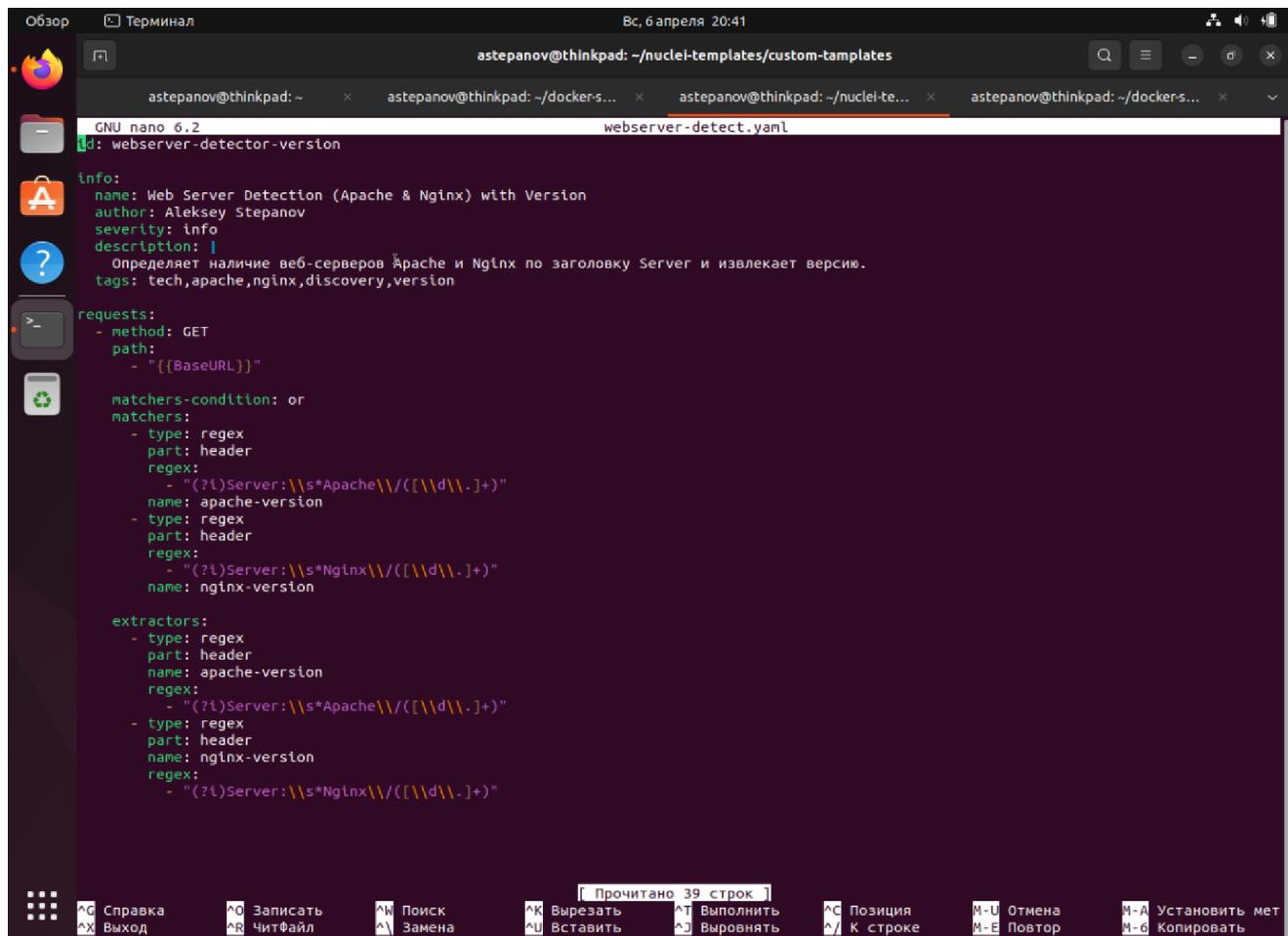


Модуль 3. Сканирование приложений на уязвимости (vo_HW)

Задание № 3.2. Детектирование заголовков с помощью Nuclei

Шаблон nuclei для детектирования серверов Apache и Nginx и их версий:



```
astepanov@thinkpad: ~$ nano webserver-detect.yaml
info:
  name: Web Server Detection (Apache & Nginx) with Version
  author: Aleksey Stepanov
  severity: info
  description: |
    Определяет наличие веб-серверов Apache и Nginx по заголовку Server и извлекает версию.
  tags: tech,apache,nginx,discovery,version

requests:
- method: GET
  path:
    - "[{BaseUrl}]"

matchers-condition: or
matchers:
- type: regex
  part: header
  regex:
    - "(?i)Server:\s*Apache\/\/([\\d\\.]+)"
      name: apache-version
  - "(?i)Server:\s*Nginx\/\/([\\d\\.]+)"
      name: nginx-version

extractors:
- type: regex
  part: header
  name: apache-version
  regex:
    - "(?i)Server:\s*Apache\/\/([\\d\\.]+)"
- type: regex
  part: header
  name: nginx-version
  regex:
    - "(?i)Server:\s*Nginx\/\/([\\d\\.]+)"
```

Описание работы шаблона:

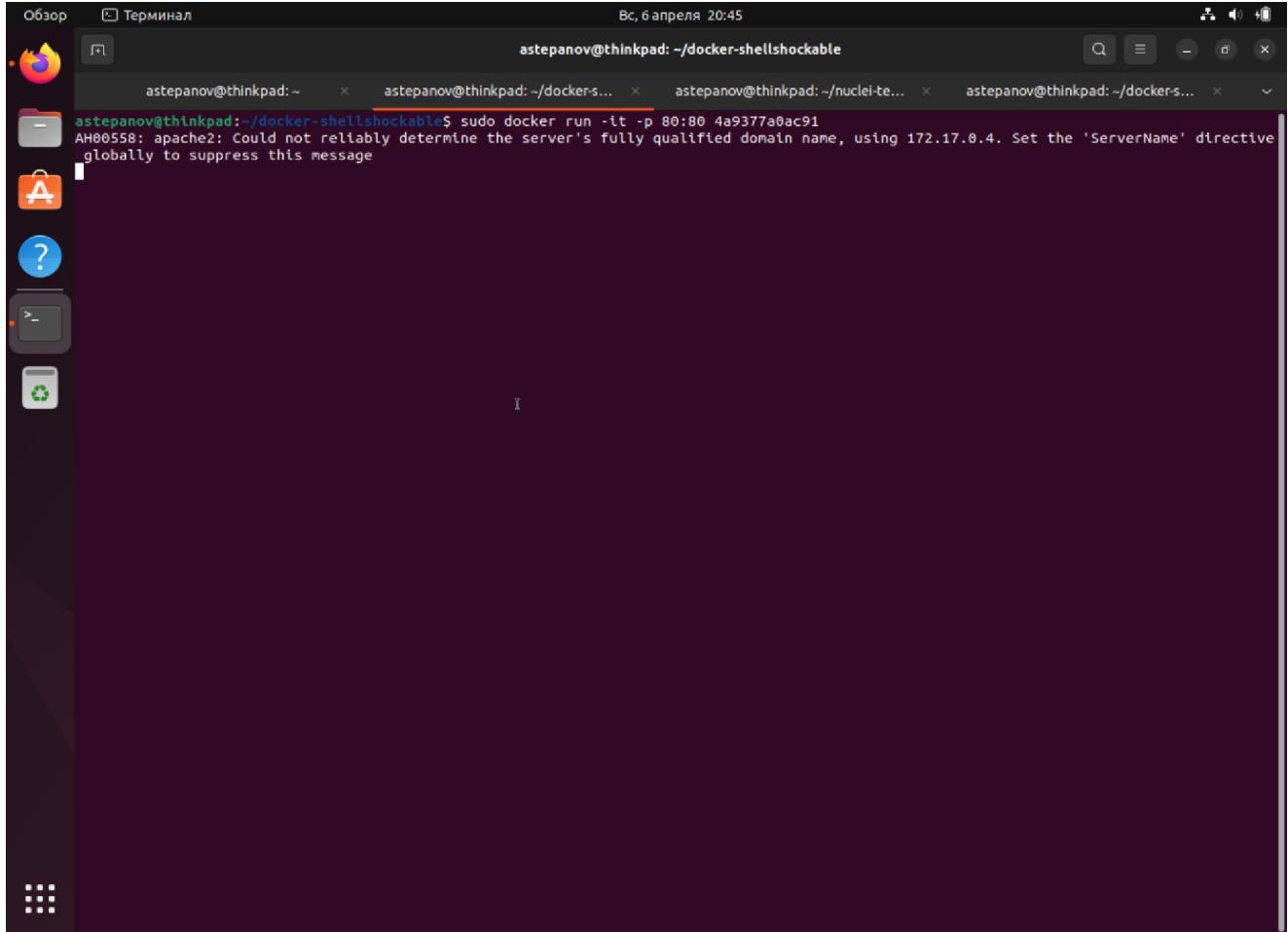
Шаблон для Nuclei, предназначенный для детектирования версий веб-серверов Apache и Nginx, отправляет HTTP-запрос на целевой сервер и анализирует его ответ, обращая внимание на заголовок "Server". В зависимости от содержимого этого заголовка, шаблон проверяет, является ли сервер Apache или Nginx, а также извлекает информацию о версии сервера. Регулярные выражения ищут строки, которые содержат информацию о версии сервера, например, "Apache/2.4.41" или "Nginx/1.18.0". Если в заголовке присутствуют такие данные, шаблон извлекает номер версии веб-сервера и помечает его как результат. Шаблон использует два регулярных выражения для каждой из платформ — для Apache и для Nginx. Это позволяет детектировать как сам сервер, так и его версию, предоставляя информацию о целевом сервере в случае успешного нахождения совпадений.

Примеры запуска и демонстрация

Проверка на сервере Apache.

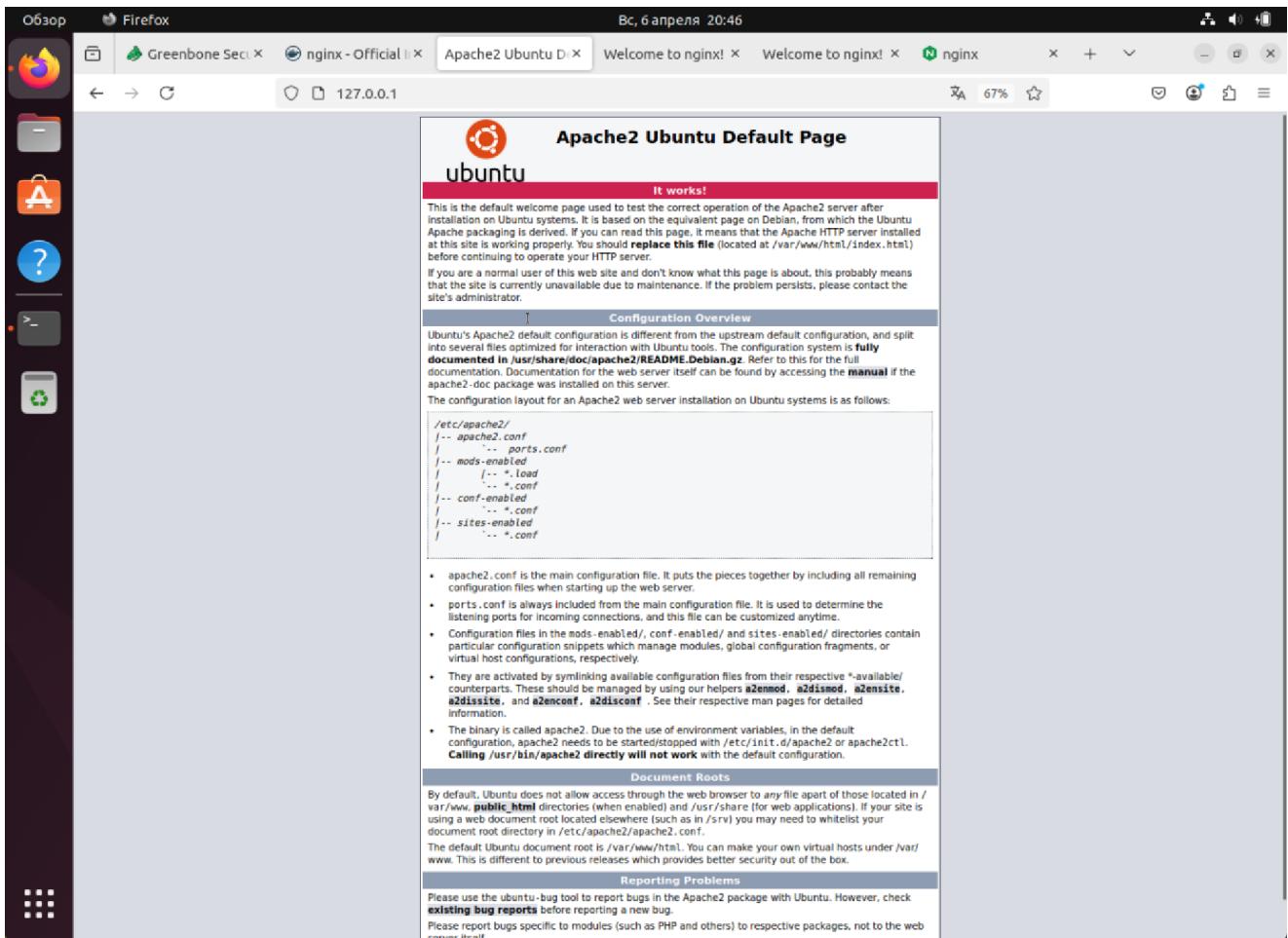
Для проверки на сервере Apache используем ранее установленный в docker-е уязвимы Apache-сервер из репозитория [Zenithar/docker-shellshockable](#). Для данных целей он вполне подойдет.

Запускаем докер контейнер с apache-сервером и прокидываем его на 80-ый стандартный http порт



The screenshot shows a Linux desktop environment with a terminal window open. The terminal window title is "Терминал" and the date and time are "Вс, 6 апреля 20:45". The terminal content shows the command: `astepanov@thinkpad:~/dockershellshockable$ sudo docker run -it -p 80:80 4a9377a0ac91`. Below it, an Apache2 error message is displayed: `AH00558: apache2: Could not reliably determine the server's fully qualified domain name, using 172.17.0.4. Set the 'ServerName' directive globally to suppress this message`.

Видим что сервер работает на стандартном http-порте на localhost'e



Проверяем как будет задетекирован наш веб сервер с помощью нашего nuclei-шаблона:

```
astepanov@thinkpad:~/nuclei-templates/custom-templates$ nuclei -u http://127.0.0.1 -t webserver-detect.yaml
[WRN] Found 1 templates loaded with deprecated protocol syntax, update before v3 for continued support.
[LIN] Current nuclei version: v3.4.1 (latest)
[LIN] Current nuclei-templates version: v10.1.6 (latest)
[WRN] Scan results upload to cloud is disabled.
[LIN] New templates added in latest release: 78
[LIN] Templates loaded for current scan: 1
[WRN] Loading 1 unsigned templates for scan. Use with caution.
[LIN] Targets loaded for current scan: 1
[webserver-detector-version:apache-version] [http] [info] http://127.0.0.1 ["Server: Apache/2.4.7"]
astepanov@thinkpad:~/nuclei-templates/custom-templates$
```

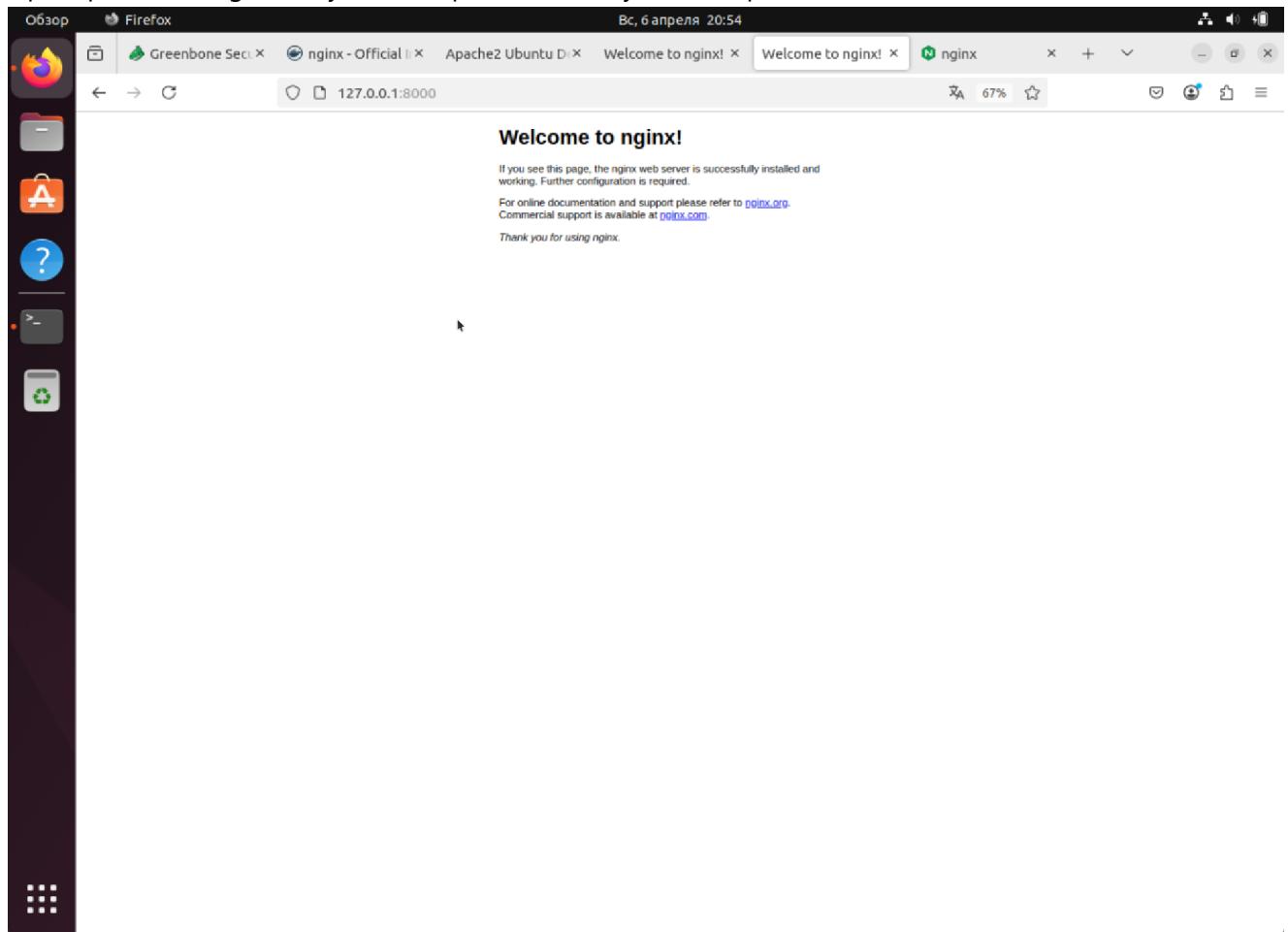
Видим, что nuclei успешно определил веб-сервер apache, в.т.ч его версию

Проверка на сервере Nginx.

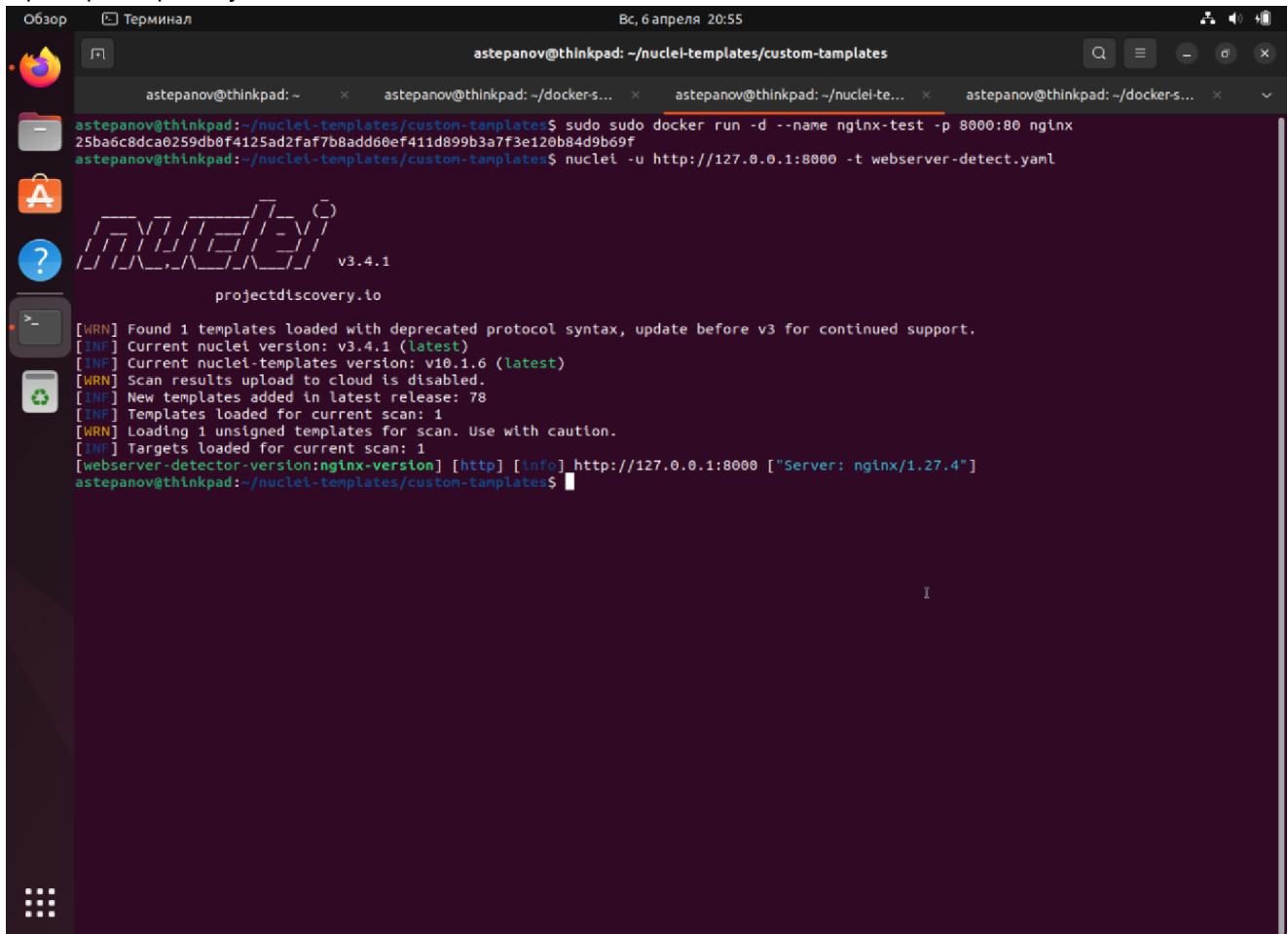
Для проверки детектирования сервера nginx, запустим сервер nginx прямо из docker-образа, прокинув его на произвольный 8000-ый порт:

```
astepanov@thinkpad: ~      astepanov@thinkpad: ~/dockers...      astepanov@thinkpad: ~/nuclei-te...      astepanov@thinkpad: ~/d
astepanov@thinkpad:~/nuclei-templates/custom-templates$ sudo docker run -d --name nginx-test -p 8000:80 nginx
25ba6c8dca0259db0f4125ad2faf7b8add60ef411d899b3a7f3e120b84d9b69f
astepanov@thinkpad:~/nuclei-templates/custom-templates$
```

Проверяем, что nginx запустился и работает на нужном порте:



Проверяем работу nuclei-шаблона на нашем хосте:



```
astepanov@thinkpad:~/nuclei-templates/custom-templates$ sudo docker run -d --name nginx-test -p 8000:80 nginx
astepanov@thinkpad:~/nuclei-templates/custom-templates$ nuclei -u http://127.0.0.1:8000 -t webserver-detect.yaml
v3.4.1
projectdiscovery.io

[WRN] Found 1 templates loaded with deprecated protocol syntax, update before v3 for continued support.
[INF] Current nuclei version: v3.4.1 (latest)
[INF] Current nuclei-templates version: v10.1.6 (latest)
[WRN] Scan results upload to cloud is disabled.
[INF] New templates added in latest release: 78
[INF] Templates loaded for current scan: 1
[WRN] Loading 1 unsigned templates for scan. Use with caution.
[INF] Targets loaded for current scan: 1
[webserver-detector-version:nginx-version] [http] [info] http://127.0.0.1:8000 ["Server: nginx/1.27.4"]
astepanov@thinkpad:~/nuclei-templates/custom-templates$
```

Видим, что nuclei так же успешно определил веб-сервер nginx и его версию!