

OpenVas - Cyber security scanner

Summary

OpenVas is a cyber security scanner, designed to perform penetration testing on internal and external systems. The documentation can be found at [immauss/openvas](https://immauss.github.io/openvas/).

Installation via docker-compose behind traefik proxy

Found 2 configurations, not sure which is the working one :/

```
openhav:  
  image: "immauss/openvas"  
  restart: always  
  labels:  
    - "traefik.enable=true"  
    - "traefik.http.routers.openvas.rule=Host(`openvas.domain.com`)"  
    - "traefik.http.routers.openvas.entrypoints=websecure"  
    - "traefik.http.routers.openvas.tls=true"  
    - "traefik.http.services.openvas.loadBalancer.server.port=9392"  
    - "traefik.docker.network=traefik"  
  networks:  
    - traefik  
  environment:  
    PASSWORD: "<PASSWORD>"
```

```
version: "2"  
services:  
  gvm:  
    image: securecompliance/gvm  
    volumes:  
      - /PATH/TO/FOLDER/openvas/gvm:/var/lib/gvm  
      - /PATH/TO/FOLDER/openvas/plugins:/var/lib/openvas/plugins  
    environment:  
      - USERNAME="USERNAME"
```

- PASSWORD="PASSWORD"

- AUTO_SYNC=true

- DB_PASSWORD="none"

ports:

- "9392:9392" # Web interface

restart: unless-stopped

version: "3"

services:

openvas:

ports:

- 8080:9392

environment:

- SKIPSYNC=true

volumes:

- /path/to/data:/data

image: immauss/openvas:22.4.32

Revision #3

Created 1 November 2021 19:20:31 by Andreas Greiner

Updated 17 January 2024 17:27:45 by Andreas Greiner