Name: Atharva Vasant Angre **Practical No. 8** **UCID: 2024510001**

Aim:

To implement and configure Greenbone Vulnerability Management (GVM) for effective monitoring and scanning of network vulnerabilities, ensuring proactive detection of security issues and improving overall cybersecurity posture.

Objectives:

- To install and configure Greenbone GVM for vulnerability scanning of hosts and network infrastructure.
- To enable real-time alerting for detected vulnerabilities and critical security risks.
- To monitor systems for weaknesses such as outdated software, misconfigurations, and open ports.
- To integrate additional feeds and plugins for comprehensive vulnerability coverage.
- To enhance IT security reliability through proactive vulnerability management and threat detection.

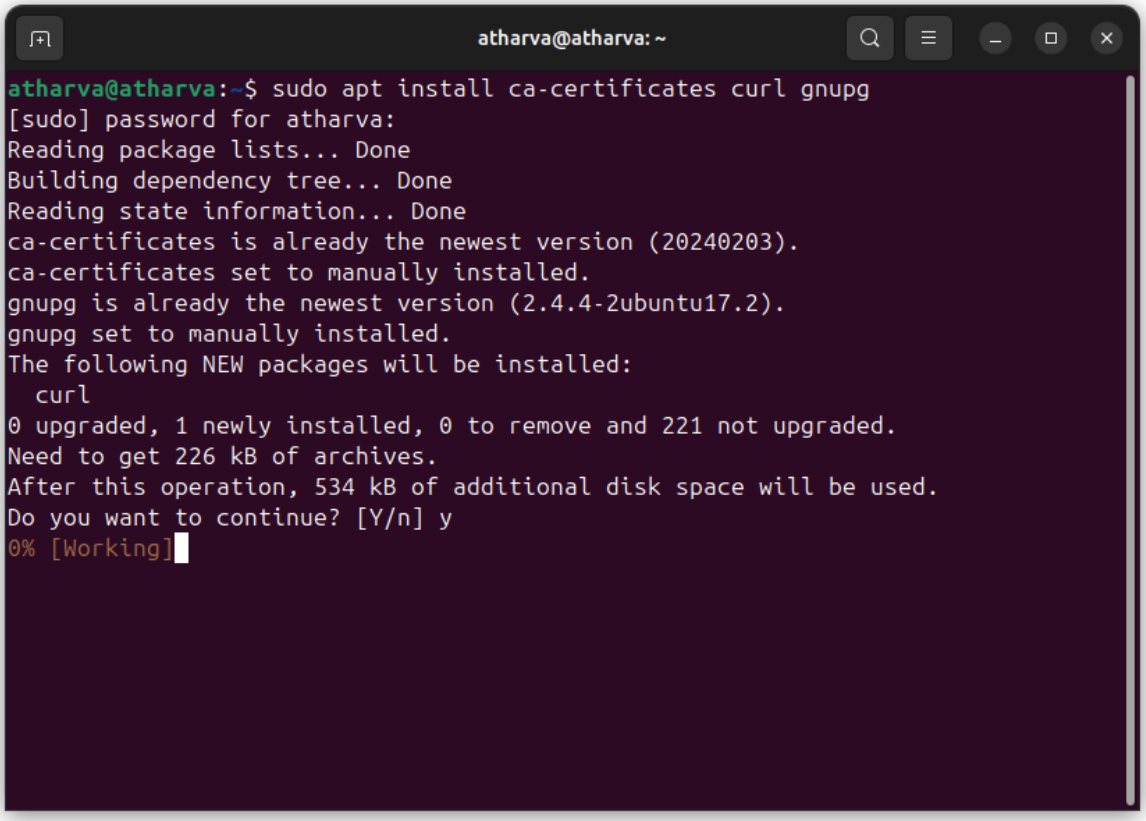
Tools Used:

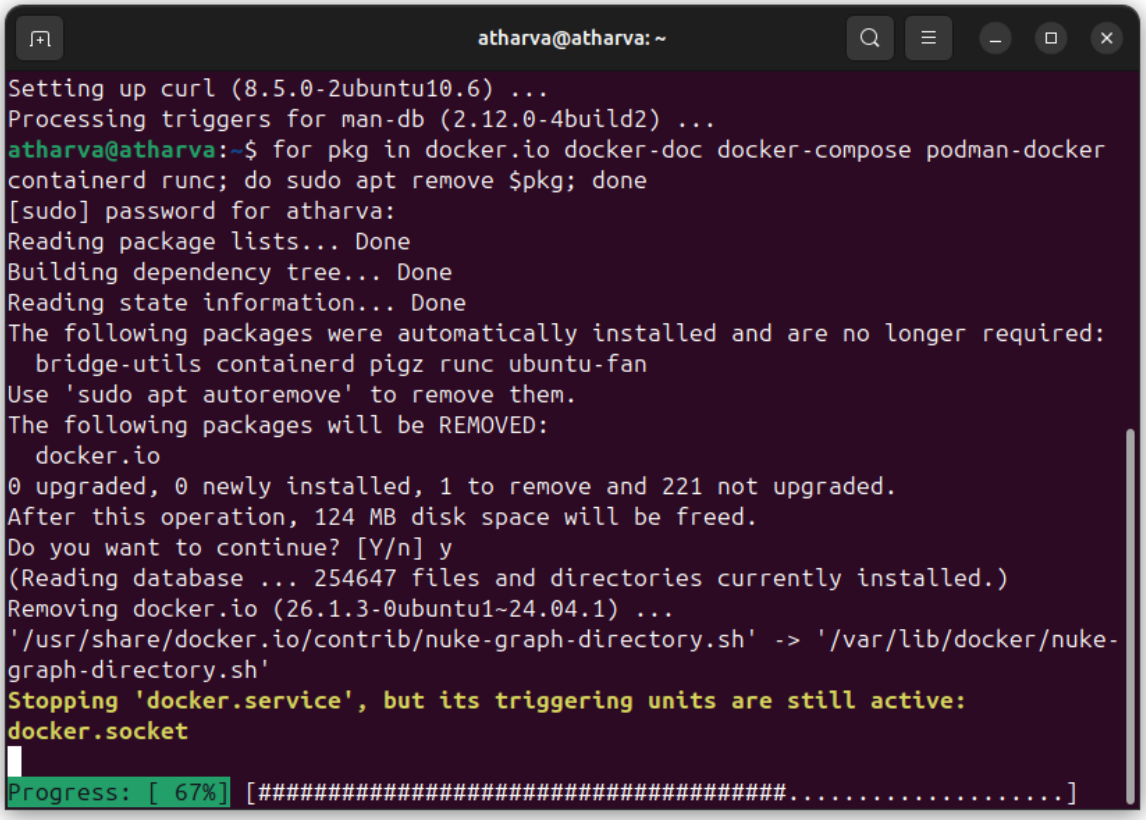
VirtualBox

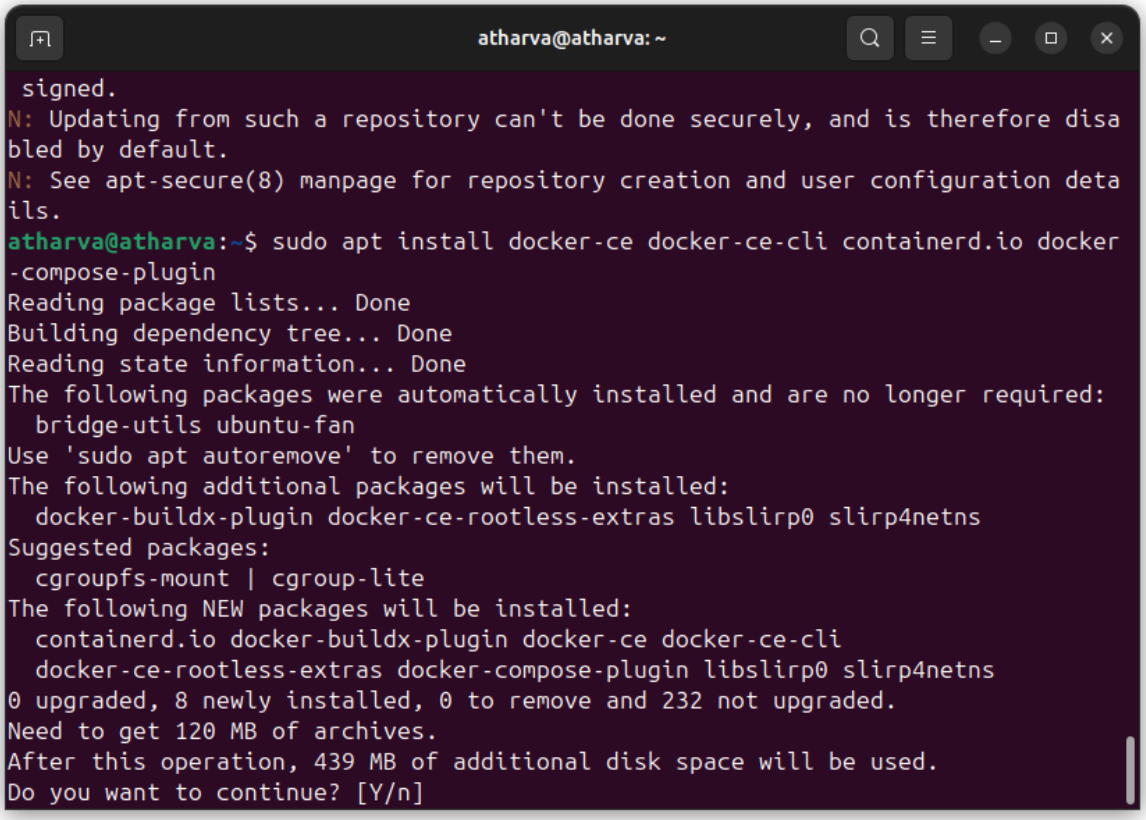
Ubuntu (Linux OS)

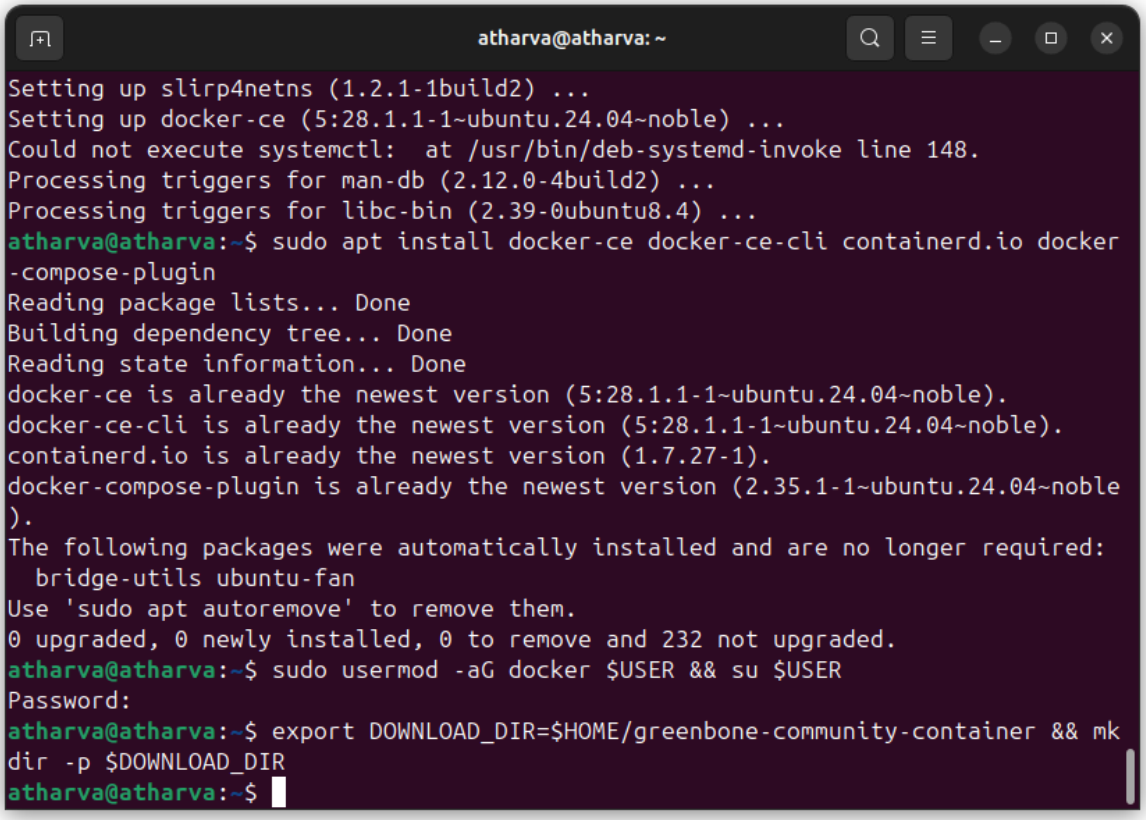
Greenbone Vulnerability Management (GVM)

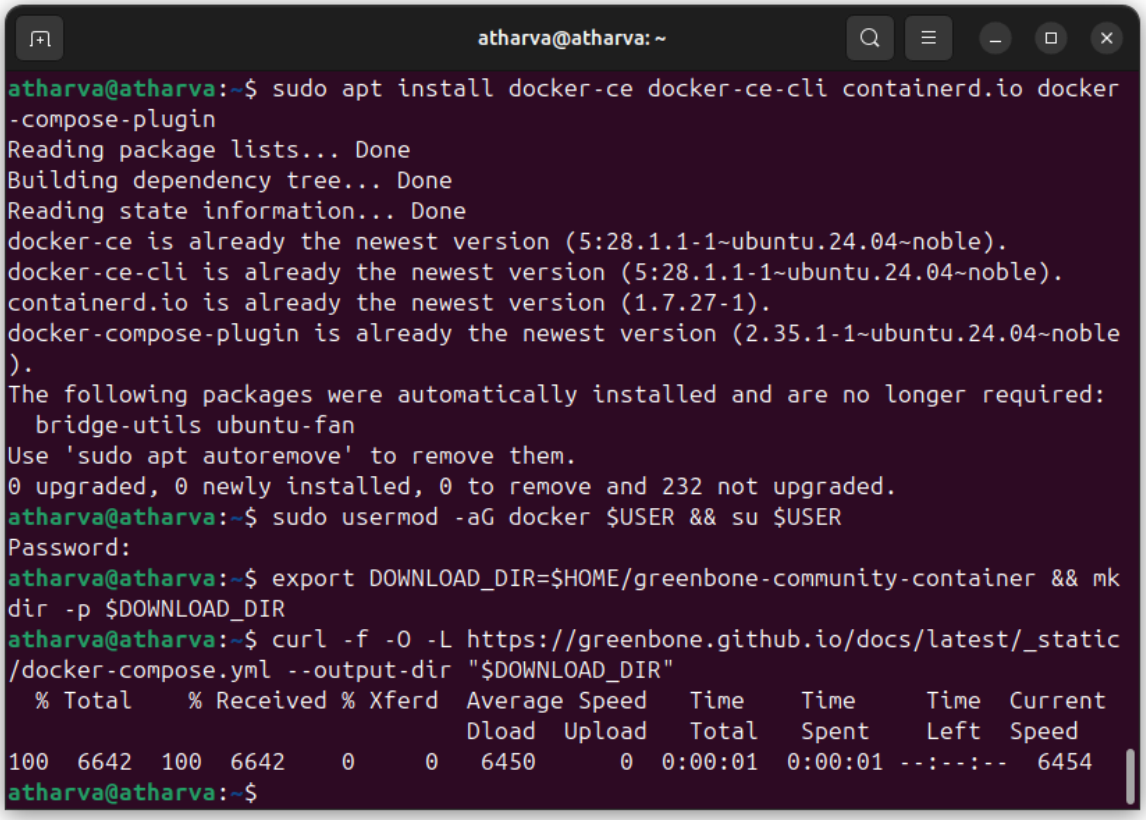
Greenbone Security Assistant (GSA)



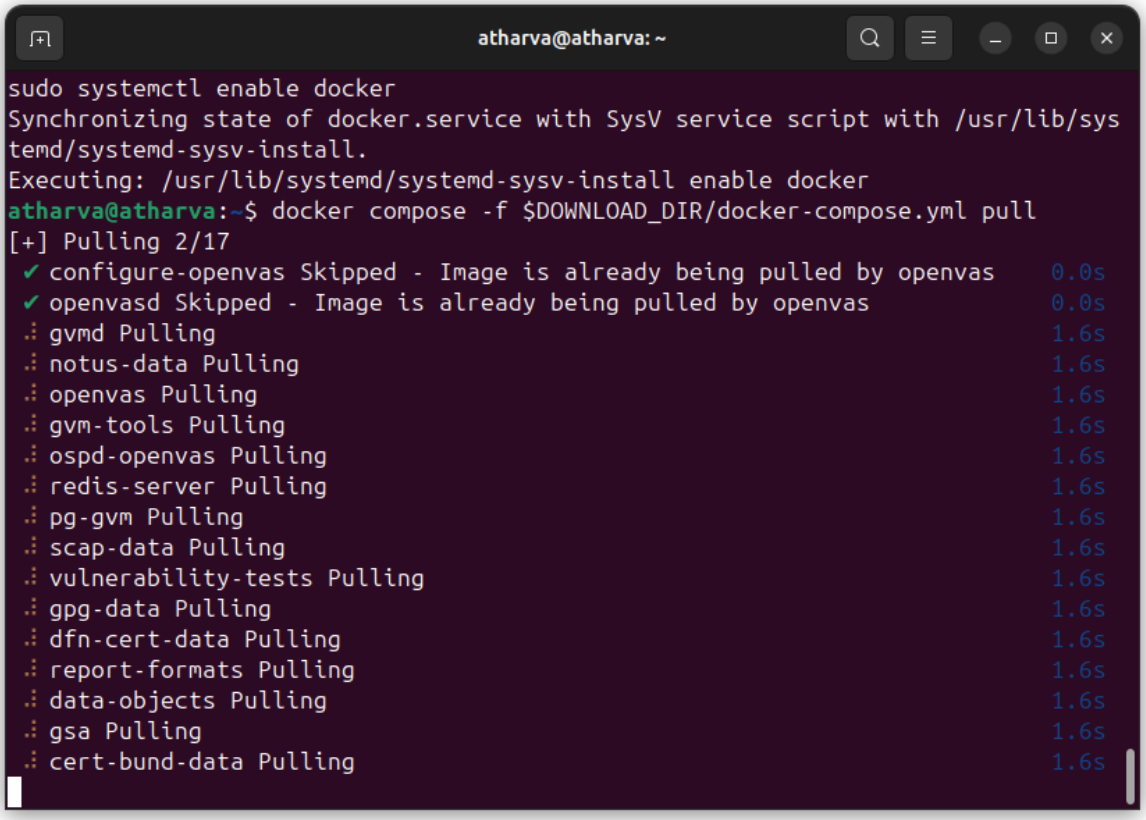

atharva@atharva: ~
Setting up curl (8.5.0-2ubuntu10.6) ...
Processing triggers for man-db (2.12.0-4build2) ...
atharva@atharva:~$ for pkg in docker.io docker-doc docker-compose podman-docker containerd runc; do sudo apt remove $pkg; done
[sudo] password for atharva:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
bridge-utils containerd pigz runc ubuntu-fan
Use 'sudo apt autoremove' to remove them.
The following packages will be REMOVED:
docker.io
0 upgraded, 0 newly installed, 1 to remove and 221 not upgraded.
After this operation, 124 MB disk space will be freed.
Do you want to continue? [Y/n] y
(Reading database ... 254647 files and directories currently installed.)
Removing docker.io (26.1.3-0ubuntu1~24.04.1) ...
'/usr/share/docker.io/contrib/nuke-graph-directory.sh' -> '/var/lib/docker/nuke-graph-directory.sh'
Stopping 'docker.service', but its triggering units are still active:
docker.socket
Progress: [67%] [###.....................]

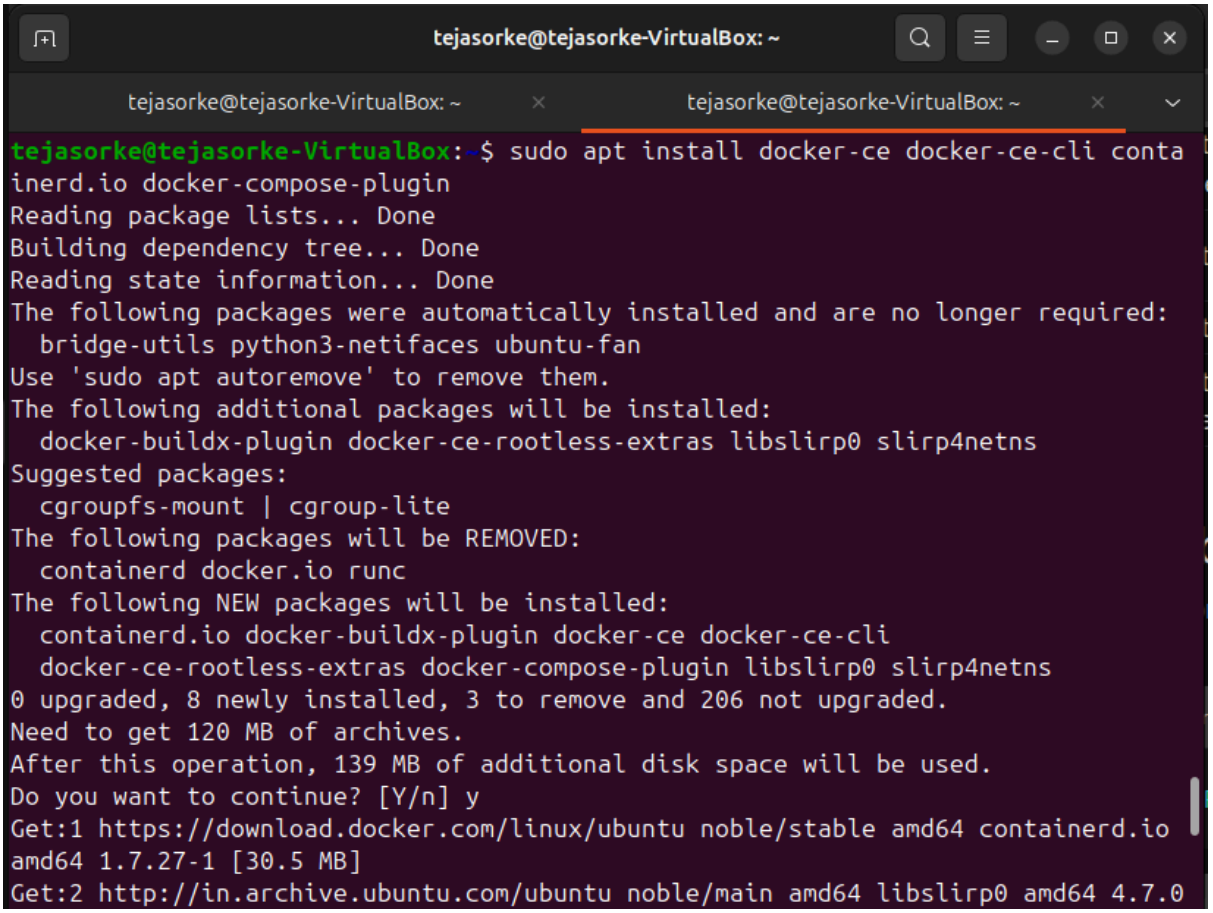

atharva@atharva: ~
signed.
N: Updating from such a repository can't be done securely, and is therefore disabled by default.
N: See apt-secure(8) manpage for repository creation and user configuration details.
atharva@atharva:~$ sudo apt install docker-ce docker-ce-cli containerd.io docker-compose-plugin
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
bridge-utils ubuntu-fan
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
docker-buildx-plugin docker-ce-rootless-extras libslirp0 slirp4netns
Suggested packages:
cgroupfs-mount | cgroup-lite
The following NEW packages will be installed:
containerd.io docker-buildx-plugin docker-ce docker-ce-cli
docker-ce-rootless-extras docker-compose-plugin libslirp0 slirp4netns
0 upgraded, 8 newly installed, 0 to remove and 232 not upgraded.
Need to get 120 MB of archives.
After this operation, 439 MB of additional disk space will be used.
Do you want to continue? [Y/n]


atharva@atharva: ~
Setting up slirp4netns (1.2.1-1build2) ...
Setting up docker-ce (5:28.1.1-1~ubuntu.24.04~noble) ...
Could not execute systemctl: at /usr/bin/deb-systemd-invoke line 148.
Processing triggers for man-db (2.12.0-4build2) ...
Processing triggers for libc-bin (2.39-0ubuntu8.4) ...
atharva@atharva:~$ sudo apt install docker-ce docker-ce-cli containerd.io docker
-compose-plugin
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
docker-ce is already the newest version (5:28.1.1-1~ubuntu.24.04~noble).
docker-ce-cli is already the newest version (5:28.1.1-1~ubuntu.24.04~noble).
containerd.io is already the newest version (1.7.27-1).
docker-compose-plugin is already the newest version (2.35.1-1~ubuntu.24.04~noble
).
The following packages were automatically installed and are no longer required:
  bridge-utils ubuntu-fan
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 232 not upgraded.
atharva@atharva:~$ sudo usermod -aG docker $USER && su $USER
Password:
atharva@atharva:~$ export DOWNLOAD_DIR=$HOME/greenbone-community-container && mk
dir -p $DOWNLOAD_DIR
atharva@atharva:~$


atharva@atharva: ~
atharva@atharva:~$ sudo apt install docker-ce docker-ce-cli containerd.io docker
-compose-plugin
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
docker-ce is already the newest version (5:28.1.1-1~ubuntu.24.04~noble).
docker-ce-cli is already the newest version (5:28.1.1-1~ubuntu.24.04~noble).
containerd.io is already the newest version (1.7.27-1).
docker-compose-plugin is already the newest version (2.35.1-1~ubuntu.24.04~noble
).
The following packages were automatically installed and are no longer required:
  bridge-utils ubuntu-fan
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 232 not upgraded.
atharva@atharva:~$ sudo usermod -aG docker $USER && su $USER
Password:
atharva@atharva:~$ export DOWNLOAD_DIR=$HOME/greenbone-community-container && mk
dir -p $DOWNLOAD_DIR
atharva@atharva:~$ curl -f -O -L https://greenbone.github.io/docs/latest/_static
/docker-compose.yml --output-dir "$DOWNLOAD_DIR"
  % Total   % Received % Xferd Average Speed   Time   Time   Time Current
                                 Dload Upload   Total   Spent   Left Speed
100 6642 100 6642   0   0   6450   0 0:00:01 0:00:01 --:--:-- 6454
atharva@atharva:~$

```
tejasorke@tejasorke-VirtualBox:~$ sudo install -m 0755 -d /etc/apt/keyrings
curl -fsSL https://download.docker.com/linux/ubuntu/gpg | sudo gpg --dearmor -o
/etc/apt/keyrings/docker.gpg
sudo chmod a+r /etc/apt/keyrings/docker.gpg
echo \
  "deb [arch="$(dpkg --print-architecture)" signed-by=/etc/apt/keyrings/docker.g
pg] https://download.docker.com/linux/ubuntu \
  "$(. /etc/os-release && echo "$VERSION_CODENAME")" stable" | \
  sudo tee /etc/apt/sources.list.d/docker.list > /dev/null
sudo apt update
Get:1 https://download.docker.com/linux/ubuntu noble InRelease [48.8 kB]
Ign:2 https://pkg.jenkins.io/debian-stable binary/ InRelease
Hit:3 https://pkg.jenkins.io/debian-stable binary/ Release
Hit:4 http://in.archive.ubuntu.com/ubuntu noble InRelease
Get:5 http://in.archive.ubuntu.com/ubuntu noble-updates InRelease [126 kB]
Get:7 http://security.ubuntu.com/ubuntu noble-security InRelease [126 kB]
Hit:8 https://ppa.launchpadcontent.net/ansible/ansible/ubuntu noble InRelease
Ign:9 https://ppa.launchpadcontent.net/mrazavi/gvm/ubuntu noble InRelease
Err:10 https://ppa.launchpadcontent.net/mrazavi/gvm/ubuntu noble Release
  404  Not Found [IP: 185.125.190.80 443]
Get:11 https://download.docker.com/linux/ubuntu noble/stable amd64 Packages [24.
0 kB]
Get:12 http://in.archive.ubuntu.com/ubuntu noble-backports InRelease [126 kB]
```





Docker compose.yml

```
name: greenbone-community-edition


services:
  vulnerability-tests:
    image: registry.community.greenbone.net/community/vulnerability-tests
    environment:
      FEED_RELEASE: "24.10"
    volumes:
      - vt_data_vol:/mnt


  notus-data:
    image: registry.community.greenbone.net/community/notus-data
    volumes:
      - notus_data_vol:/mnt
```

```
scap-data:
  image: registry.community.greenbone.net/community/scap-data
  volumes:
    - scap_data_vol:/mnt

cert-bund-data:
  image: registry.community.greenbone.net/community/cert-bund-data
  volumes:
    - cert_data_vol:/mnt

dfn-cert-data:
  image: registry.community.greenbone.net/community/dfn-cert-data
  volumes:
    - cert_data_vol:/mnt
  depends_on:
    - cert-bund-data

data-objects:
  image: registry.community.greenbone.net/community/data-objects
  environment:
    FEED_RELEASE: "24.10"
  volumes:
    - data_objects_vol:/mnt

report-formats:
  image: registry.community.greenbone.net/community/report-formats
  environment:
    FEED_RELEASE: "24.10"
  volumes:
```

```
    - data_objects_vol:/mnt
  depends_on:
    - data-objects

gpg-data:
  image: registry.community.greenbone.net/community/gpg-data
  volumes:
    - gpg_data_vol:/mnt

redis-server:
  image: registry.community.greenbone.net/community/redis-server
  restart: on-failure
  volumes:
    - redis_socket_vol:/run/redis/

pg-gvm:
  image: registry.community.greenbone.net/community/pg-gvm:stable
  restart: on-failure
  volumes:
    - psql_data_vol:/var/lib/postgresql
    - psql_socket_vol:/var/run/postgresql

gvmd:
  image: registry.community.greenbone.net/community/gvmd:stable
  restart: on-failure
  volumes:
    - gvmd_data_vol:/var/lib/gvm
    - scap_data_vol:/var/lib/gvm/scap-data/
    - cert_data_vol:/var/lib/gvm/cert-data
    - data_objects_vol:/var/lib/gvm/data-objects/gvmd
```

```
    - vt_data_vol:/var/lib/openvas/plugins
    - psql_data_vol:/var/lib/postgresql
    - gvmd_socket_vol:/run/gvmd
    - ospd_openvas_socket_vol:/run/ospd
    - psql_socket_vol:/var/run/postgresql
  depends_on:
    pg-gvm:
      condition: service_started
    scap-data:
      condition: service_completed_successfully
    cert-bund-data:
      condition: service_completed_successfully
    dfn-cert-data:
      condition: service_completed_successfully
    data-objects:
      condition: service_completed_successfully
    report-formats:
      condition: service_completed_successfully

gsa:
  image: registry.community.greenbone.net/community/gsa:stable
  restart: on-failure
  ports:
    - 127.0.0.1:9392:80
  volumes:
    - gvmd_socket_vol:/run/gvmd
  depends_on:
    - gvmd
# Sets log level of openvas to the set LOG_LEVEL within the env
# and changes log output to /var/log/openvas instead /var/log/gvm
```

```
  # to reduce likelyhood of unwanted log interferences
  configure-openvas:
    image: registry.community.greenbone.net/community/openvas-scanner:stable
    volumes:
      - openvas_data_vol:/mnt
      - openvas_log_data_vol:/var/log/openvas
    command:
      - /bin/sh
      - -c
      - |
        printf "table_driven_lsc = yes\nopenvasd_server = http://openvasd:80\n" >
/mnt/openvas.conf
        sed "s/127/128/" /etc/openvas/openvas_log.conf | sed 's/gvm/openvas/' >
/mnt/openvas_log.conf
        chmod 644 /mnt/openvas.conf
        chmod 644 /mnt/openvas_log.conf
        touch /var/log/openvas/openvas.log
        chmod 666 /var/log/openvas/openvas.log


  # shows logs of openvas
  openvas:
    image: registry.community.greenbone.net/community/openvas-scanner:stable
    restart: on-failure
    volumes:
      - openvas_data_vol:/etc/openvas
      - openvas_log_data_vol:/var/log/openvas
    command:
      - /bin/sh
      - -c
      - |
        cat /etc/openvas/openvas.conf
```

```
    tail -f /var/log/openvas/openvas.log
  depends_on:
    configure-openvas:
      condition: service_completed_successfully


openvasd:
  image: registry.community.greenbone.net/community/openvas-scanner:stable
  restart: on-failure
  environment:
    # `service_notus` is set to disable everything but notus,
    # if you want to utilize openvasd directly, remove `OPENVASD_MODE`
    OPENVASD_MODE: service_notus
    GNUPGHOME: /etc/openvas/gnupg
    LISTENING: 0.0.0.0:80
  volumes:
    - openvas_data_vol:/etc/openvas
    - openvas_log_data_vol:/var/log/openvas
    - gpg_data_vol:/etc/openvas/gnupg
    - notus_data_vol:/var/lib/notus
  # enable port forwarding when you want to use the http api from your host machine
  # ports:
  #   - 127.0.0.1:3000:80
  depends_on:
    vulnerability-tests:
      condition: service_completed_successfully
    configure-openvas:
      condition: service_completed_successfully
    gpg-data:
      condition: service_completed_successfully
  networks:
```

```
    default:
      aliases:
        - openvasd


ospd-openvas:
  image: registry.community.greenbone.net/community/ospd-openvas:stable
  restart: on-failure
  hostname: ospd-openvas.local
  cap_add:
    - NET_ADMIN # for capturing packages in promiscuous mode
    - NET_RAW # for raw sockets e.g. used for the boreas alive detection
  security_opt:
    - seccomp=unconfined
    - apparmor=unconfined
  command:
    [
      "ospd-openvas",
      "-f",
      "--config",
      "/etc/gvm/ospd-openvas.conf",
      "--notus-feed-dir",
      "/var/lib/notus/advisories",
      "-m",
      "666",
    ]
  volumes:
    - gpg_data_vol:/etc/openvas/gnupg
    - vt_data_vol:/var/lib/openvas/plugins
    - notus_data_vol:/var/lib/notus
    - ospd_openvas_socket_vol:/run/ospd
```

```
    - redis_socket_vol:/run/redis/
    - openvas_data_vol:/etc/openvas/
    - openvas_log_data_vol:/var/log/openvas
  depends_on:
    redis-server:
      condition: service_started
    gpg-data:
      condition: service_completed_successfully
    vulnerability-tests:
      condition: service_completed_successfully
    configure-openvas:
      condition: service_completed_successfully

 gvm-tools:
  image: registry.community.greenbone.net/community/gvm-tools
  volumes:
    - gvmd_socket_vol:/run/gvmd
    - ospd_openvas_socket_vol:/run/ospd
  depends_on:
    - gvmd
    - ospd-openvas

volumes:
 gpg_data_vol:
 scap_data_vol:
 cert_data_vol:
 data_objects_vol:
 gvmd_data_vol:
 psql_data_vol:
 vt_data_vol:
```

notus_data_vol:

psql_socket_vol:

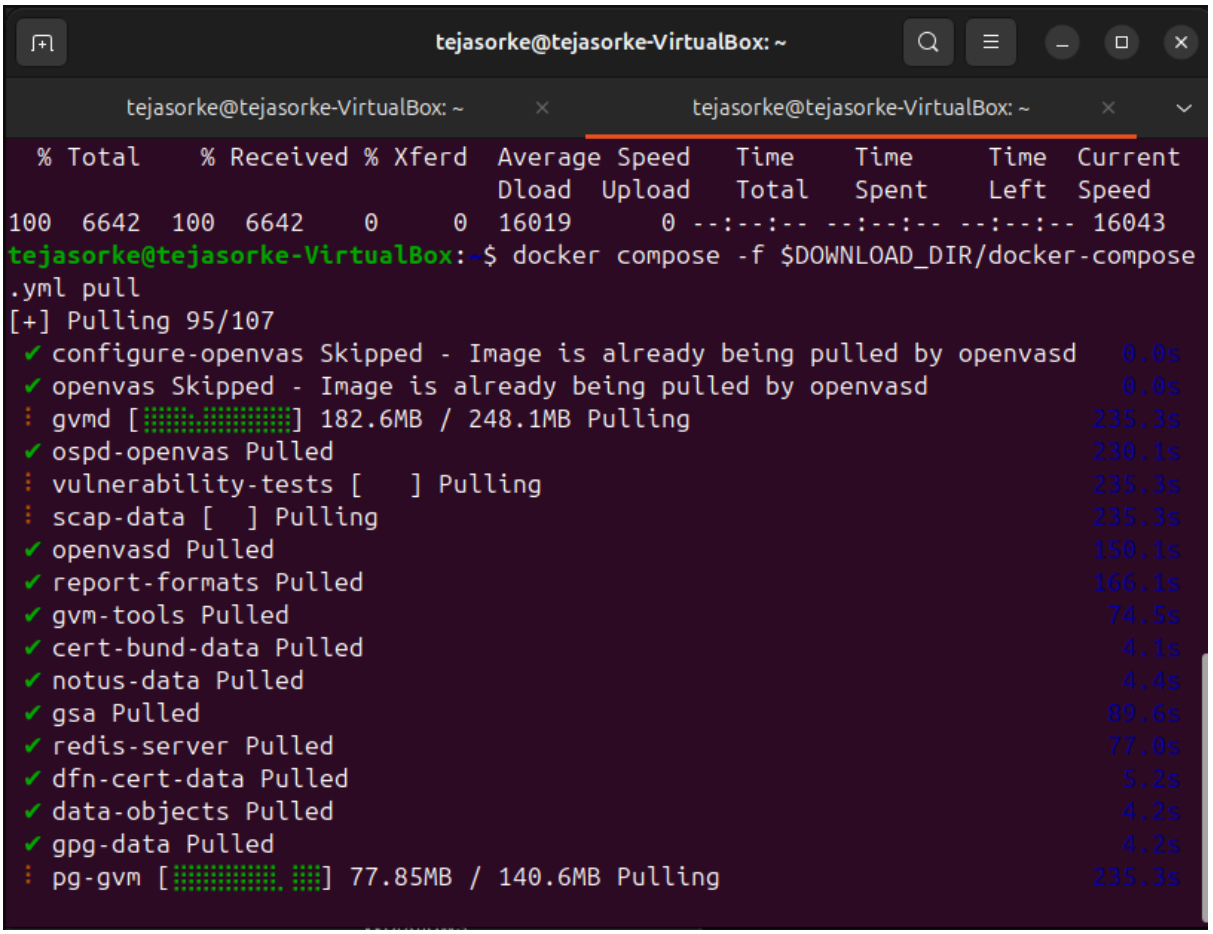
gvmd_socket_vol:

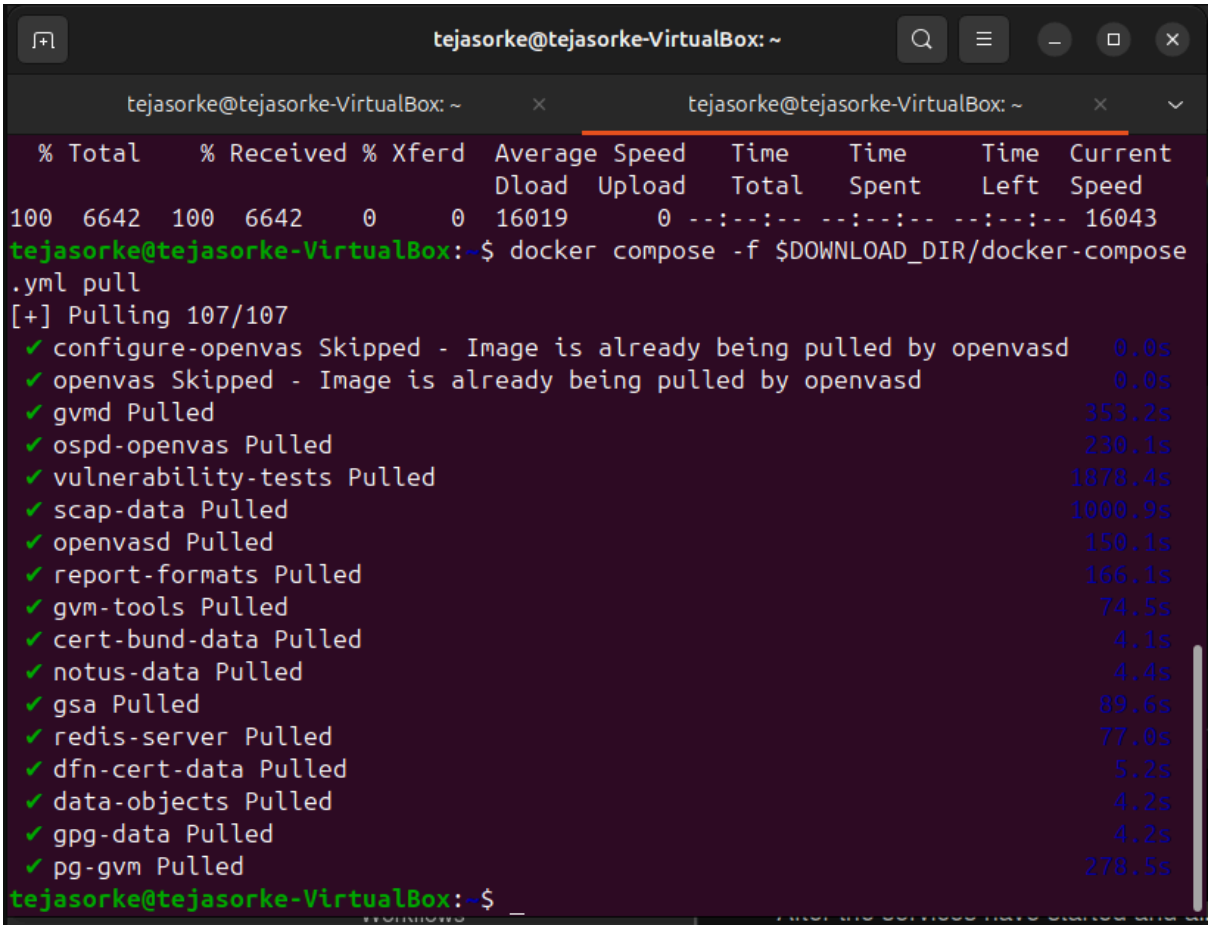
ospd_openvas_socket_vol:

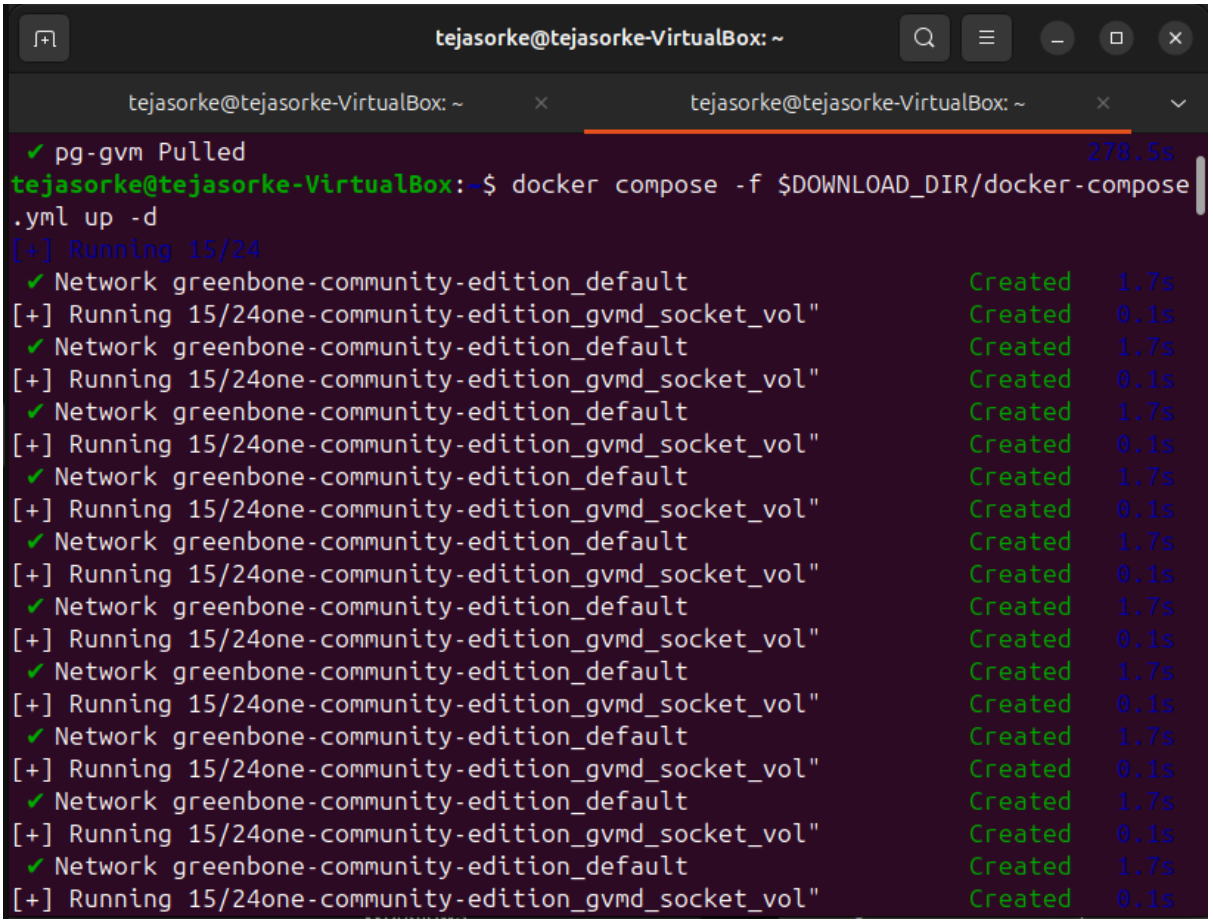
redis_socket_vol:

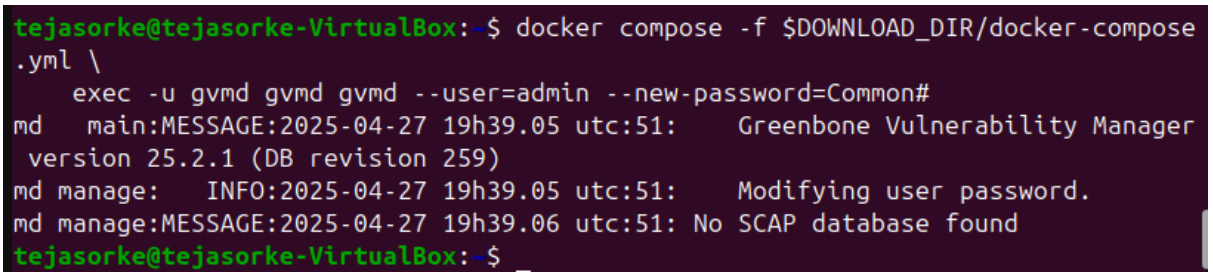
openvas_data_vol:

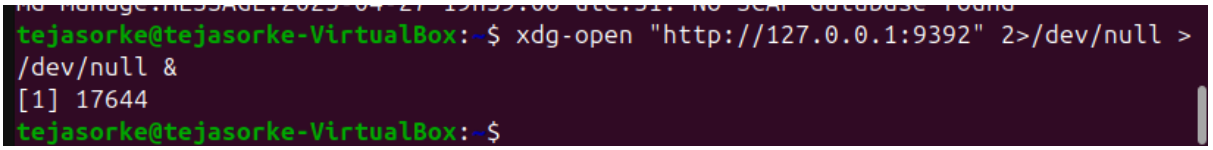
openvas_log_data_vol:



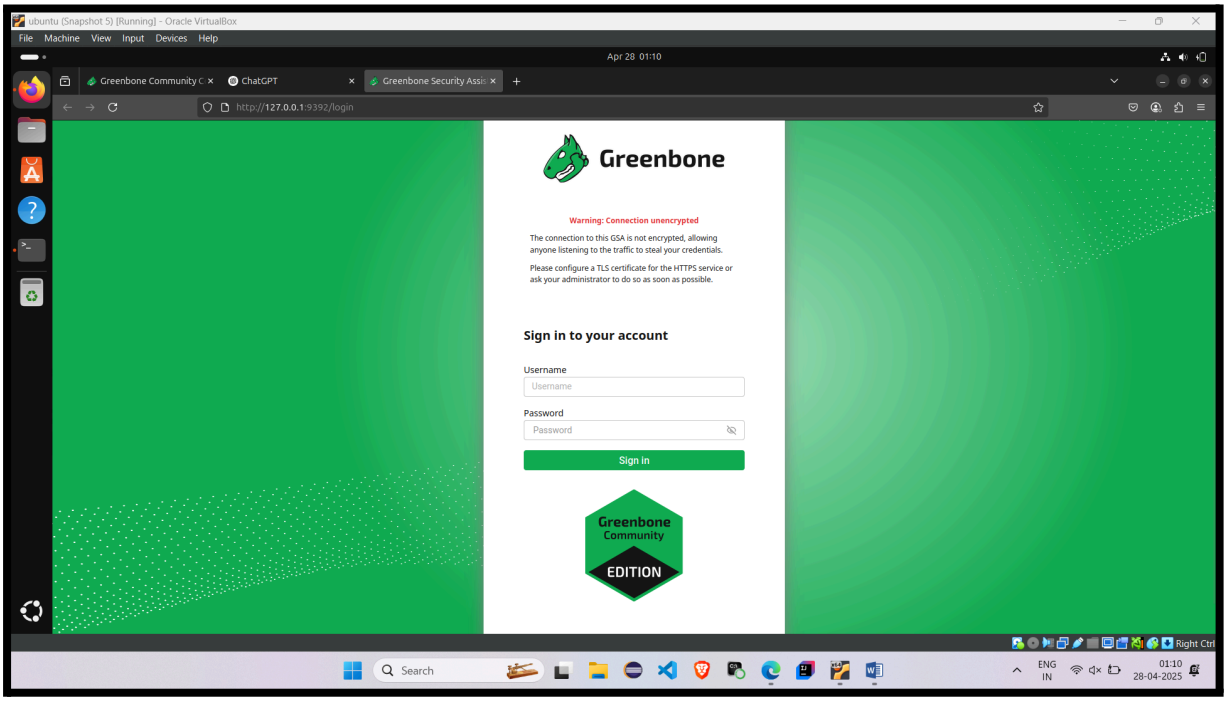

tejasorke@tejasorke-VirtualBox: ~
tejasorke@tejasorke-VirtualBox: ~
tejasorke@tejasorke-VirtualBox: ~
% Total % Received % Xferd Average Speed Time Time Time Current
Dload Upload Total Spent Left Speed
100 6642 100 6642 0 0 16019 0 --:--:-- --:--:-- --:--:-- 16043
tejasorke@tejasorke-VirtualBox:~$ docker compose -f $DOWNLOAD_DIR/docker-compose
.yml pull
[+] Pulling 107/107
✔ configure-openvas Skipped - Image is already being pulled by openvasd 0.0s
✔ openvas Skipped - Image is already being pulled by openvasd 0.0s
✔ gvmd Pulled 353.2s
✔ ospd-openvas Pulled 230.1s
✔ vulnerability-tests Pulled 1878.4s
✔ scap-data Pulled 1000.9s
✔ openvasd Pulled 150.1s
✔ report-formats Pulled 166.1s
✔ gvm-tools Pulled 74.5s
✔ cert-bund-data Pulled 4.1s
✔ notus-data Pulled 4.4s
✔ gsa Pulled 89.6s
✔ redis-server Pulled 77.0s
✔ dfn-cert-data Pulled 5.2s
✔ data-objects Pulled 4.2s
✔ gpg-data Pulled 4.2s
✔ pg-gvm Pulled 278.5s
tejasorke@tejasorke-VirtualBox:~$ _


tejasorke@tejasorke-VirtualBox: ~
tejasorke@tejasorke-VirtualBox: ~
tejasorke@tejasorke-VirtualBox: ~
✔ pg-gvm Pulled 278.5s
tejasorke@tejasorke-VirtualBox:~$ docker compose -f $DOWNLOAD_DIR/docker-compose.yml up -d
[+] Running 15/24
✔ Network greenbone-community-edition_default Created 1.7s
[+] Running 15/24one-community-edition_gvmd_socket_vol" Created 0.1s

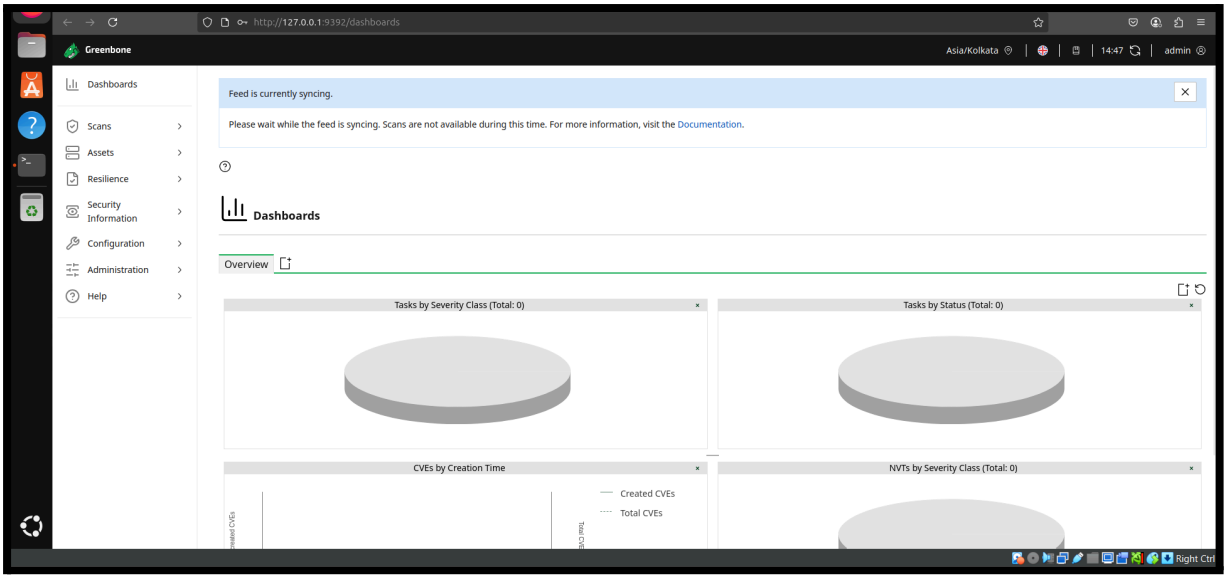

tejasorke@tejasorke-VirtualBox:~$ docker compose -f $DOWNLOAD_DIR/docker-compose.yml \
exec -u gvmd gvmd gvmd --user=admin --new-password=Common#
md main:MESSAGE:2025-04-27 19h39.05 utc:51: Greenbone Vulnerability Manager version 25.2.1 (DB revision 259)
md manage: INFO:2025-04-27 19h39.05 utc:51: Modifying user password.
md manage:MESSAGE:2025-04-27 19h39.06 utc:51: No SCAP database found
tejasorke@tejasorke-VirtualBox:~$

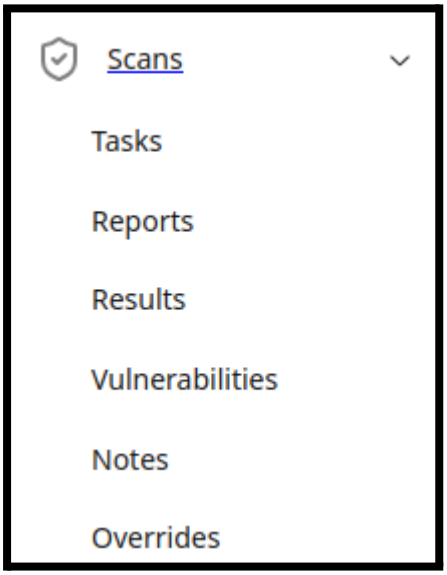

tejasorke@tejasorke-VirtualBox:~$ xdg-open "http://127.0.0.1:9392" 2>/dev/null >/dev/null &
[1] 17644
tejasorke@tejasorke-VirtualBox:~$

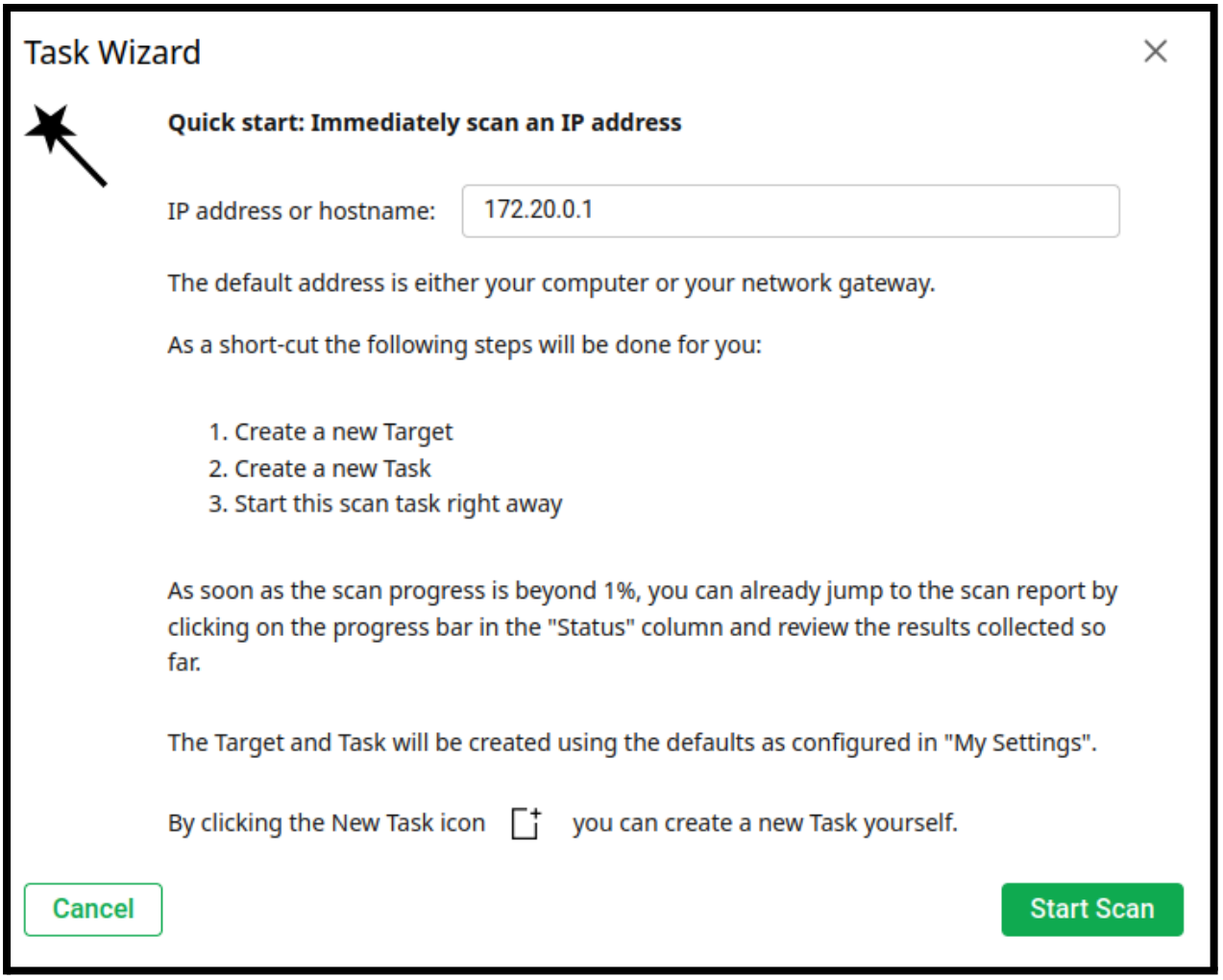
```
tejasorke@tejasorke-VirtualBox:~/greenbone-community-container$ sudo docker comp
ose -f $DOWNLOAD_DIR/docker-compose.yml run --rm greenbone-feed-sync greenbone-f
eed-sync --type nasl
Trying to acquire lock on /var/lib/openvas/feed-update.lock
Acquired lock on /var/lib/openvas/feed-update.lock
 Downloading NASL files from
rsync://feed.community.greenbone.net/community/vulnerability-feed/24.10/vt-data/
nasl/ to /var/lib/openvas/plugins
Releasing lock on /var/lib/openvas/feed-update.lock

tejasorke@tejasorke-VirtualBox:~/greenbone-community-container$ docker compose -
f $DOWNLOAD_DIR/docker-compose.yml \
    run --rm greenbone-feed-sync greenbone-feed-sync --type notus
Trying to acquire lock on /var/lib/openvas/feed-update.lock
Acquired lock on /var/lib/openvas/feed-update.lock
 Downloading Notus files from
rsync://feed.community.greenbone.net/community/vulnerability-feed/24.10/vt-data/
notus/ to /var/lib/notus
Releasing lock on /var/lib/openvas/feed-update.lock

tejasorke@tejasorke-VirtualBox:~/greenbone-community-container$
```

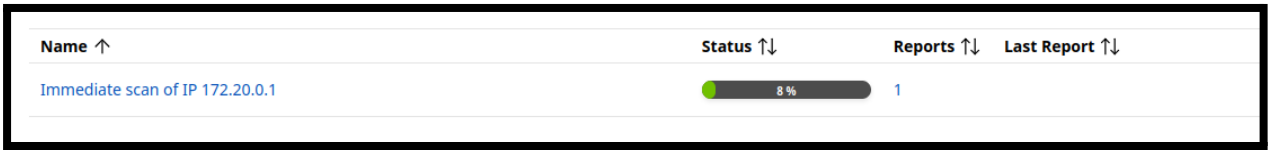


Name: Atharva Vasant Angre **Practical No. 8** **UCID: 2024510001**









Observation :

The Docker-based deployment of Greenbone Vulnerability Management (GVM) using the provided docker-compose.yml demonstrates a modular and efficient setup for proactive cybersecurity monitoring. Each component—such as vulnerability feeds, OpenVAS scanner, and Greenbone Security Assistant (GSA)—is containerized for better scalability and isolation. The configuration supports real-time vulnerability detection, feed synchronization, and detailed report generation through GSA's web interface. By using volume mapping and service dependencies, the system ensures data persistence and smooth inter-container communication. Overall, this setup provides a robust foundation for automated, continuous vulnerability assessment in a networked environment.