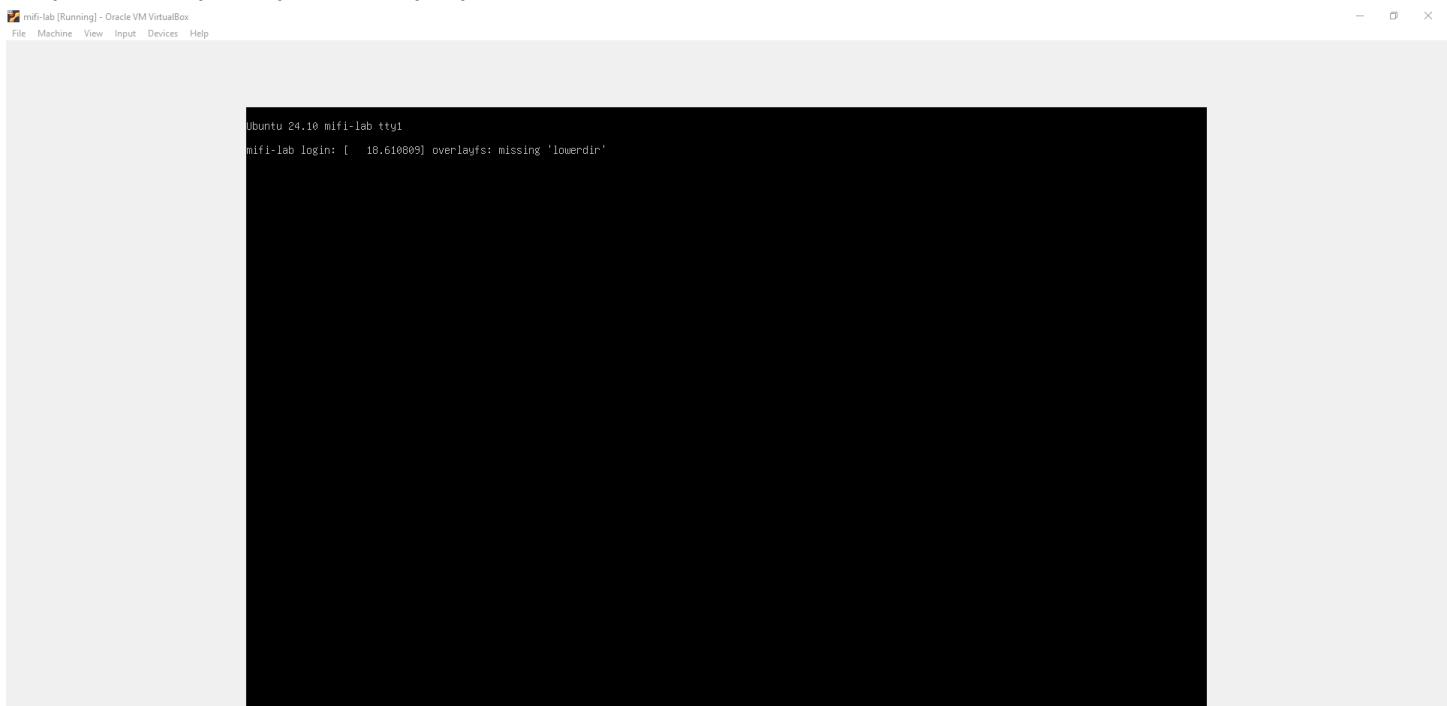
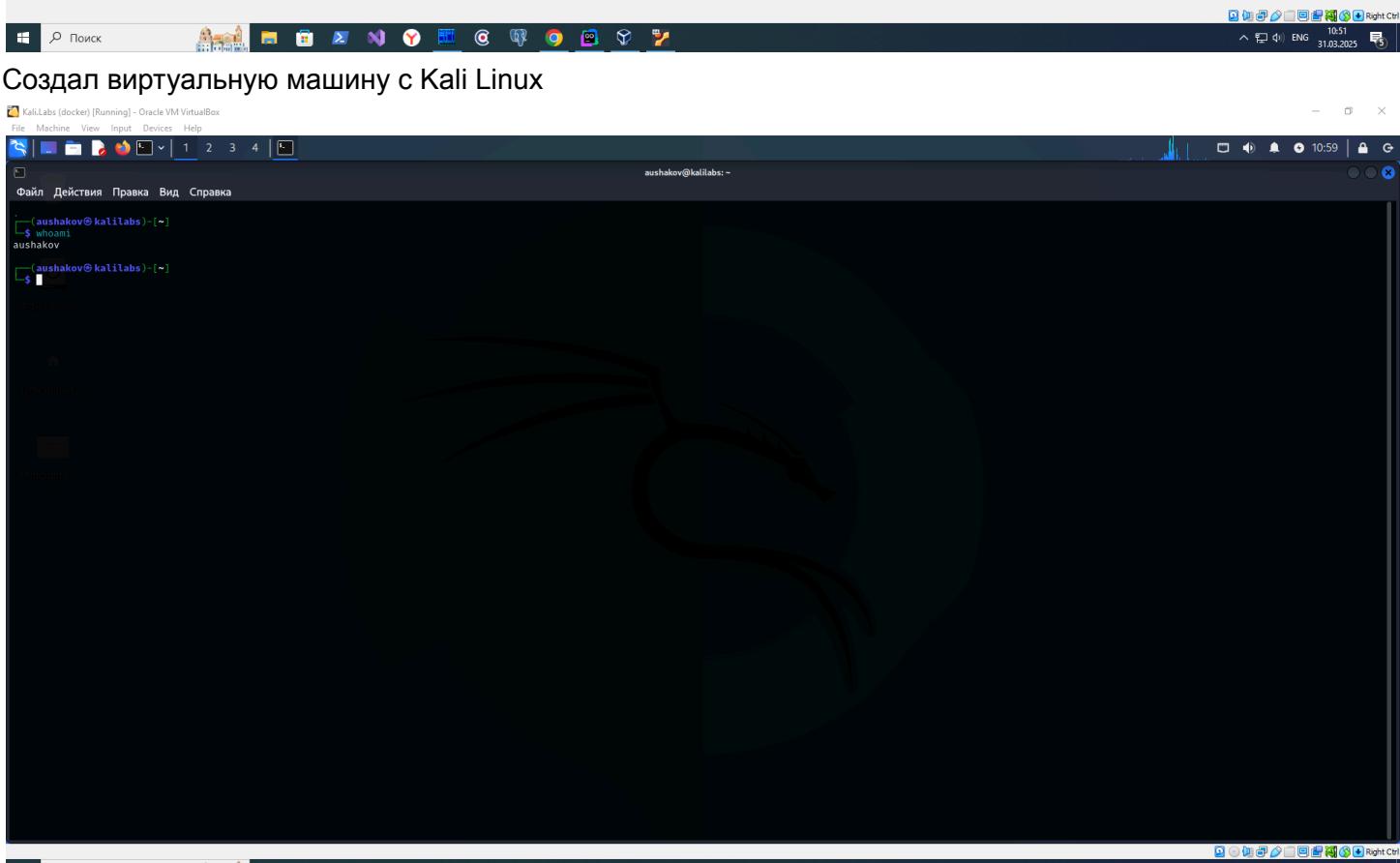


Запустил виртуальную машину с уязвимостями



Создал виртуальную машину с Kali Linux



Определяю ip-адрес машины с уязвимостями:

```
[aushakov@kali: ~]
$ sudo nmap -v -p 8888 --open 192.168.1.0/24
[sudo] пароль для aushakov:
Starting Nmap 7.91 ( https://nmap.org ) at 2025-03-31 19:09 +05
Initiating ARP Ping Scan at 19:09
Scanning 255 hosts [1 port/host]
Completed ARP Ping Scan at 19:09, 1.98s elapsed (255 total hosts)
Initiating Parallel DNS resolution of 7 hosts. at 19:09
Completed Parallel DNS resolution of 7 hosts. at 19:09, 0.51s elapsed
Initiating Parallel DNS resolution of 1 host. at 19:09
Completed Parallel DNS resolution of 1 host. at 19:09, 0.50s elapsed
Initiating SYN Stealth Scan at 19:09
Scanning 7 hosts [1 port/host]
Completed open port 8888/tcp on 192.168.1.136
Completed SYN Stealth Scan at 19:09, 0.22s elapsed (7 total ports)
Nmap scan report for 192.168.1.136
Host is up (0.00072s latency).

PORT      STATE SERVICE
8888/tcp  open  sun-answerbook
MAC Address: 08:00:27:64:8D:2F (PC Systemtechnik/Oracle VirtualBox virtual NIC)

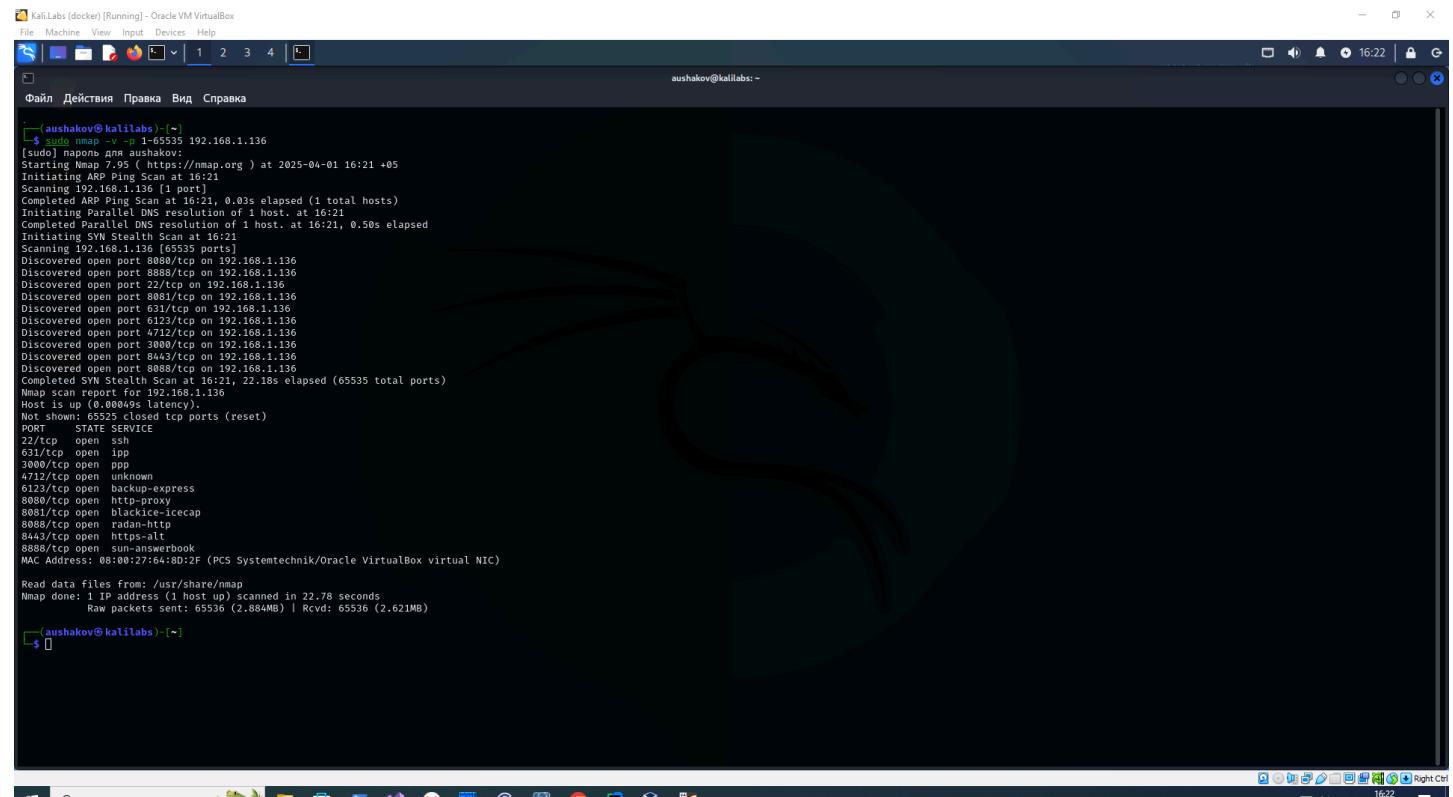
Initiating SYN Stealth Scan at 19:09
Scanning 192.168.1.136 [1 port]
Completed SYN Stealth Scan at 19:09, 0.01s elapsed (1 total ports)
Read data files from: /usr/share/nmap
Nmap done: 256 IP addresses (8 hosts up) scanned in 3.32 seconds
Raw packets sent: 517 (14.620KB) | Rcvd: 20 (664B)
```

Для этого я использую следующую команду: ping -v -p 8888 --open 192.168.1.0/24. Видно, что ip-адрес машины с уязвимостями следующий: 192.168.1.136.

Можно еще проверить, что данная машина пингуется:

```
[aushakov@kali: ~]
$ ping 192.168.1.136
PING 192.168.1.136 (192.168.1.136) 56(84) bytes of data.
64 bytes from 192.168.1.136: icmp_seq=1 ttl=64 time=0.576 ms
64 bytes from 192.168.1.136: icmp_seq=2 ttl=64 time=0.540 ms
64 bytes from 192.168.1.136: icmp_seq=3 ttl=64 time=0.566 ms
64 bytes from 192.168.1.136: icmp_seq=4 ttl=64 time=0.617 ms
```
--- 192.168.1.136 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3056ms
rtt min/avg/max/mdev = 0.540/0.574/0.617/0.027 ms
```

Проверяю с помощью nmap, какие порты открыты с указанием 1-65535 в качестве диапазона проверяемых портов (можно, например, для простоты использовать опцию -F: быстрое сканирование ограниченного количества портов)



```
[aushakov@kalilabs:~] $ sudo nmap -v -r 1-65535 192.168.1.136
[sudo] пароль для aushakov:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-01 16:21 +05
Initiating ARP Ping Scan at 16:21
Scanner Version: 7.95 (https://nmap.org)
Completed ARP Ping Scan at 16:21, 0.03s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 16:21
Completed Parallel DNS resolution of 1 host. at 16:21, 0.50s elapsed
Initiating SYN Stealth Scan at 16:21
Scanning 192.168.1.136 [65535 ports]
Discovered open port 8088/tcp on 192.168.1.136
Discovered open port 8080/tcp on 192.168.1.136
Discovered open port 22/tcp on 192.168.1.136
Discovered open port 8081/tcp on 192.168.1.136
Discovered open port 631/tcp on 192.168.1.136
Discovered open port 6123/tcp on 192.168.1.136
Discovered open port 4712/tcp on 192.168.1.136
Discovered open port 3000/tcp on 192.168.1.136
Discovered open port 8083/tcp on 192.168.1.136
Discovered open port 8084/tcp on 192.168.1.136
Completed SYN Stealth Scan at 16:21, 22.18s elapsed (65535 total ports)
Nmap scan report for 192.168.1.136
Host is up (0.00049s latency).
Not shown: 65525 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
631/tcp   open  ipp
3000/tcp  open  ppp
4712/tcp  open  unknown
6123/tcp  open  backup-express
8080/tcp  open  http-proxy
8081/tcp  open  blackice-icecap
8083/tcp  open  radan-http
8443/tcp  open  https-alt
8888/tcp  open  sun-answerbook
MAC Address: 08:00:27:64:8D:2F (PC Systemtechnik/Oracle VirtualBox virtual NIC)

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 22.78 seconds
Raw packets sent: 65536 (2.884MB) | Rcvd: 65536 (2.621MB)
[aushakov@kalilabs:~] $
```

Для этого я использую следующую команду: nmap -v -r 1-65535 192.168.1.136

Результаты ее работы следующие (продублировал информацию со скриншота выше) - обнаружено 10 открытых портов:

```
22/tcp open ssh
631/tcp open ipp
3000/tcp open ppp
4712/tcp open unknown
6123/tcp open backup-express
8080/tcp open http-proxy
8081/tcp open blackice-icecap
8088/tcp open radan-http
8443/tcp open https-alt
8888/tcp open sun-answerbook
```

Определяю с помощью nmap службы и их версии на обнаруженных ранее открытых портах.

1. Использую для параметра version-intensity значение 2:

Для этого я использую следующую команду:

птар -у -р 22 631 3000 4712 6123 8080 8081 8088 8443 8888 -sV --version-intensity 2 192 168 1 1 136

Результаты ее работы следующие (продублировал информацию со скриншота выше):

22/tcp open ssh OpenSSH 9.7p1 Ubuntu 7ubuntu4.2 (Ubuntu Linux; protocol 2.0)  
631/tcp open ipp CUPS 2.4

```

3000/tcp open  http      Grafana http
4712/tcp open  unknown
6123/tcp open  backup-express?
8080/tcp open  http      mini_httpd 1.29 23May2018
8081/tcp open  blackice-icecap?
8088/tcp open  http      Apache httpd 2.4.62 ((Debian))
8443/tcp open  ssl/http  nginx 1.11.13
8888/tcp open  http      Jetty

```

## 2. Использую для параметра version-intensity значение 6:

```

KaliLabs (docke) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Machine View Input Devices Help
Файл Действия Правка Вид Справка
sushakov@kalilabs: ~
$ sudo nmap -T4 -O -v -sV --version-intensity 6 192.168.1.136
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-01 16:44 +05
NSE: Loaded 47 scripts for scanning
Initiating ARP Ping Scan at 16:44
Scanning 192.168.1.136 [1 port]
Completed ARP Ping Scan at 16:44, 0.03s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 16:44
Completed Parallel DNS resolution of 1 host. at 16:44, 0.00s elapsed
Initiating SYN Stealth Scan at 16:44
Scanning 192.168.1.136 [10 ports]
Discovered open port 8888/tcp on 192.168.1.136
Discovered open port 22/tcp on 192.168.1.136
Discovered open port 8080/tcp on 192.168.1.136
Discovered open port 8081/tcp on 192.168.1.136
Discovered open port 6123/tcp on 192.168.1.136
Discovered open port 8088/tcp on 192.168.1.136
Discovered open port 8443/tcp on 192.168.1.136
Discovered open port 3000/tcp on 192.168.1.136
Discovered open port 4712/tcp on 192.168.1.136
Discovered open port 8088/tcp on 192.168.1.136
Completed SYN Stealth Scan at 16:44, 0.025s elapsed (10 total ports)
Initiating Service scan on all open ports
Scanning 10 services on 192.168.1.136
Completed Service scan at 16:45, 76.08s elapsed (10 services on 1 host)
NSE: Script scanning 192.168.1.136.
Initiating NSE at 16:45
Completed NSE at 16:45, 0.01s elapsed
Initiating NSE at 16:45
Completed NSE at 16:45, 0.00s elapsed
Nmap scan report for 192.168.1.136
Host is up (0.0006s latency).

PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 9.7p1 Ubuntu 7ubuntu4.2 (Ubuntu Linux; protocol 2.0)
631/tcp   open  ipp          CUPS 2.4
4712/tcp  open  http         Grafana http
2901/tcp  open  unknown
6123/tcp  open  spark        Apache Spark
8080/tcp  open  http         mini_httpd 1.29 23May2018
8081/tcp  open  blackice-icecap?
8088/tcp  open  http         Apache httpd 2.4.62 ((Debian))
8443/tcp  open  ssl/http    nginx 1.11.13
8888/tcp  open  http         Jetty

Nmap done: 1 IP address (1 host up) scanned in 76.08 seconds

```

The screenshot shows a terminal window titled "KaliLabs (docke) [Running] - Oracle VM VirtualBox". The terminal displays the output of an nmap scan on host 192.168.1.136. The scan uses version-intensity 6 and includes options for parallel DNS resolution and SYN stealth scanning. The output lists various open ports and the services running on them, such as Grafana, Apache Spark, and Jetty. The terminal also shows the host is up with a latency of 0.0006s.

Для этого я использую следующую команду:

```
nmap -v -p 22,631,3000,4712,6123,8080,8081,8088,8443,8888 -sV --version-intensity 5 192.168.1.136
```

Результаты ее работы следующие (продублировал информацию со скриншота выше):

```
22/tcp open ssh          OpenSSH 9.7p1 Ubuntu 7ubuntu4.2 (Ubuntu Linux; protocol 2.0)
631/tcp open ipp         CUPS 2.4
3000/tcp open http        Grafana http
4712/tcp open unknown
6123/tcp open spark       Apache Spark
8080/tcp open http        mini_httpd 1.29 23May2018
8081/tcp open blackice-icecap?
8088/tcp open http        Apache httpd 2.4.62 ((Debian))
8443/tcp open ssl/http    nginx 1.11.13
8888/tcp open http        Jetty
```

3. Использую для параметра version-intensity значение 9:

Для этого я использую следующую команду:

прар -у -р 22 631 3000 4712 6123 8080 8081 8088 8443 8888 -sУ --version-intensity 9 192 168 1 136

Результаты ее работы следующие (продублировал информацию со скриншота выше):

22/tcp open ssh OpenSSH 9.7p1 Ubuntu 7ubuntu4.2 (Ubuntu Linux; protocol 2.0)  
631/tcp openipp CLIPS 2.4

```

3000/tcp open http      Grafana http
4712/tcp open unknown
6123/tcp open spark     Apache Spark
8080/tcp open http      mini_httpd 1.29 23May2018
8081/tcp open blackice-icecap?
8088/tcp open http      Apache httpd 2.4.62 ((Debian))
8443/tcp open ssl/http   nginx 1.11.13
8888/tcp open http      Jetty

```

Результат определения сервисов и их версий:

| порт     | сервис   | версия                                                       |
|----------|----------|--------------------------------------------------------------|
| 22/tcp   | ssh      | OpenSSH 9.7p1 Ubuntu 7ubuntu4.2 (Ubuntu Linux; protocol 2.0) |
| 631/tcp  | ipp      | CUPS 2.4                                                     |
| 3000/tcp | http     | Grafana http                                                 |
| 4712/tcp | -        | Неизвестный сервис                                           |
| 6123/tcp | spark    | Apache Spark                                                 |
| 8080/tcp | http     | mini_httpd 1.29 23May2018                                    |
| 8081/tcp | blackice | icecap (nmap до конца не уверен в этом)                      |
| 8088/tcp | http     | Apache httpd 2.4.62 ((Debian))                               |
| 8443/tcp | ssl/http | nginx 1.11.13                                                |
| 8888/tcp | http     | Jetty                                                        |

Выводы:

- С помощью nmap мы нашли 10 открытых портов
- С помощью nmap определили сервисы и их версии.
- nmap не смог полностью определить один сервис: который слушает на порту 4712/tcp. Хотя судя по выводу (смотри скриншот), этот сервис не смог стартовать корректно и выводит некоторое сообщение об ошибке в текстовом виде.
- nmap не уверен определить один сервис: который слушает на порту 8081/tcp
- Для 3 сервисов nmap не смог определить их версии: который слушают на портах 3000/tcp (Grafana http), 6123/tcp (Apache Spark) и 8888/tcp (Jetty).
- Для всех остальных сервисов nmap смог определить и его тип и его версию.