

A close-up, high-contrast photograph of a person's face, partially obscured by shadows. The person is wearing a dark hoodie with a visible zipper and drawstring. The lighting is dramatic, highlighting the contours of the face and the texture of the clothing.

РУКОВОДСТВО ХАЦКЕРА

ЧАСТЬ 1
СКАНЕР AWS

@HASKAR

Вступление.

Приветствую тебя читатель! В этой части я расскажу про AWVS - Acunetix Web Vulnerability Scanner. Источником и вдохновением стала группа GreyTeam. Она существует в ВК и ссылочку на неё оставляю в конце нашего приключения :)

Ну... что-ж приступим!

Acunetix – это не просто сканер веб-уязвимостей.

При развертывании в среде docker, всего одним человеком с одним компьютером, это комплексное решение для тестирования безопасности веб-приложений может быть использовано как автономный инструмент сканирования для выполнения сложной задачи сканирования.

В этом рассказе показано, как искать, установить AWVS docker с помощью командной строки, а также как изменить учетные данные по умолчанию.

Ну... что-ж перелистывай страницу :)

Примечание: Информация для исследования, обучения или проведения аудита. Применение в корыстных целях карается законодательством РФ.

Поиск образа AWVS docker

Ого ты уже тут? Молодец!

Самый простой способ узнать, какой образ AWVS вам следует использовать, – это поиск и использование того образа, который имеет наибольшее количество звезд.

Команда: **sudo docker search awvs**

```
sudo -i
~# docker search awvs
NAME                                DESCRIPTION                                STARS
OFFICIAL    AUTOMATED
secfa/docker-awvs                    AWS 14.4.210816098 Linux Version Crack By ... 53
leishianquan/awvs-nessus            21
xrsec/awvs                          Aws 14 Scanner、fahai                      5
lazj/awvs13                          1
tiancizzz/awvs                      一款知名的网络漏洞扫描工具                1
k3rwin/awvs13                        0
hangezhao/awvs                      0
xxlm/awvs13cn                       0
smarttang/awvs_2019_07              0
xfantasy/awvs                       0
110110/awvs13                      0
zeyanlin/awvs                       0
jstang/awvs                         配置了API密钥的容器镜像                    0
littlehoury/awvs                    A wonderful virtual sleep                  0
meterpreter/awvs                    0
yakoazz/awvsnessus                  0
saline/awvsengine                   0
evil0x0/awvs                        0
sigle0724/awvs                      0
xschur666/awvs                      0
nienie/awvs13                       0
yimingy72/awvs14                    0
cure0jvs/awvs-engine                0
ganl/awvs                           0
srsecmmm/awvs13                     分布式部署                                0
```

secfa/docker-awvs имеет больше всего звезд, чем другие образы.
Docker hub: **<https://hub.docker.com/r/secfa/docker-awvs>**

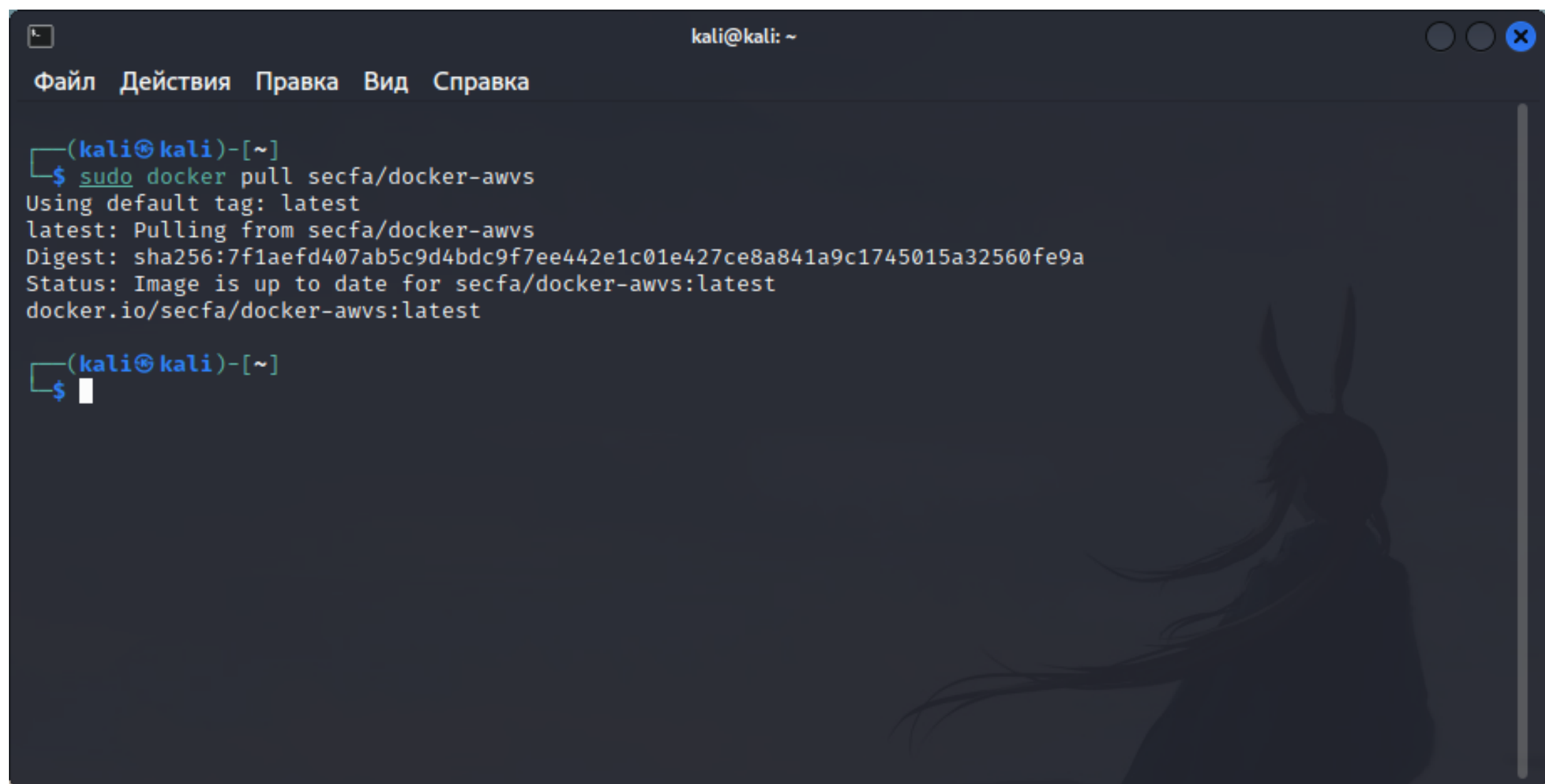
Дорогой читатель теперь, тебе на следующую страницу :)

Создание контейнера AWVS

Молодец , теперь приступим к установке!

Из командной строки:

sudo docker pull secfa/docker-awvs

A screenshot of a terminal window titled 'kali@kali: ~'. The window has a menu bar with 'Файл', 'Действия', 'Правка', 'Вид', and 'Справка'. The terminal shows the command 'sudo docker pull secfa/docker-awvs' being executed. The output indicates that the image is up to date. The terminal background features a faint, stylized illustration of a person with long hair and a hood, possibly a hacker or a character from a game.

```
(kali@kali)-[~]
$ sudo docker pull secfa/docker-awvs
Using default tag: latest
latest: Pulling from secfa/docker-awvs
Digest: sha256:7f1aefd407ab5c9d4bdc9f7ee442e1c01e427ce8a841a9c1745015a32560fe9a
Status: Image is up to date for secfa/docker-awvs:latest
docker.io/secfa/docker-awvs:latest

(kali@kali)-[~]
$
```

Как пройдет установка нашего docker-a.

После чего можно уже запустить docker командой:

sudo docker run -it -d -p 3443:3443 secfa/docker-awvs

Я использую порт 3443 для привязки порта 3443 в docker.

Если у вас нету docker, то его следует установить!

Команда для Kali Linux: sudo apt install docker.io

Теперь дорогой друг перейдем на следующую страницу ^_^

Заходим в Web Gui

Когда AWVS будет запущен, зайдите на сайт **https://YOUR_Public_IP:3443/**.

Где-же найти YOUR_Public_IP ? Все очень просто пропишите команду в терминал: **ifconfig**

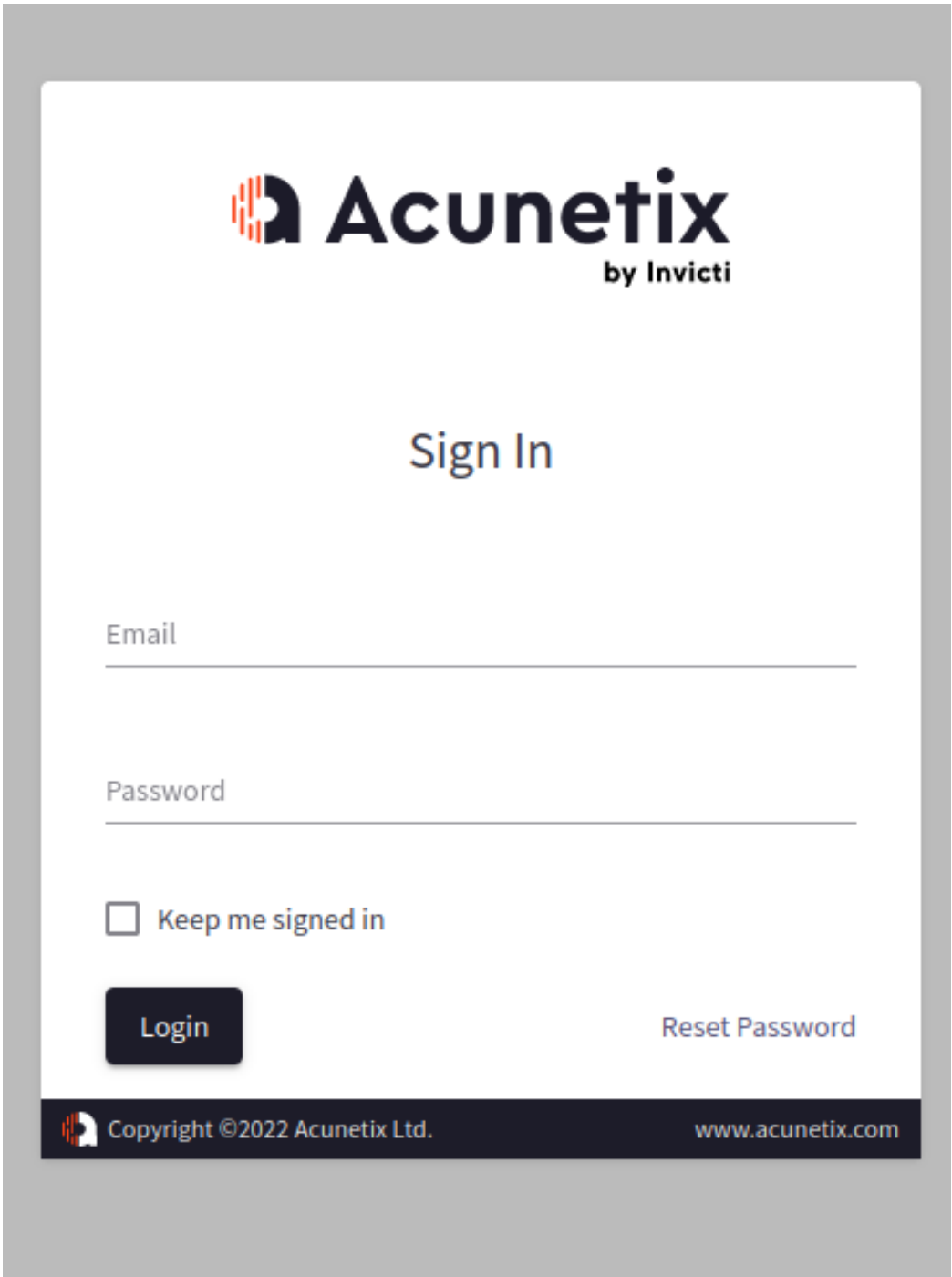
После чего найдите строку docker, например docker0, а там уже инайдите строку **inet**, там и будет тот самый YOUR_Public_IP.

**Внимание! Соединение происходит через https://
Если будет http://, соединения не будет!**

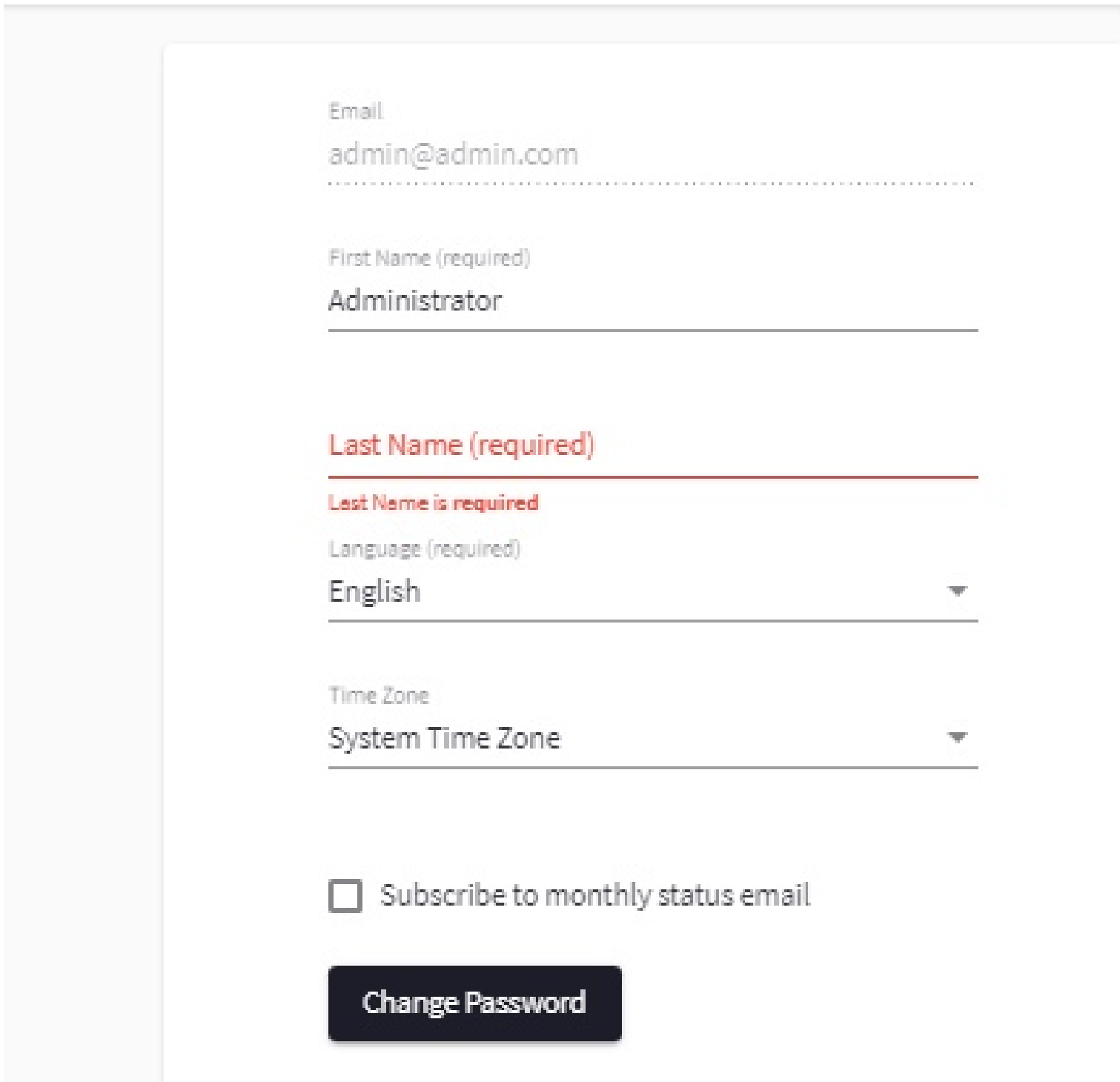
Зайдя на страницу, нас встретит окно авторизации, стандартный логин и пароль такие:

Логин: admin@admin.com

Пароль: Admin123



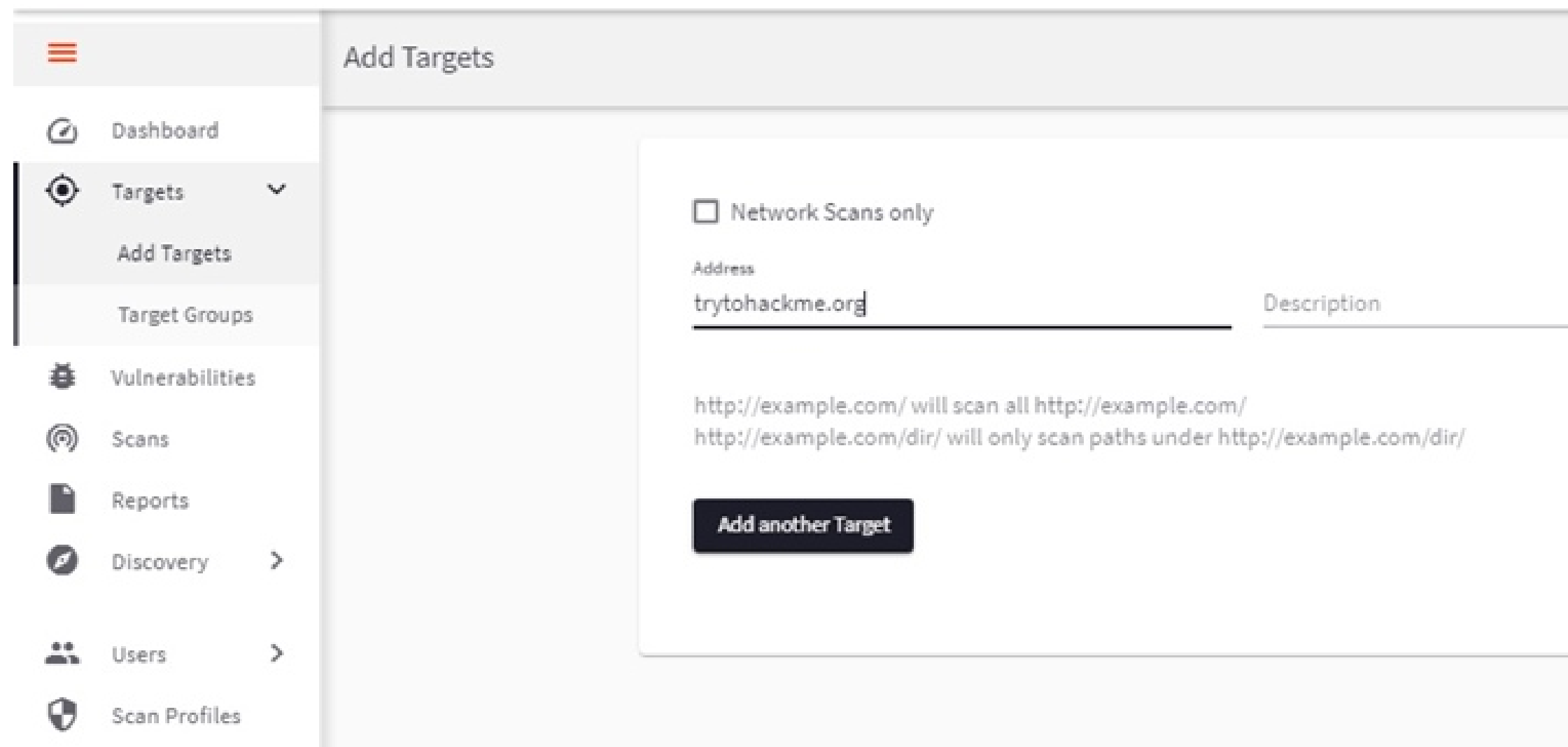
Вы можете изменить пароль после входа в систему в профиле.



Как изменить электронную почту / имя пользователя из командной строки:

```
docker ps                ac647bcba732
docker exec -it id /bin/bash ac647bcba732
cd /home/acunetix/.acunetix
./change_credentials.sh
```

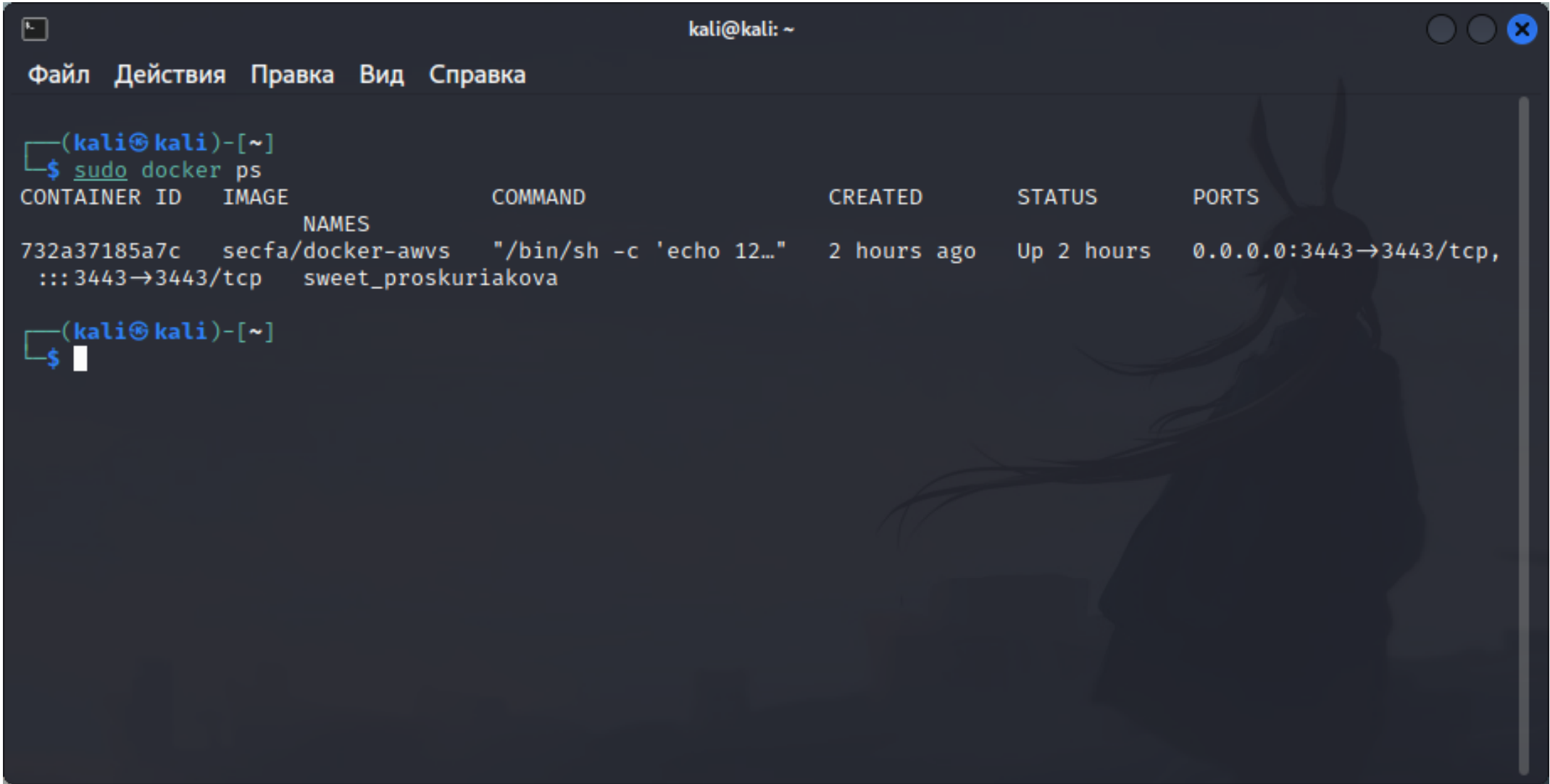
Добавим целевой хост.



Далее переходим в Scans -> New Scan

Как остановить docker.

Для начало пропишем команду: sudo docker ps



Видим **CONTAINER ID** это id контейнера, копируем его.
После чего для того чтобы остановить docker пропишем команду:
sudo docker stop CONTAINER ID

У меня получилось так: sudo docker stop 732a37185a7c
После чего docker завершит свою работу.

Вот и всё !
Спасибо дорогой читатель, что был со мной ^_^

Источники.

1.Статья от GreyTeam:

<https://vk.com/@greyteam-awvs-acunetix-web-vulnerability-scanner-ustanovka-docker>

2.Мой ютуб канал Хаскарь:

<https://www.youtube.com/channel/UCVrl2OQJrimaaRQV8oIYi1w>