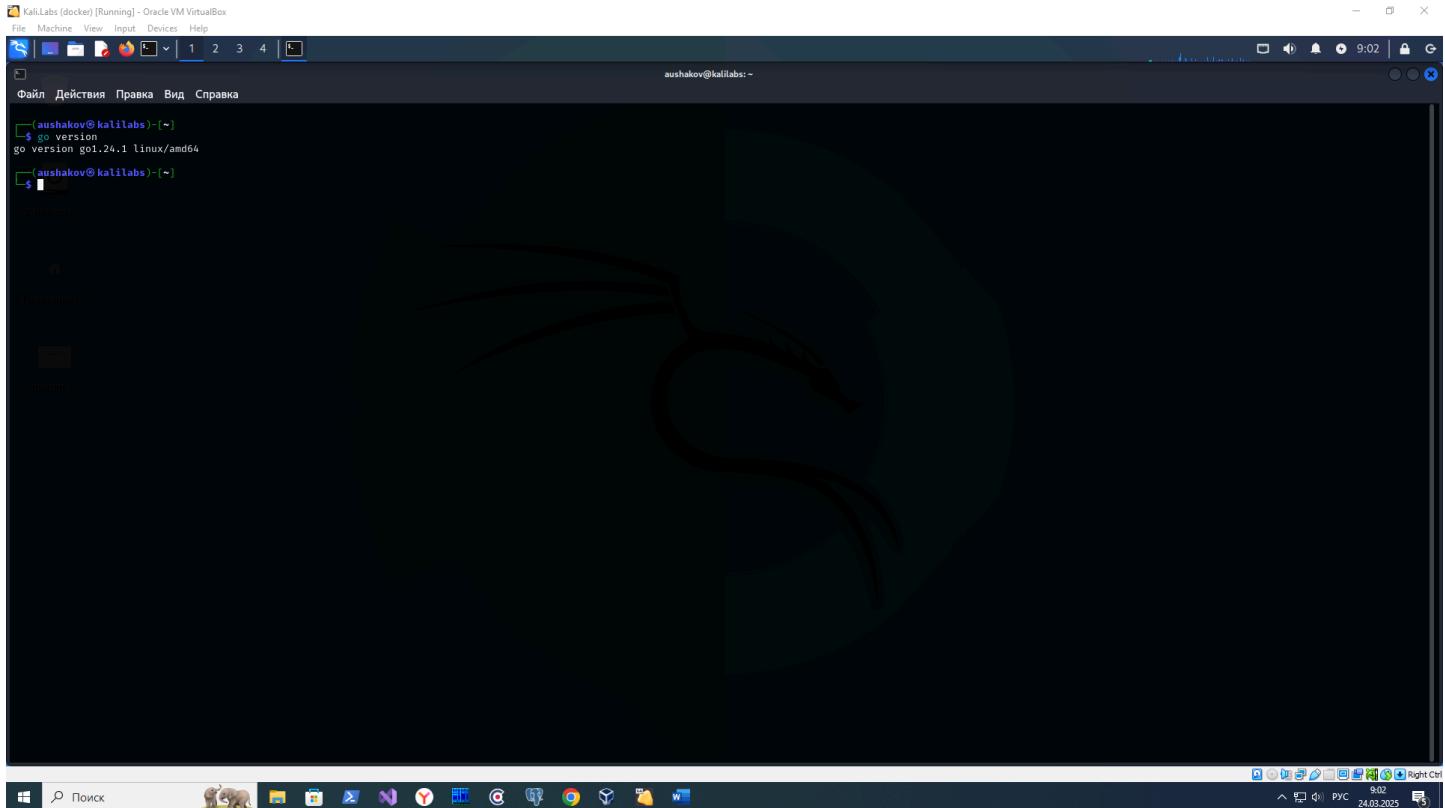


Создаю виртуальную машину на Kali Linux

A screenshot of a KaliLabs docker instance within an Oracle VM VirtualBox environment. The desktop has a dark, minimalist theme. At the top, there's a standard Windows-style menu bar with 'File', 'Machine', 'View', 'Input', 'Devices', and 'Help'. The system tray shows the date as '8:56' and the day as 'Monday, 2021-03-15'. The main workspace features a large, semi-transparent watermark of a hand holding a steering wheel. In the top-left corner, a terminal window is open with a dark background and light-colored text, displaying the command '\$ whoami' followed by the output 'ushakov'. Below the terminal, there's a small text input field with a cursor. The desktop also includes a dock at the bottom with icons for a search bar, file manager, terminal, and other system utilities.

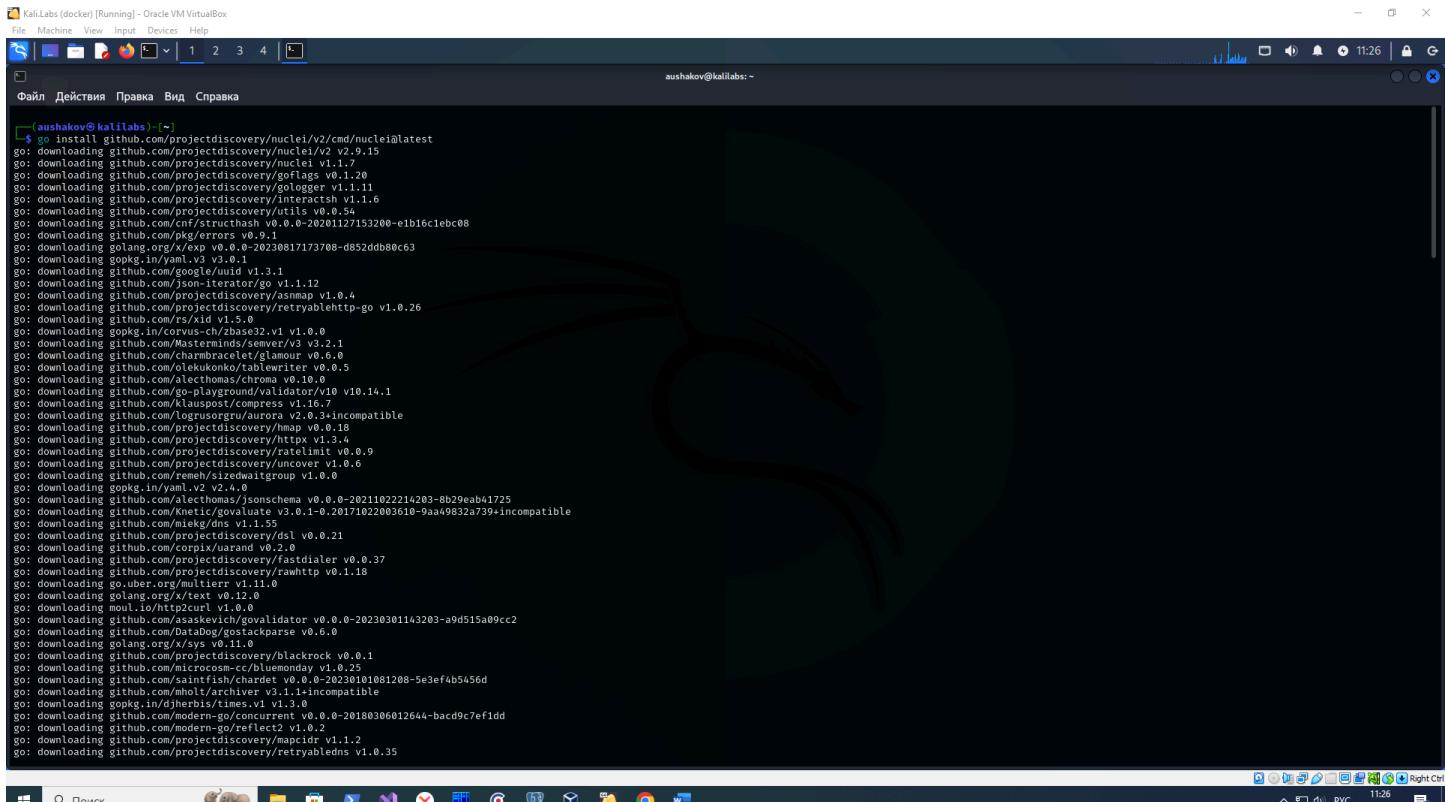
Устанавливаю golang для работы с Nuclei

Проверяю версию qolang



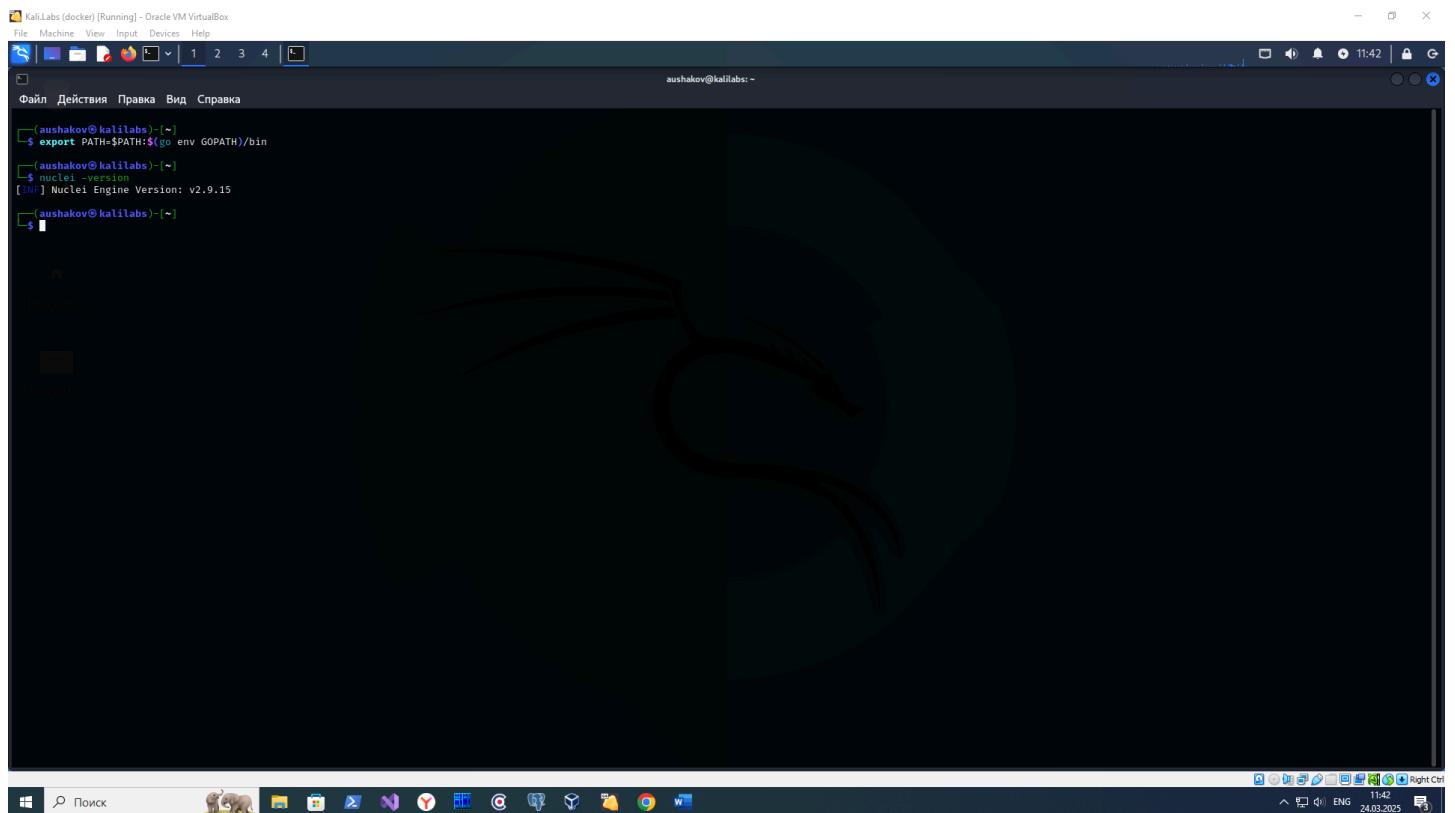
```
aushakov@kalilabs: ~
$ go version
go version go1.24.1 linux/amd64
```

Устанавливаю Nuclei



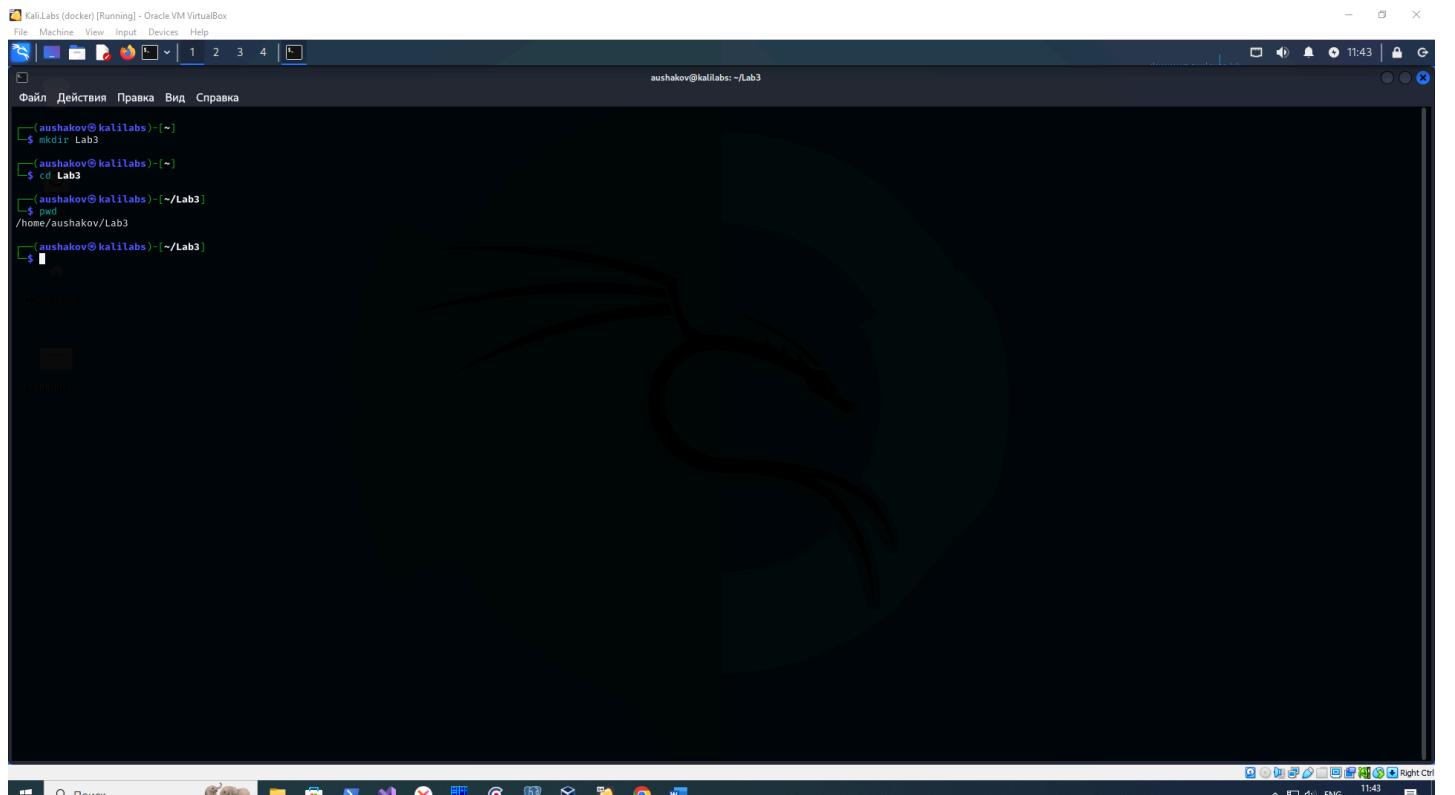
```
aushakov@kalilabs: ~
$ go install github.com/projectdiscovery/nuclei/v2/cmd/nuclei@latest
go: downloading github.com/projectdiscovery/nuclei/v2 v2.9.15
go: downloading github.com/projectdiscovery/nuclei v1.1.7
go: downloading github.com/projectdiscovery/goflags v0.1.20
go: downloading github.com/projectdiscovery/gologger v1.1.11
go: downloading github.com/projectdiscovery/interactsh v1.1.6
go: downloading github.com/projectdiscovery/utils v0.0.54
go: downloading github.com/cnfs/structhash v0.0.20201127153200-e1b16c1ebc08
go: downloading github.com/pkg/errors v0.0.1
go: downloading golang.org/x/exp v0.0.0-20230817173700-d852ddb80e63
go: downloading goopkg.in/yaml.v3 v3.0.1
go: downloading github.com/google/uuid v1.3.1
go: downloading github.com/json-iterator/go v1.1.12
go: downloading github.com/projectdiscovery/retryablehttp-go v1.0.26
go: downloading github.com/rs/xid v1.5.0
go: downloading goopkg.in/corus-ch/zbase32.v1 v1.0.0
go: downloading github.com/Masterminds/server/v3 v3.2.1
go: downloading github.com/charmbracelet/glamour v0.6.0
go: downloading github.com/olekukonko/tui v0.10.0.5
go: downloading github.com/alethomas/chroma v0.10.0
go: downloading github.com/go-playground/validator/v10 v10.14.1
go: downloading github.com/kluspost/compress v1.16.7
go: downloading github.com/legruszgru/aurora v2.0.3+incompatible
go: downloading github.com/projectdiscovery/hmap v0.0.18
go: downloading github.com/projectdiscovery/httpx v1.3.4
go: downloading github.com/projectdiscovery/ratelimit v0.0.9
go: downloading github.com/projectdiscovery/uncover v1.0.6
go: downloading github.com/remeh/sizedxmlgroup v1.0.0
go: downloading goopkg.in/yaml.v2 v2.4.0
go: downloading goopkg.in/alethomas/jonschema v0.0.0-20211022214203-8b29eab41725
go: downloading github.com/knetic/govulntr v3.0.1-0.2017102003610-9aa49832a739+incompatible
go: downloading github.com/miekg/dns v1.1.55
go: downloading github.com/projectdiscovery/cvecheck v0.0.21
go: downloading github.com/containernetworking/del v0.0.20
go: downloading github.com/projectdiscovery/fastdialer v0.0.37
go: downloading github.com/projectdiscovery/rawhttp v0.1.18
go: downloading go.uber.org/multier v1.11.0
go: downloading golang.org/x/text v0.12.0
go: downloading moul.io/http2curl v1.0.0
go: downloading goopkg.in/alethomas/jonschema v0.0.0-2020301143203-a9d515a09cc2
go: downloading github.com/saskevicius/govulntr v0.0.0-2020301143203-a9d515a09cc2
go: downloading github.com/projectdiscovery/gopathparse v0.6.0
go: downloading golang.org/x/sys v0.11.0
go: downloading github.com/projectdiscovery/blackrock v0.0.1
go: downloading github.com/microcosm-cc/bluemonday v1.0.25
go: downloading github.com/saintfish/charset v0.0.0-20230101081208-5e3ef4b5456d
go: downloading github.com/mholt/archiver v3.1.1+incompatible
go: downloading github.com/olekukonko/tui/v1 v1.0.0.5
go: downloading github.com/modern-go/concurrent v0.0.0-20180306012644-bacd9c7ef1dd
go: downloading github.com/modern-go/reflect2 v1.0.2
go: downloading github.com/projectdiscovery/mapiaddr v1.1.2
go: downloading github.com/projectdiscovery/retryabledns v1.0.35
```

Проверяю версию Nuclei



Kali.Labs (docker) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Файл Действия Правка Вид Справка
ausshakov@kalilabs: ~
ausshakov@kalilabs: ~\$ export PATH=\$PATH:\$go env GOPATH)/bin
ausshakov@kalilabs: ~\$ nuclei --version
[INFO] Nuclei Engine Version: v2.9.15
ausshakov@kalilabs: ~\$

Создаю директорию для моих шаблонов Nuclei



Kali.Labs (docker) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Файл Действия Правка Вид Справка
ausshakov@kalilabs: ~\$ mkdir Lab3
ausshakov@kalilabs: ~\$ cd Lab3
ausshakov@kalilabs: ~/Lab3\$ pwd
/home/ausshakov/Lab3
ausshakov@kalilabs: ~/Lab3\$

Создаю файл для шаблона Nuclei для детектирования типа веб-сервера (сам шаблон приложен отдельным файлом)

```
(aushakov㉿kalilabs) [~/Lab3]
$ touch server-detect.yml
(aushakov㉿kalilabs) [~/Lab3]
$ ls -la
итого 8
drwxrwxr-x 2 aushakov aushakov 4096 мар 24 23:27 .
drwxrwxr-x 19 aushakov aushakov 4096 мар 24 23:24 ..
-rw-rw-r-- 1 aushakov aushakov 0 мар 24 23:27 server-detect.yml
(aushakov㉿kalilabs) [~/Lab3]
```

```
GNU nano 8.3
server-detect.yml *
id: lab3-server-detect
info:
  name: Lab3 Apache & Nginx server detector
  author: me
  severity: info
  description: Lab3 Apache & Nginx server detector
requests:
- method: GET
  path:
    - {{BaseUrl}}
  headers:
    User-Agent: "Nuclei: Apache & Nginx server detector"
  matchers:
    - type: word
      words:
        - "Server: Apache"
        - "Server: nginx"
      part: header
```



Описание шаблона:

Этот шаблон Nuclei предназначен для обнаружения веб-серверов Apache и Nginx, основываясь на заголовке Server в HTTP-ответе. Шаблон отправляет GET-запрос к целевому хосту и проверяет заголовок ответа. Если в заголовке Server присутствует строка Apache или nginx, то шаблон определяет, что соответствующий веб-сервер был найден.

В качестве сервера, который я буду проверять с помощью моего шаблона Nuclei, я возьму образ `jacopen/cve-2014-6271-apache-debian` для создания docker контейнера, который я использовал в прошлых лабораторных (я знаю, что в нем используется Apache в качестве веб-сервера).

The screenshot shows the Docker Hub interface. At the top, there's a banner with the text "Introducing our new CEO Don Johnson - Read More →". Below it, the "dockerhub" logo is on the left, and a search bar with the placeholder "Search Docker Hub" is on the right. A navigation bar includes links for "Explore", "Sign In", and "Sign up". The main content area displays the repository "jacopen/cve-2014-6271-apache-debian" by "jacopen". It shows a small icon of a cube, a star rating of 0, and 10 forks. Below this, there are tabs for "Overview" (which is selected) and "Tags". The "Overview" section contains a message stating "No overview available" and "This repository doesn't have an overview". To the right, a "Docker Pull Command" box contains the command "docker pull jacopen/cve-2014-6271-apache-debian" with a "Copy" button.

The screenshot shows a terminal window titled "KaliLabs (docker) [Running] - Oracle VM VirtualBox". The window title bar includes icons for File, Machine, View, Input, Devices, Help, and a search bar. The status bar at the bottom shows "aushakov@kallabs: ~/CVE-2014-6271" and the date/time "23.03.2025 21:17". The terminal itself displays the following Dockerfile content:

```
FROM jacopen/cve-2014-6271-apache-debian:buster
RUN echo "ServerName localhost" >> /etc/apache2/apache2.conf
```

The terminal has a dark background with white text. The bottom of the window features a toolbar with various icons for file operations like "Справка" (Help), "Записать" (Save), "Чтение" (Read), "Вырезать" (Cut), "Выровнять" (Align), "Позиция" (Position), "Отмена" (Undo), "Установите метку" (Set marker), "На скобку" (To brace), "Повтор" (Redo), "Копировать" (Copy), "Обр. поиск" (Search backward), "Предыдущий" (Previous), "Следующий" (Next), "Назад" (Back), "Вперед" (Forward), "ПредСлово" (Previous page), "СледСлово" (Next page), and "Начало" (Start).

Запускаю сборку образа моего контейнера docker

```
aushakov@kali:~/[~]~/CVE-2014-6271$ sudo docker build -t shellshock .
[+] Building 20.0s (6/6) FINISHED
   --> [internal] load build context
   --> transferring dockerfile: 147B
   --> [internal] load metadata for docker.io/jacopen/cve-2014-6271-apache-debian:buster
   --> [internal] load .dockerignore
   --> transferring context: 2B
   --> FROM docker.io/jacopen/cve-2014-6271-apache-debian:buster@a25643577482c8a140aef04e9213508eb09a1918fa8a4089d67e3331af6679dd5
   --> RUN curl -L https://raw.githubusercontent.com/jacopen/cve-2014-6271-apache-debian/master/Dockerfile > /etc/docker/Dockerfile
   --> sha256:43577a02c8a140aef04e9213508eb09a1918fa8a4089d67e3331af6679dd5
   --> sha256:1dd5a6a2e6d15110b19269792e2080621708a3b556623a612e3a1fbaef1f44 2.67kB / 2.57kB
   --> sha256:a970f51a5eaa86e137ca7a7612407b53ebab97f7374ad15a6e2c052c682b500 50.5MB / 50.5MB
   --> sha256:1d93bebfbc74ccf6a9931de699e9915c71fcce01ad46e3f0e0c23c3d574db90000 41.93MB / 41.93MB
   --> sha256:c80795a6a03e35cbc01a6608789d204cadad98851368200428988dd109 3.12MB / 3.12MB
   --> sha256:67d220874fe98cc05a72d01969363505a3050a13a3e89c61aefb984833edea 228B / 228B
   --> sha256:136972061a32bd7232080640a3a5c12067c7230715041d0d088833e000 395B / 395B
   --> sha256:a970f51a5eaa86e137ca7a7612407b53ebab97f73fd4df15a642d52c662b500
   --> extracting sha256:a970f51a5eaa86e137ca7a7612407b53ebab97f73fd4df15a642d52c662b500
   --> extracting sha256:c80795a6a03e35beed14668789d2b4ac8ade958051368200428988dd109
   --> extracting sha256:67d220874fe98ccf5a72d01969363509a3050a13a3e89c61aefb984833edea
   --> extracting sha256:0f0474d02b0b96c36fd8e0d8f51a7d027a09a78f9f5a41ad08345a3585c04
   --> sha256:136972061a32bd7232080640a3a5c12067c7230715041d0d088833e000
   --> [2/2] RUN echo "ServerName localhost" >> /etc/apache2/apache2.conf
   --> exporting to image
   --> exporting layers
   --> writing image sha256:a20e529a998eea4b1431477b7604f3dda3cd8c57af9e6df41eb7f36330ee9ea
   --> naming to docker.io/library/shellshock
aushakov@kali:~/[~]~/CVE-2014-6271$
```

Запускаю созданный контейнер docker (с учетом необходимости проброса портов)

```
aushakov@kali:~/[~]~/CVE-2014-6271$ sudo docker run -rm -p 8080:80 shellshock
aushakov@kali:~/[~]~/CVE-2014-6271$
```

```
aushakov@kalilabs: ~/CVE-2014-6271$ sudo docker ps
[sudo] пароль для aushakov:
CONTAINER ID        IMAGE               COMMAND             CREATED            STATUS              PORTS
163071f409fb        shellshock          "/usr/sbin/apache2ctz"   45 seconds ago    Up 44 seconds      0.0.0.0:8080->80/tcp, :::8080->80/tcp
   gallant_hermann
```

Запускаю выполнение Nuclei только на моем созданном шаблоне

```
aushakov@kalilabs: ~/Lab3$ nuclei -t ./server-detect.yaml -u http://localhost:8080
v2.9.15
projectdiscovery.io

[WRN] Found 1 templates loaded with deprecated protocol syntax, update before v3 for continued support.
[INF] Current nuclei version: v2.9.15 (outdated)
[INF] Current nuclei-templates version: v10.1.5 (latest)
[INF] New templates added in latest release: 281
[INF] Templates loaded for current scan: 1
[INF] Targets loaded for current scan: 1
[Lab3-Server-Detect] [https] [info] http://localhost:8080
aushakov@kalilabs: ~/Lab3$
```

Видно, что Nuclei определил, что на испытуемом веб-сервере используется Apache с помощью моего созданного шаблона. Это означает, что шаблон создан корректно.