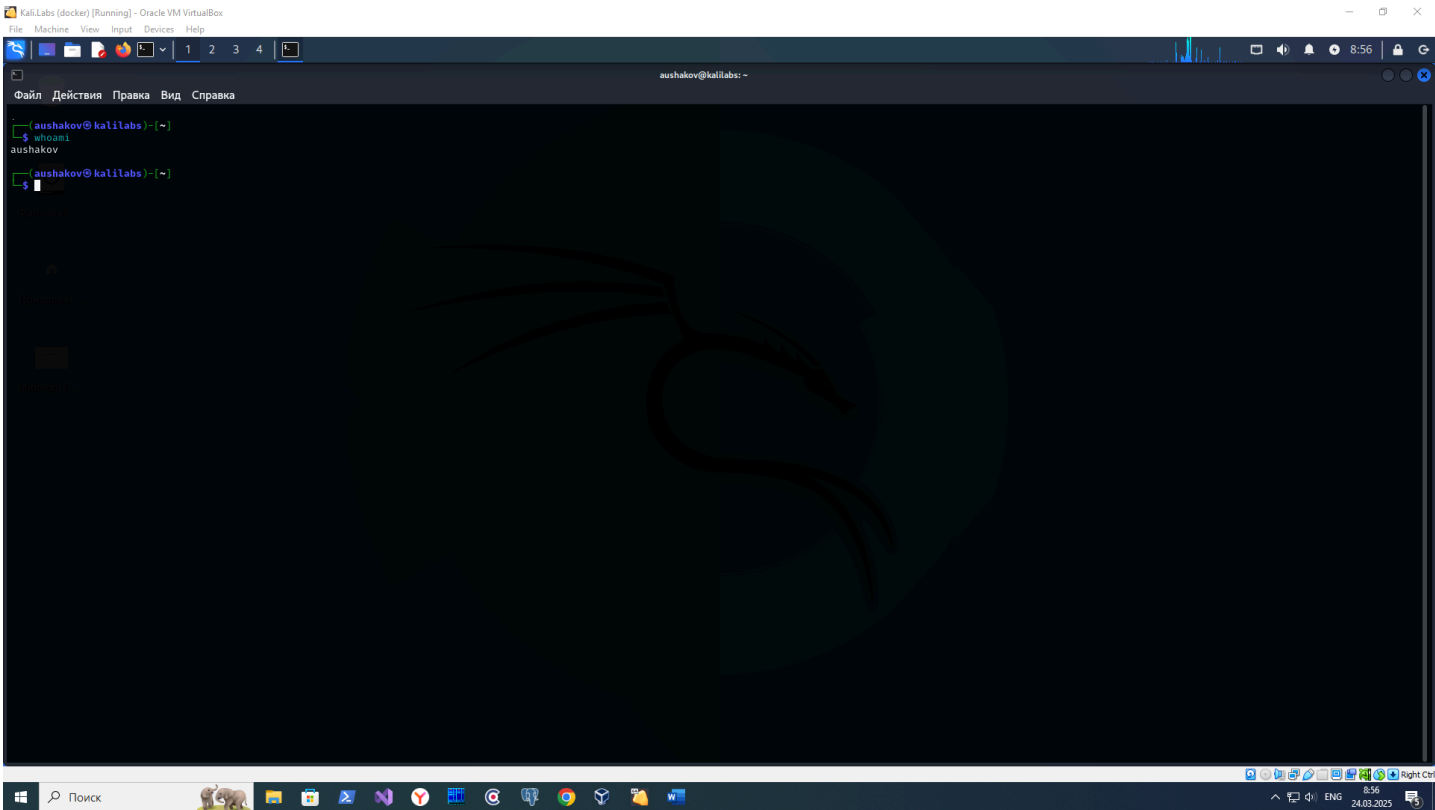
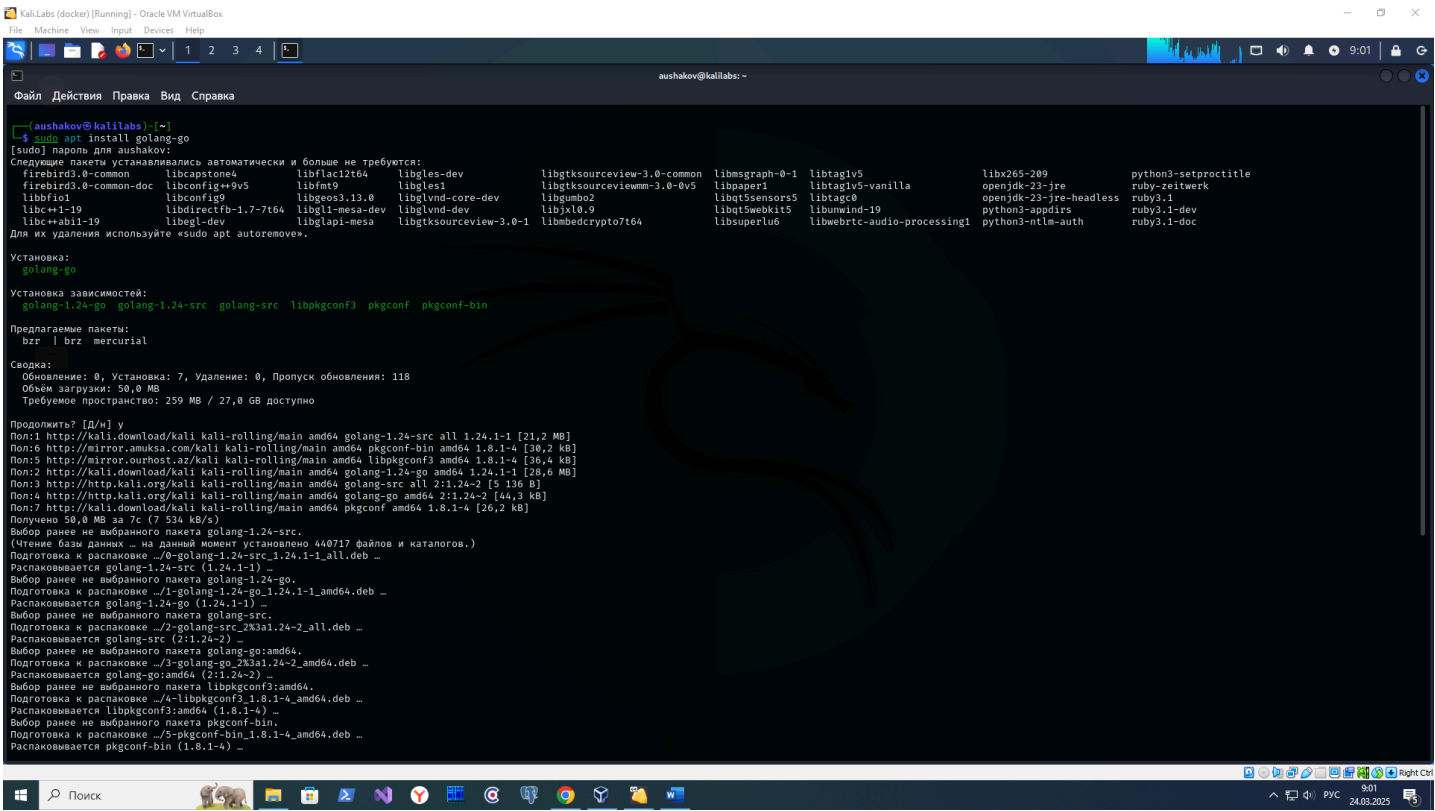


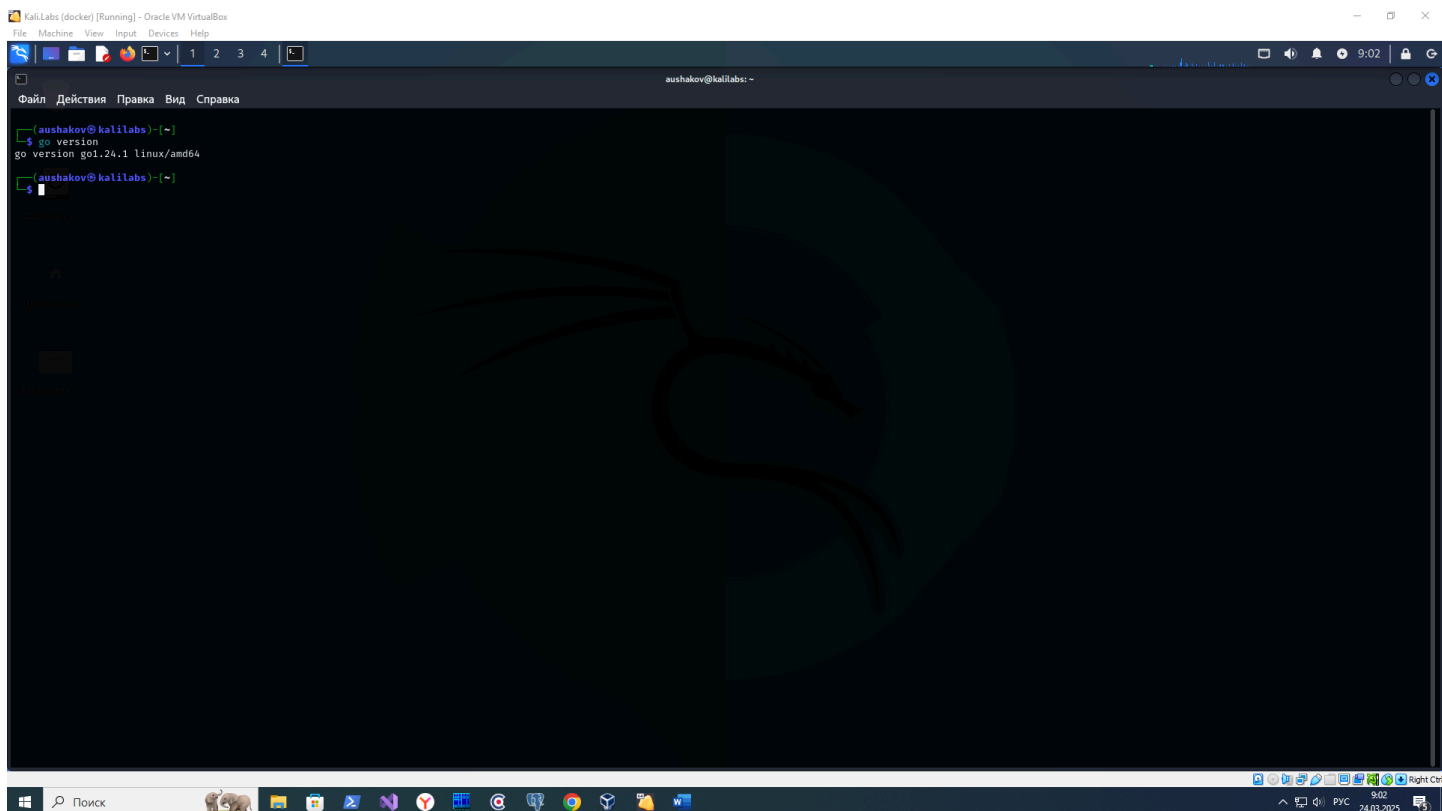
Создаю виртуальную машину на Kali Linux



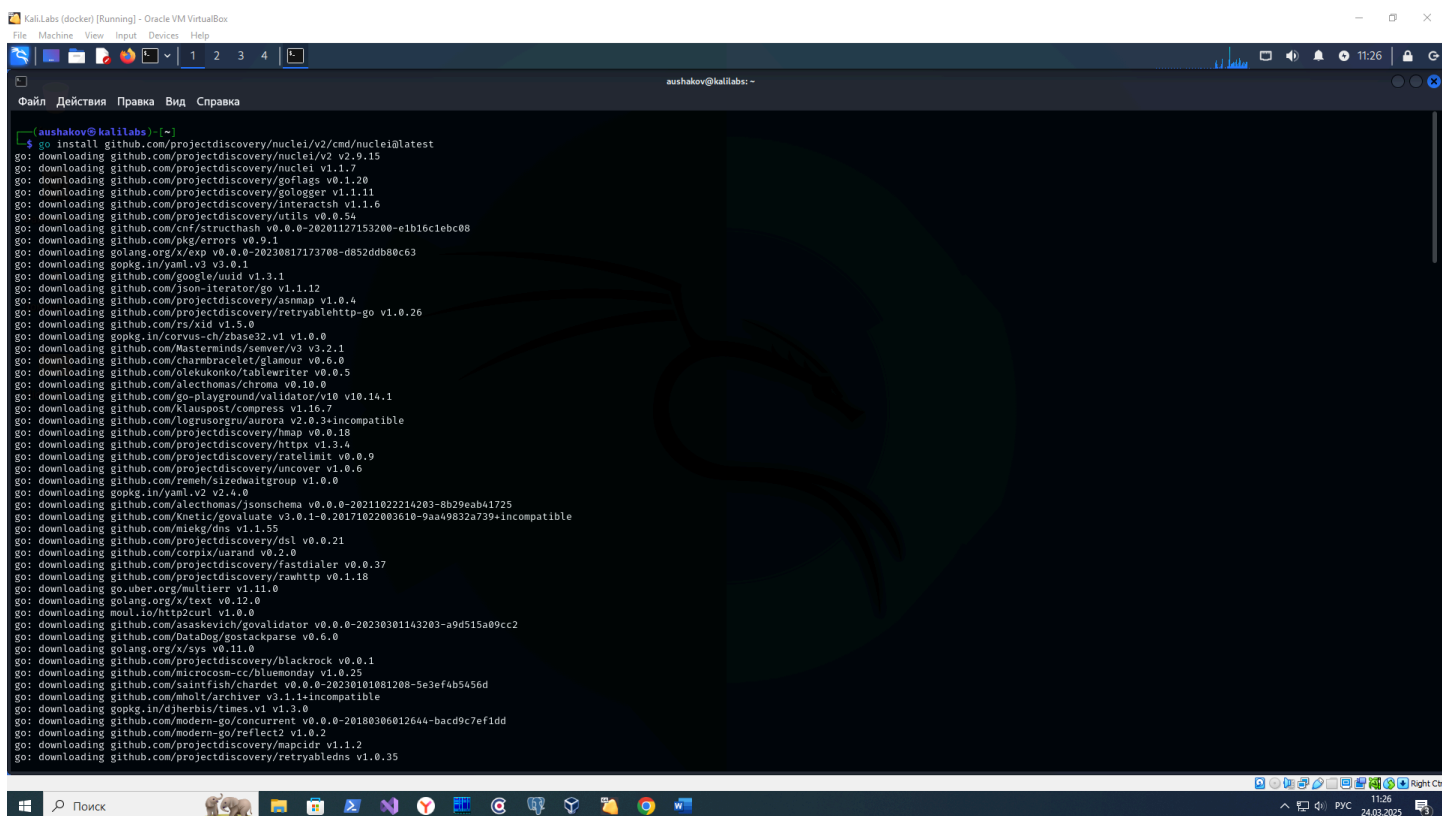
Устанавливаю golang для работы с Nuclei



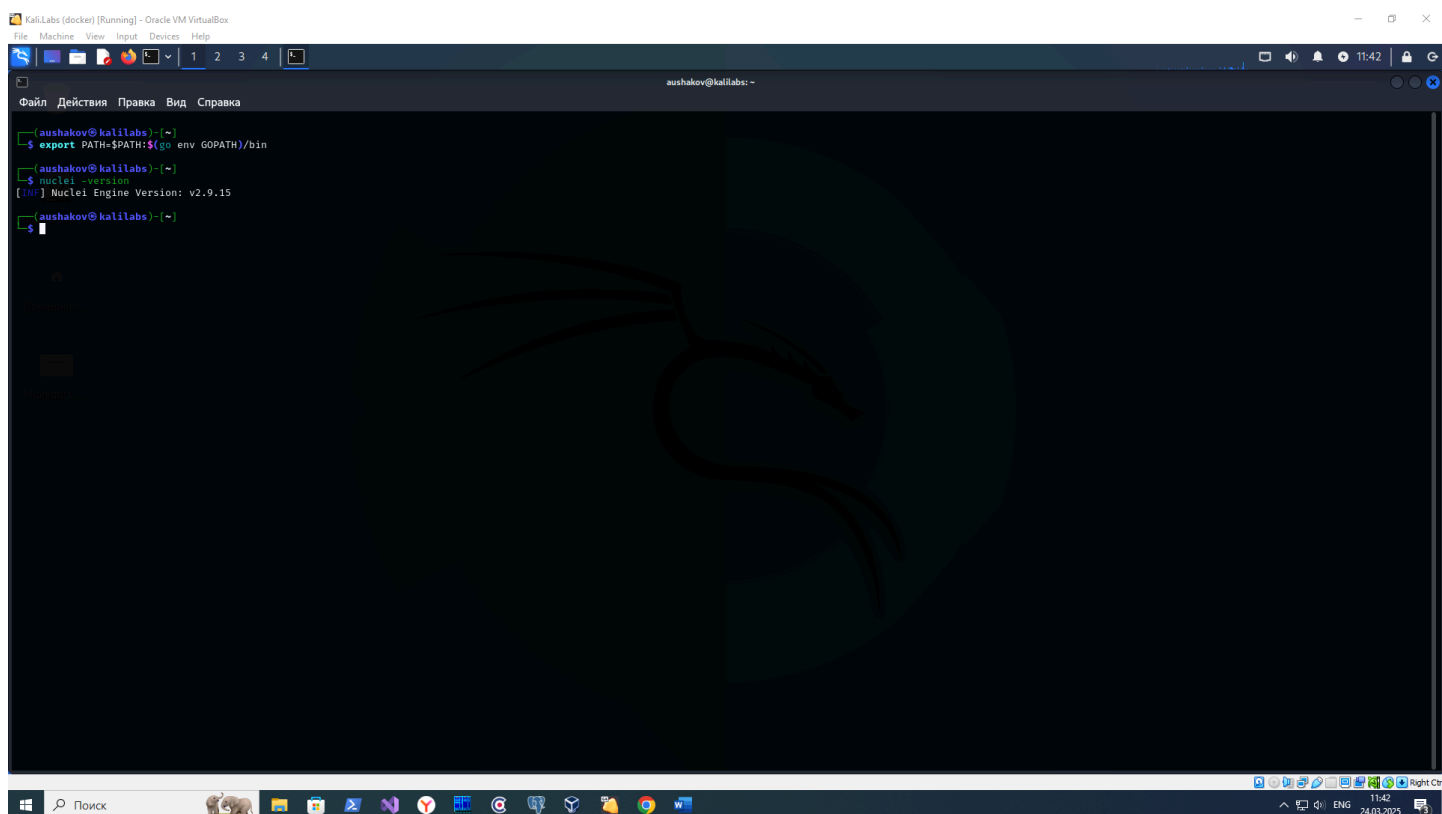
Проверяю версию golang



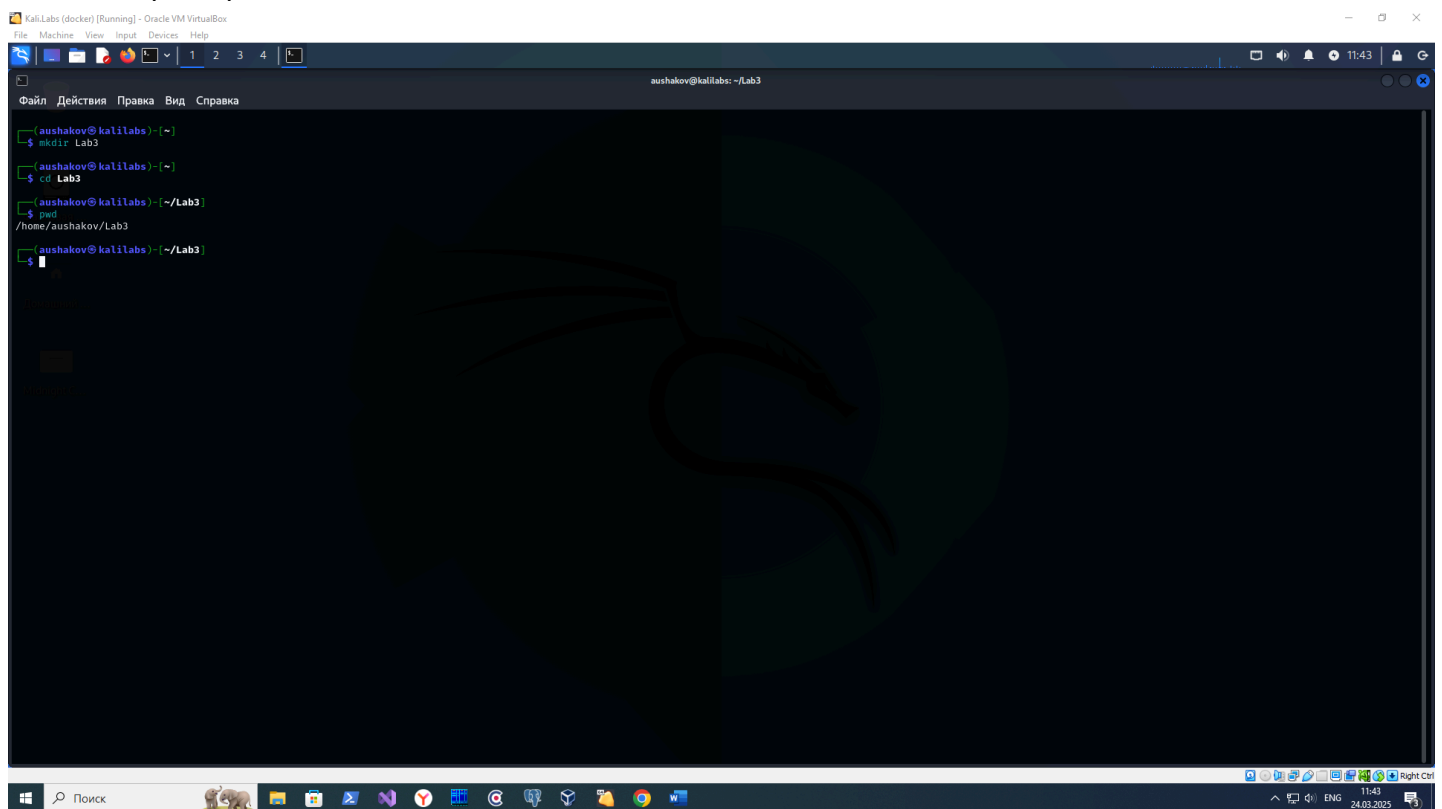
Устанавливаю Nuclei



Проверяю версию Nuclei



Создаю директорию для моих шаблонов Nuclei



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

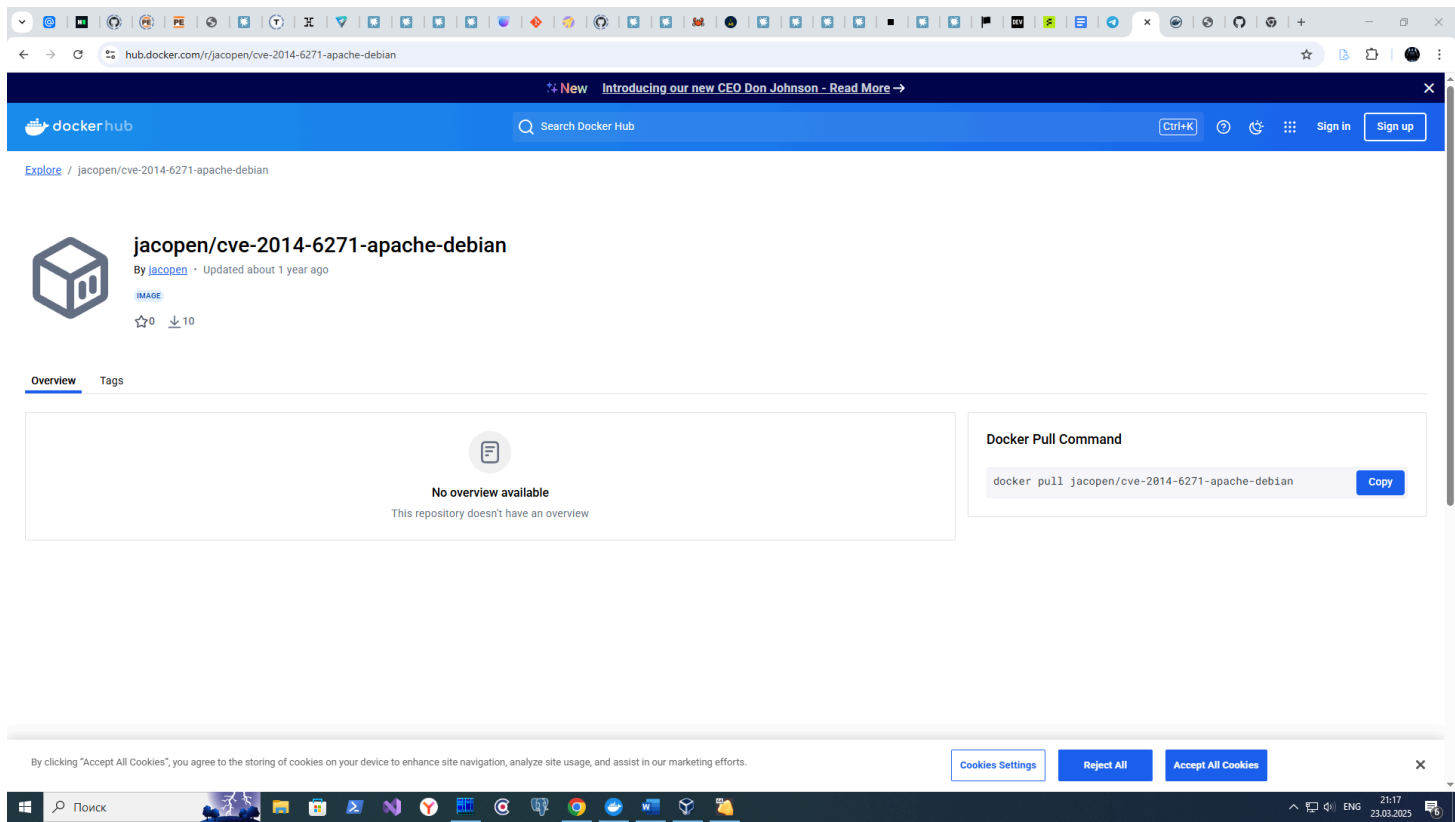
```
Kali.Labs (docker) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
aushakov@kalilabs: ~/Lab3
$ touch server-detect.yml
$ ls -la
итого 8
drwxrwxr-x 2 aushakov aushakov 4096 мар 24 23:27 .
drwxr-xr-x 19 aushakov aushakov 4096 мар 24 23:24 ..
-rw-rw-r-- 1 aushakov aushakov 0 мар 24 23:27 server-detect.yml
$
```

```
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
```

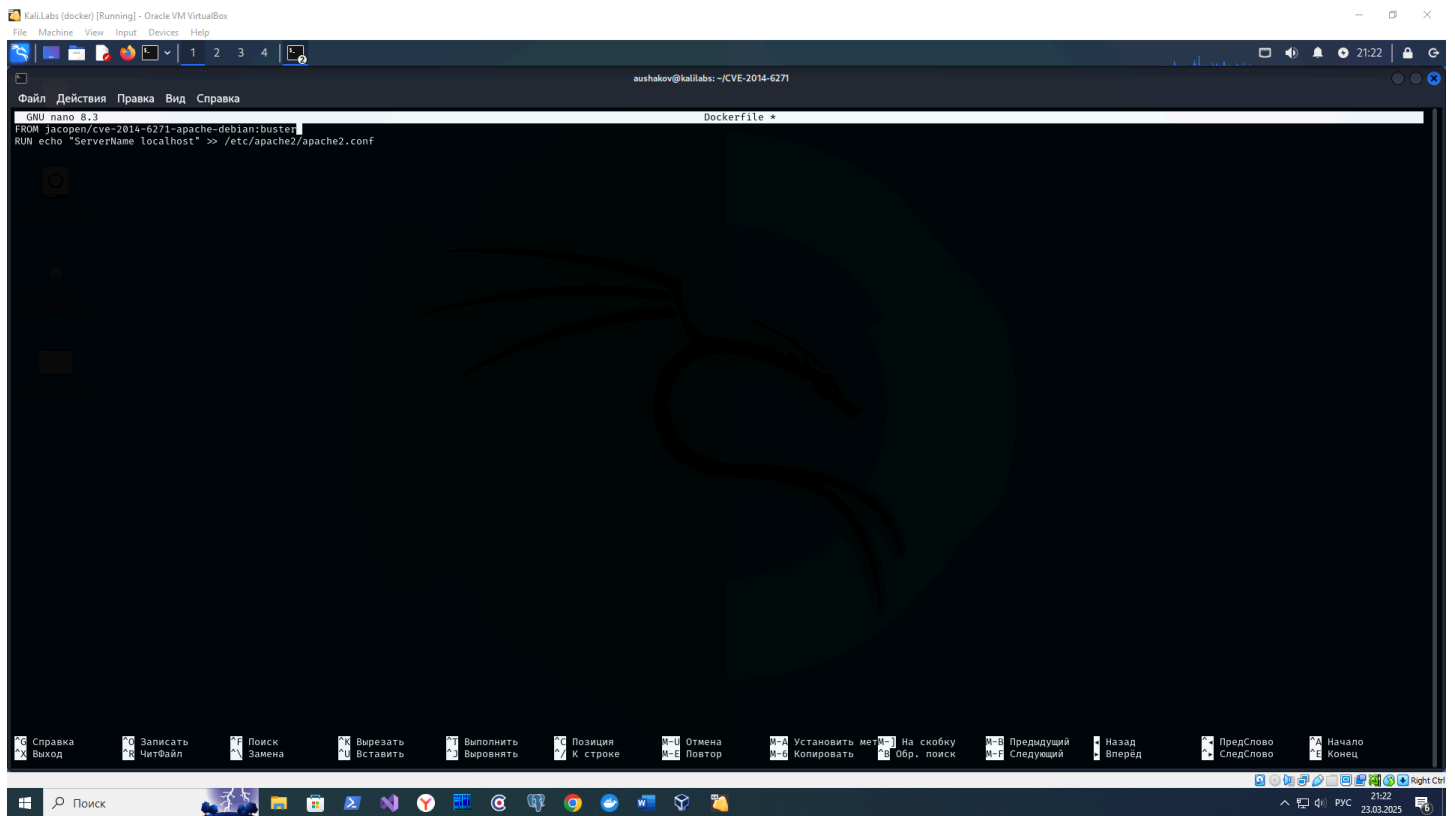
Описание шаблона:

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).



Создаю Dockerfile на основе образа `jacopen/cve-2014-6271-apache-debian`:



Запускаю сборку образа моего контейнера docker

```
kaliLabs [docker] [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
aushakov@kali: ~ /CVE-2014-6271

aushakov@kali:~$ sudo docker build -t shellshock .
[+] Building 20.0s (6/6) FINISHED
=> [internal] load build definition from Dockerfile
=> => transferring dockerfile: 147B
=> [internal] load metadata for docker.io/jacopen/cve-2014-6271-apache-debian:buster
=> [internal] load .dockerignore
=> => transferring context: 2B
=> [1/2] FROM docker.io/jacopen/cve-2014-6271-apache-debian:buster@sha256:43577a82c8a14baaf84e9213588eb0a1918fa8a4d89d6b7e33371af6679ddb5
=> resolve docker.io/jacopen/cve-2014-6271-apache-debian:buster@sha256:43577a82c8a14baaf84e9213588eb0a1918fa8a4d89d6b7e33371af6679ddb5
=> sha256:43577a82c8a14baaf84e9213588eb0a1918fa8a4d89d6b7e33371af6679ddb5 1.57kB / 1.57kB
=> sha256:1dd5a6a2e6d153108519269792e8206662170e53ab556623e612e3aaf6ae1f44 2.67kB / 2.67kB
=> sha256:a9a7bf5165e4a8e137c0a7612407053eb4b07f73f4d6f15a64c2d52c681d500 50.50MB / 50.50MB
=> sha256:1d93abefbc7accf6a9031d6e99e891c71fcc001adb63f0ecc33cd574db900ae 41.93MB / 41.93MB
=> sha256:cb67058af6a03e35cbecd1466b6789d2baac8ade958051368200a28988dd1d99 3.12MB / 3.12MB
=> sha256:67d22087dfe98ccdf5a72db19693655d9b3058c1a3489c61eafb98ae03eed4c 228B / 228B
=> sha256:0f0474da28b696c36fd8edbd8f51a7db27ad96a70f9f50a14d0b345ae3585c84 395B / 395B
=> sha256:3269720d198a32bd7230e9b40ac8a63c72de97c229076ee56eafe018f02d07d4 3.49kB / 3.49kB
=> extracting sha256:a9a7bf5165e4a8e137c0a7612407053eb4b07f73f4d6f15a64c2d52c681d500
=> extracting sha256:1d93abefbc7accf6a9031d6e99e891c71fcc001adb63f0ecc33cd574db900ae
=> extracting sha256:cb67058af6a03e35cbecd1466b6789d2baac8ade958051368200a28988dd1d99
=> extracting sha256:67d22087dfe98ccdf5a72db19693655d9b3058c1a3489c61eafb98ae03eed4c
=> extracting sha256:0f0474da28b696c36fd8edbd8f51a7db27ad96a70f9f50a14d0b345ae3585c84
=> extracting sha256:3269720d198a32bd7230e9b40ac8a63c72de97c229076ee56eafe018f02d07d4
[2/2] RUN echo "ServerName localhost" >> /etc/apache2/apache2.conf
=> exporting to image
=> writing image sha256:a20e529a998ee4b1431477b7064f3dda3cd8c57afd9e6df4eb7f36330ee9ea
=> naming to docker.io/library/shellshock
aushakov@kali:~$
```

Запускаю созданный контейнер docker (с учетом необходимости проброса портов)

```
kaliLabs [docker] [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
aushakov@kali: ~ /CVE-2014-6271

aushakov@kali:~$ sudo docker run --rm -p 8080:80 shellshock
```

```
Kali.Labs (docker) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

aushakov@kalilabs: ~/CVE-2014-6271

aushakov@kalilabs:~/CVE-2014-6271$ sudo docker ps
[sudo] пароль для aushakov:
CONTAINER ID   IMAGE     COMMAND                  CREATED        STATUS        PORTS                               NAMES
163071f409fb   shellshock  "/usr/sbin/apache2ctl..." 45 seconds ago Up 44 seconds  0.0.0.0:8080->80/tcp, :::8080->80/tcp  gallant_hermann

aushakov@kalilabs:~/CVE-2014-6271$
```

Запускаю выполнение Nuclei только на моем созданном шаблоне

```
Kali.Labs (docker) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

aushakov@kalilabs: ~/Lab3

aushakov@kalilabs:~/Lab3$ nuclei -t ./server-detect.yaml -u http://localhost:8080

nuclei
v2.9.15
projectdiscovery.io

[WARN] Found 1 templates loaded with deprecated protocol syntax, update before v3 for continued support.
[INFO] Current nuclei version: v2.9.15 (outdated)
[INFO] Current nuclei-templates version: v10.1.5 (latest)
[INFO] New templates added in latest release: 281
[INFO] Templates loaded for current scan: 1
[INFO] Targets loaded for current scan: 1
[Lab3-server-detect] [http] [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.