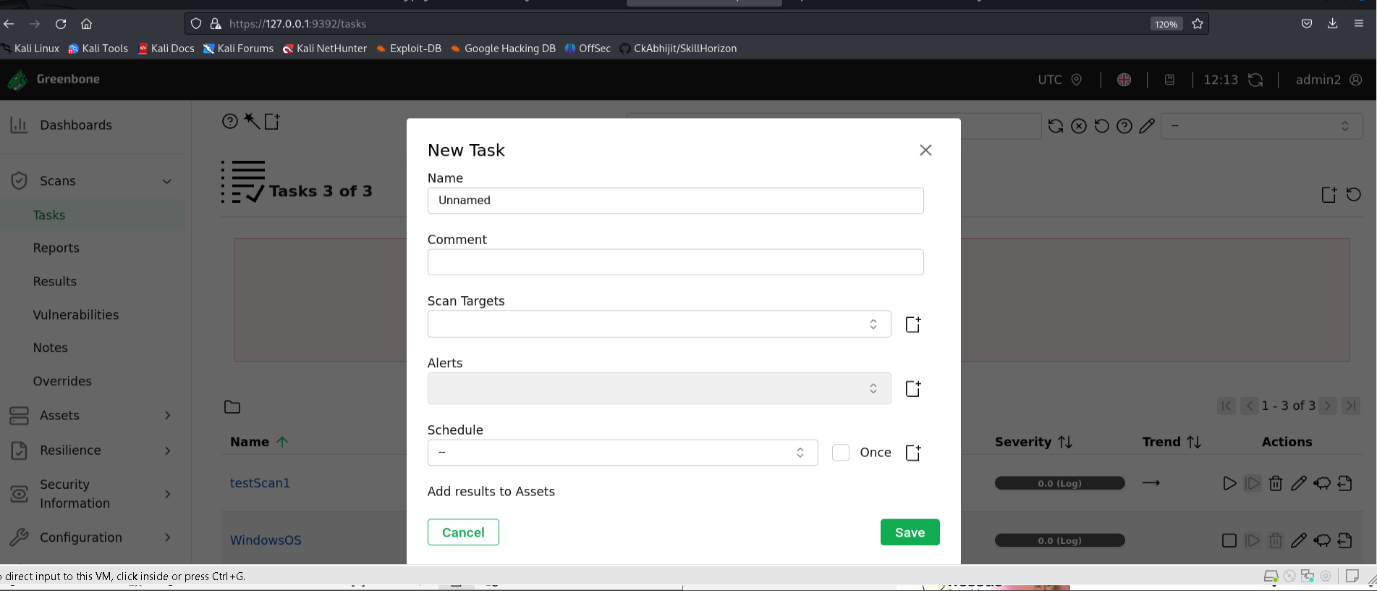
#greenbone-feed-sync –type CERT

#greenbone-feed-sync –type GVMD\_DATA

#runuser -u \_gvm –gvmd –rebuild

* Now open browser and search 127.0.0.1:9392
* Now show the OpenVAS signin page , then enter your user name and password

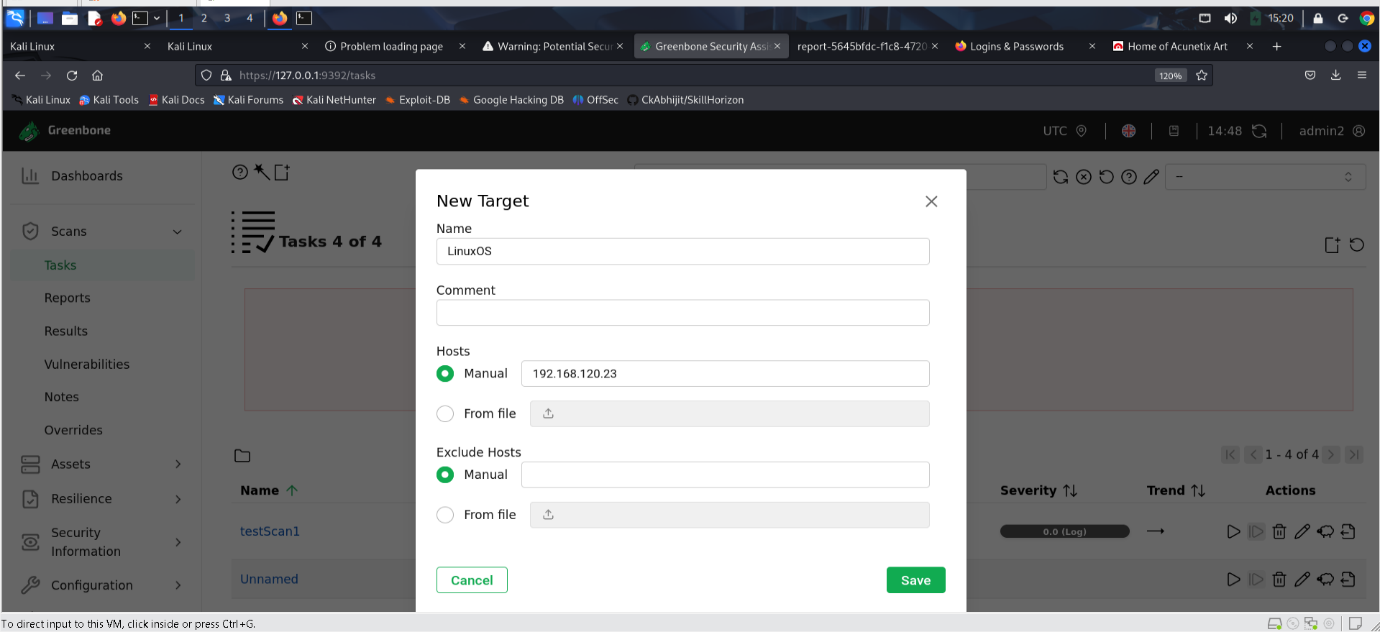




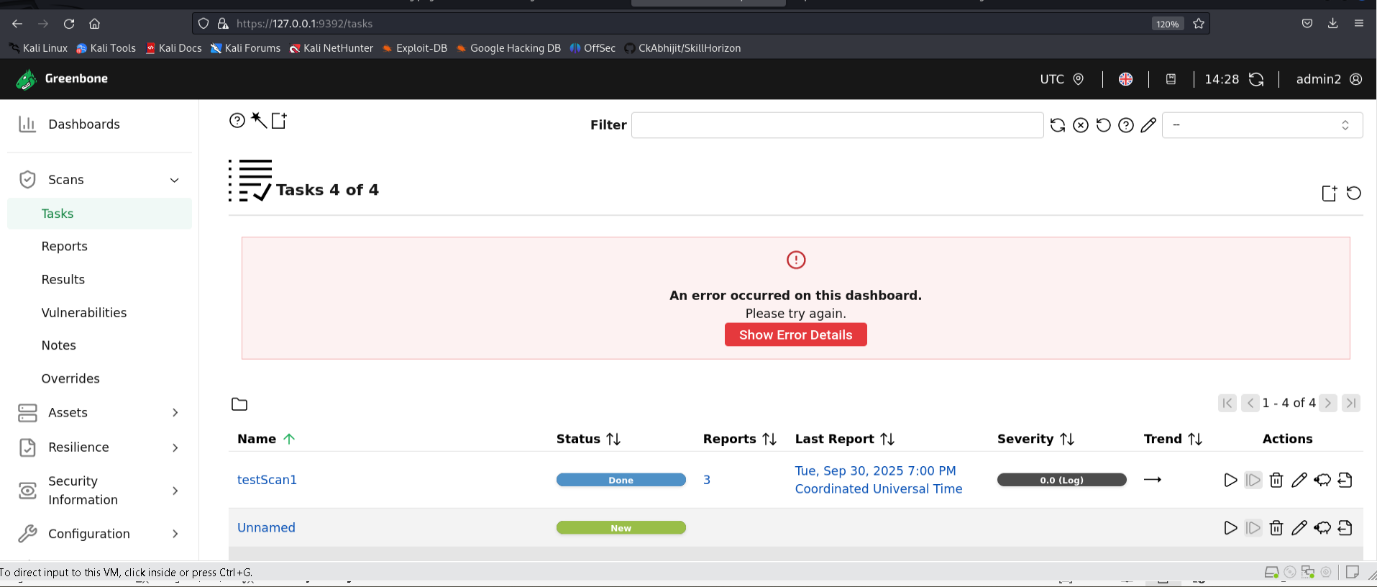
* fill-up the form and save it

2. Set up scan target as your local machine IP or localhost.

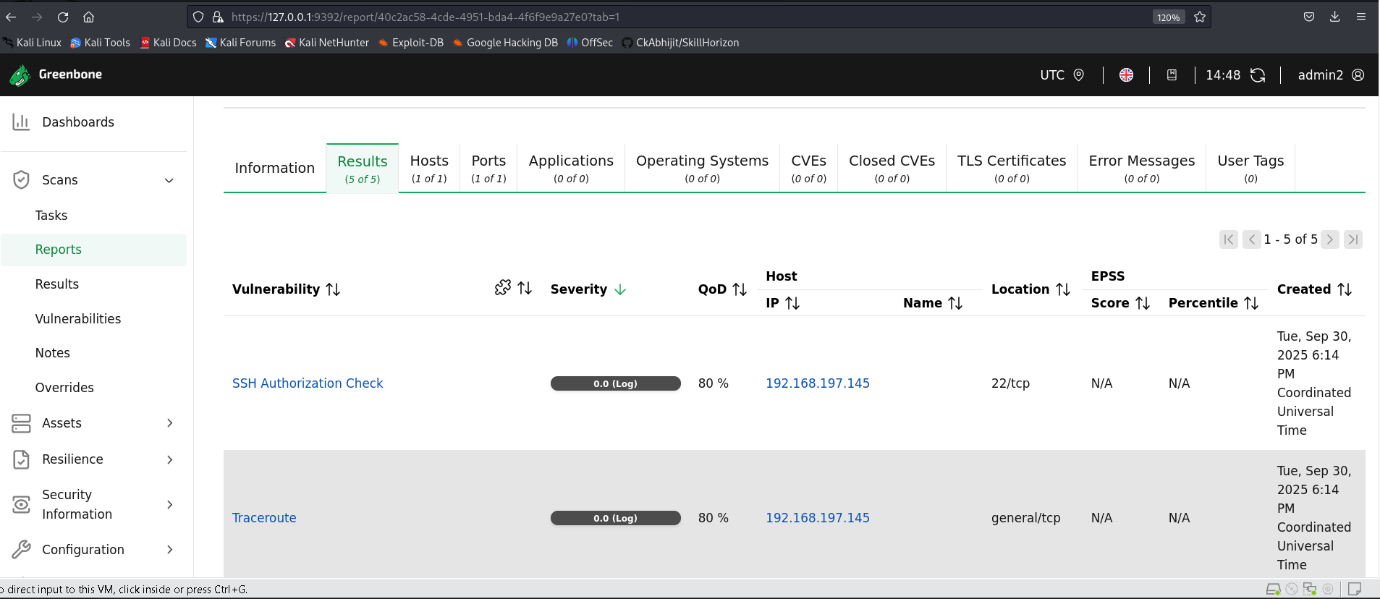
=> Target Name , and Hostname fill-up



* Now save it



* Now start Actions
* Now goto the Reports option click on



* Now we can download scan report in pdf format

