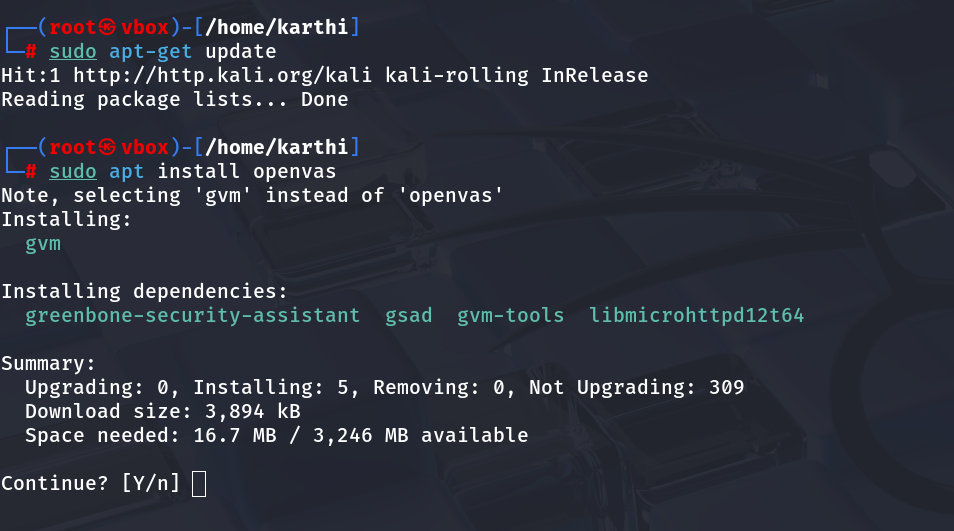
**TASK-3**

## **PERFORM BASIC VULNERABILITY SCAN ON YOUR PC.**

1. **INSTALLING OPENVAS IN LINUX ENVIRONMENT ( KALI ):**

****

* I have installed the openVAS by running the following commands in the linux environment.

**COMMANDS USED :**

**sudo su –** Switching to root user.

**sudo apt get-update –** Updating our linux environment to the latest.

**sudo apt install openvas –** Command to install openvas.

**y –** Confirming the install.

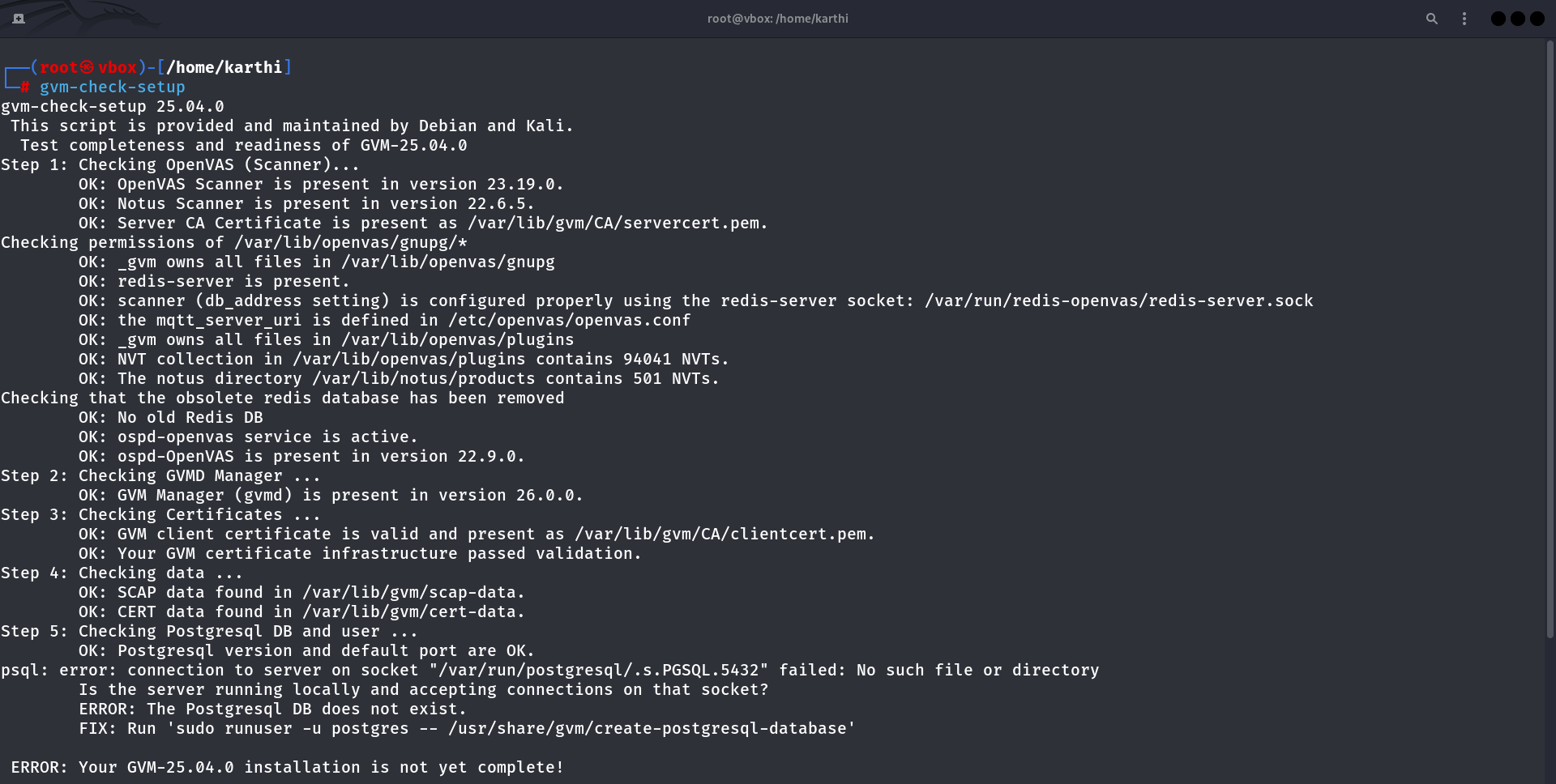
1. **SETTING UP OPENVAS :**

****

* We have to setup the OpenVAS environment after installing.

**COMMAND USED :** gvm-setup.

1. **CHECKING THE SETUP OF OPENVAS :**

****

* **I have checked the connection establishment once again.**

**COMMAND USED :** gvm-check-setup.

1. **INSTALLING PACKAGES RELATED TO GVM :**

**COMMANDS USED :**

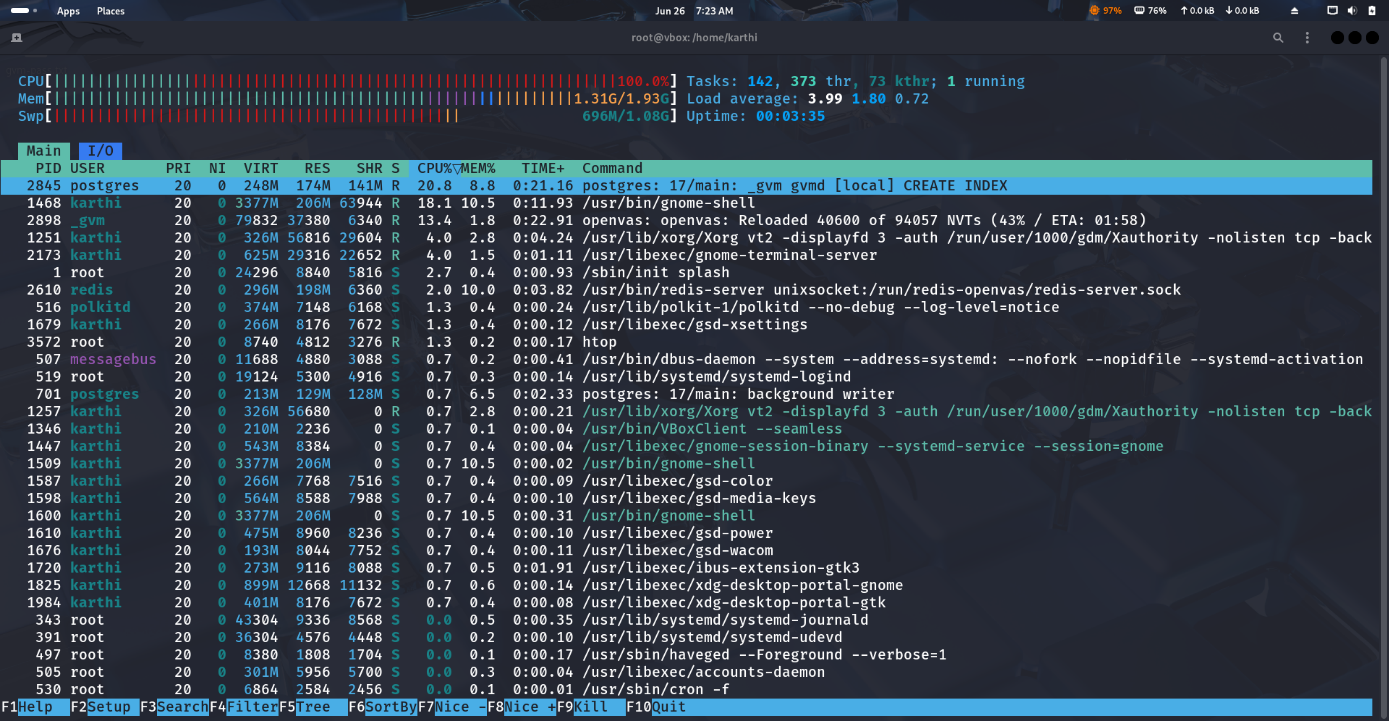
* sudo greenbone-feed-sync --type GVMD\_DATA.
* sudo greenbone-feed-sync --type SCAP.
* sudo greenbone-feed-sync --type CERT.

1. **STARTING AND ENABLING THE SERVICES :**

**COMMANDS USED :**

* gvm-start .
* systemctl start gvmd.service.

1. PROOF OF RUNNING ( CHECKED WITH – htop ):



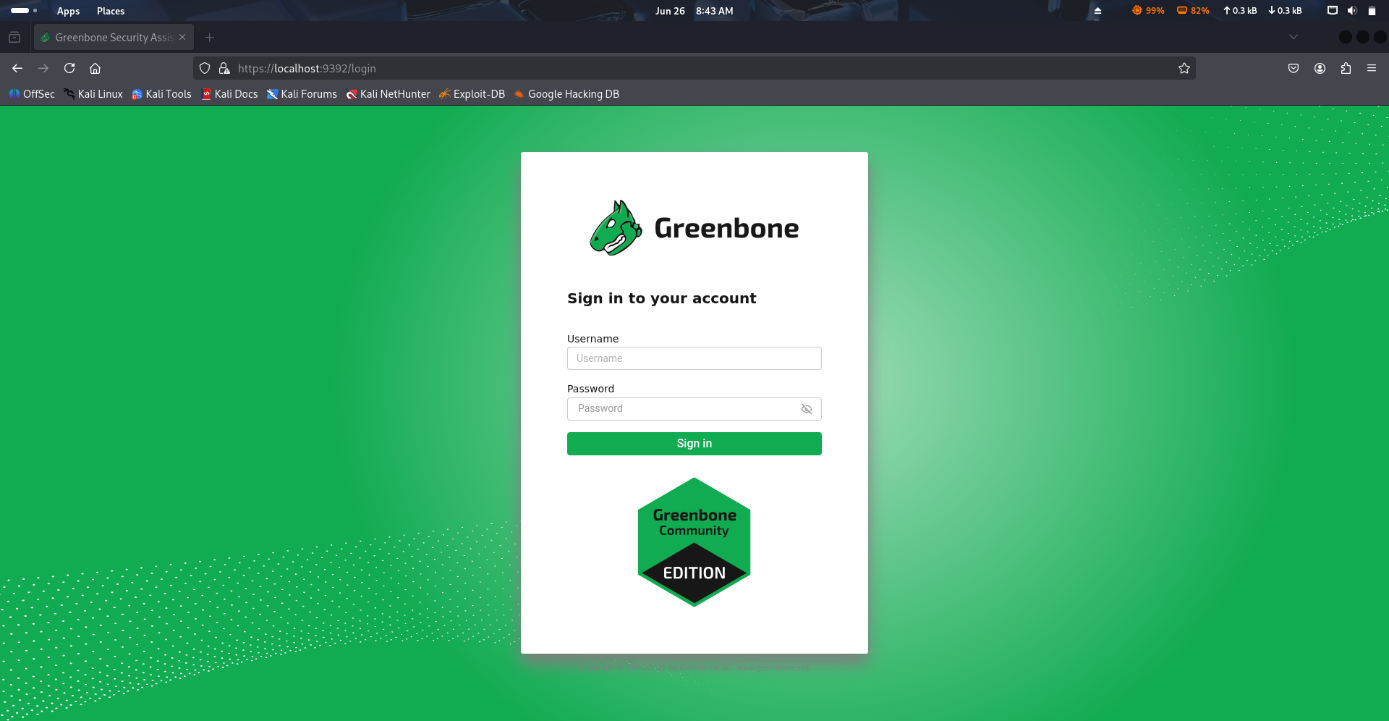
* I have used “htop” command to check what are running currently.

**COMMANDS USED :**

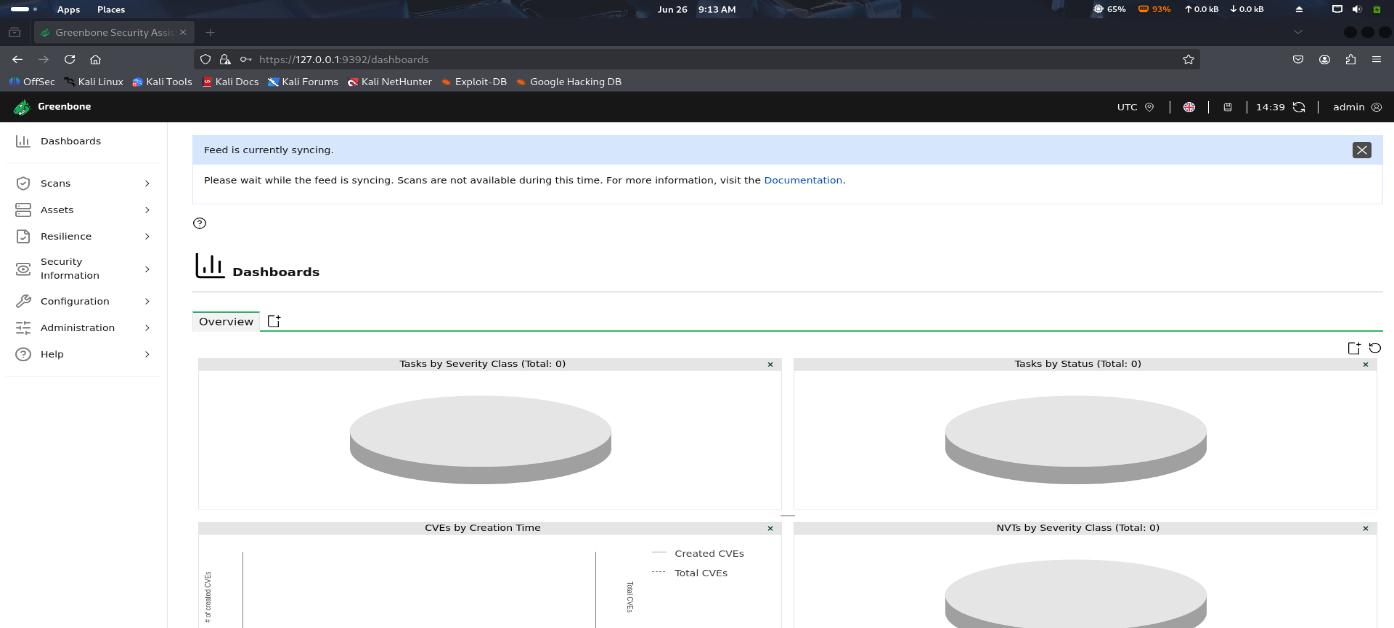
Sudo apt install htop , htop .

1. **OPENING THE SERVICE AND LOGGING IN :**

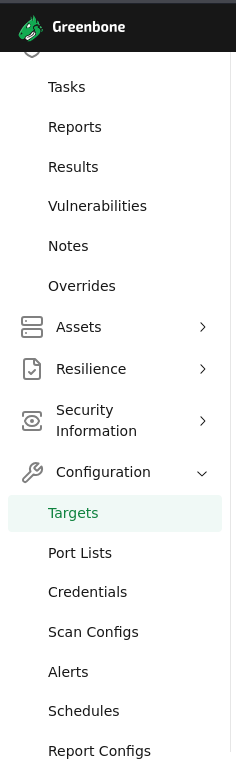
* We have to note down the displayed **username** and **password** when we have checked the gvm setup. ( **gvm-check-setup**).
* Now we will search the website : <https://localhost:9392>
* Enter the credentials to login and visit the dashboard.



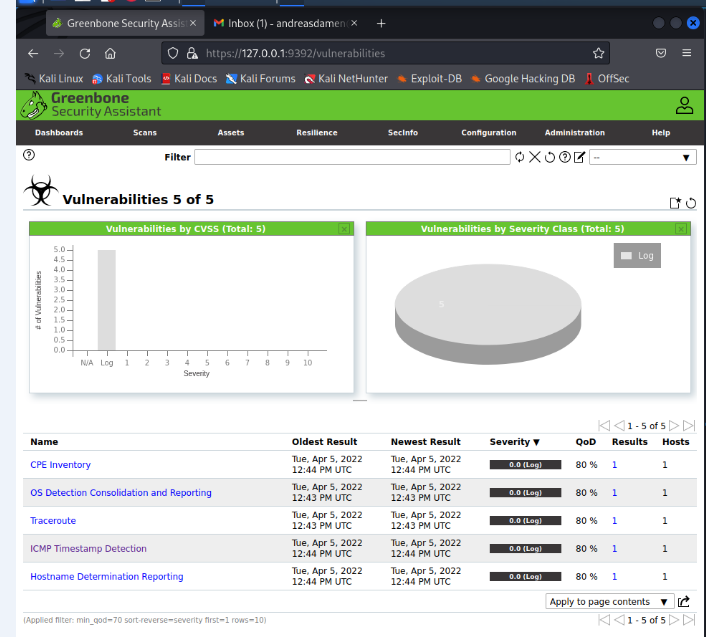
1. **DASHBOARD IMAGE :**



1. **TARGETS SECTION IMAGE :**



1. **SAMPLE RESULTS :**



1. **EXPLANATION :**

| **No.** | **Vulnerability Name** | **Description** |
| --- | --- | --- |
| 1. | **CPE Inventory** | Collects Common Platform Enumeration data to identify installed software and operating systems for vulnerability matching. |
| 2. | **OS Detection Consolidation and Reporting** | Logs and consolidates data for determining the operating system of the target system. |
| 3. | **Traceroute** | Performs a network path trace to the host, which can be useful for network mapping but poses no direct threat. |
| 4. | **ICMP Timestamp Detection** | Detects systems that respond to ICMP timestamp requests. This information can be used to estimate uptime and perform passive reconnaissance. |
| 5. | **Hostname Determination Reporting** | Reports the resolved hostname of the scanned target. Useful for asset identification and inventory. |

**Nanduri Karthikeya.**