OpenVAS: установка

OpenVAS - опенсорсный сканер уязвимостей. Если вам необходимо регулярно проверять хосты и сервисы на уязвимости - стоит попробовать OpenVAS.

Ссылки:

- https://www.openvas.org/
- https://github.com/atomicorp/gvm
- https://github.com/atomicorp/openvas-docker

OpenVAS автоматически обновляет базы уязвимостей, запускает запланированные задачи, отправляет алерты и т.д.

Для установки есть свой репозиторий для rpm-based дистрибутивов (поддерживает Redhat 8, Rocky 8, Centos 8, Fedora 33, Fedora 34), но можно запустить OpenVAS в вашем любимом Docker:

```
docker run -d \
--name openvas \
-p 443:443 \
--restart=always \
atomicorp/openvas
```

Запустить с монтированием Volume:

```
docker volume create openvas

docker run -d \
--name openvas \
-v openvas:/var/lib/openvas/mgr
-p 443:443 \
--restart=always \
atomicorp/openvas
```

Подробнее о запуске в Docker можно почитать на страничке
https://github.com/atomicorp/openvas-docker

Открываем веб-интерфейс https://ваш-сервер логин и пароль по умолчанию: admin / admin

Минимальная настройка:

- Настраиваем способ доступа к вашим системам в Configuration → Credential
- Добавляем хосты в Configuration → Targets
- Расписание проверок в Configuration → Schedules
- Добавляем задачи для проверок в Scan → Tasks

После выполнения задач можно посмотреть отчёты в меню Scan → Reports/Results

openvas, security, scanner, сканнер уязвимостей