

OPENVAS ON CONTAINERIZED ENVIRONMENT/INSTRUCTIONS

JUST COPY AND PASTE EVERY STEP ONE BY ONE

This setup works for both WSL and VMS

Step 1:

1.1

```
sudo apt update
```

1.2

```
sudo apt install -y apt-transport-https ca-certificates curl software-properties-common  
docker.io docker-compose-v2
```

Step 2:

2.1

```
mkdir -p /home/$USER/gvm-docker
```

2.2

```
cd /home/$USER/gvm-docker
```

2.3

wget <https://raw.githubusercontent.com/NetizenCorp/GVM-Docker/main/docker-compose.yml>

Step 3:

3.1

```
nano docker-compose.yml
```

3.2

```
services:
```

```
  gvm:
```

```
    image: netizensoc/gvm-scanner:latest
```

```
    volumes:
```

```
      - gvm-data:/data          # DO NOT MODIFY
```

```
    environment:
```

```
      - USERNAME="admin"        #free to change
```

```
      - PASSWORD="admin"       #free to change
```

```
      - HTTPS=true             # DO NOT MODIFY
```

```
      - TZ="ETC"               # Change to your corresponding timezone
```

```
      - SSHD=true              # Mark true if using a Remote Scanner. Mark false if  
using a standalone operation. (just put true, who cares)
```

```
      - DB_PASSWORD="dbpassword"
```

```
    ports:
```

```
      - "443:9392" # Web interface
```

```
- "5432:5432" # Access PostgreSQL database from external tools
- "2222:22" # SSH for remote sensors. You can remove if you don't plan on
using remote scanners.

# - "9390:9390" # For GVM API Access. Leave commented if you do not plan on
using the API for external web application access.

restart: unless-stopped # Remove if your using for penetration testing or one-
time scans. Only use if using for production/continuous scanning

logging:
  driver: "json-file"
  options:
    max-size: "1k"
    max-file: "3"

volumes:
  gvm-data:
```

Step 4:

4.1

```
sudo docker compose up -d
```

DONE!!!!!!!!!!!!

GO TO: "*https://IP_ADDRESS*"

(You do not need to put the port)