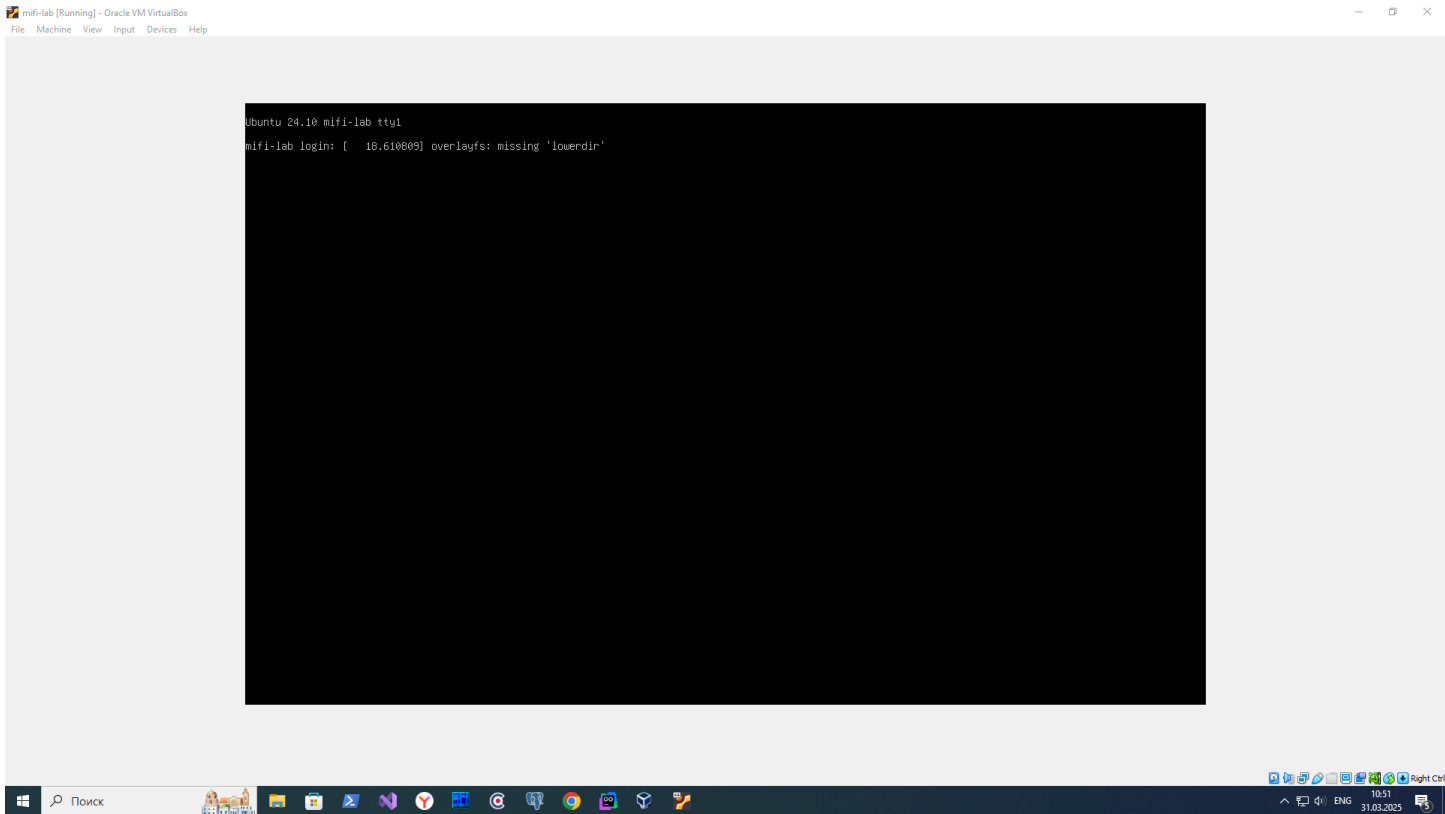
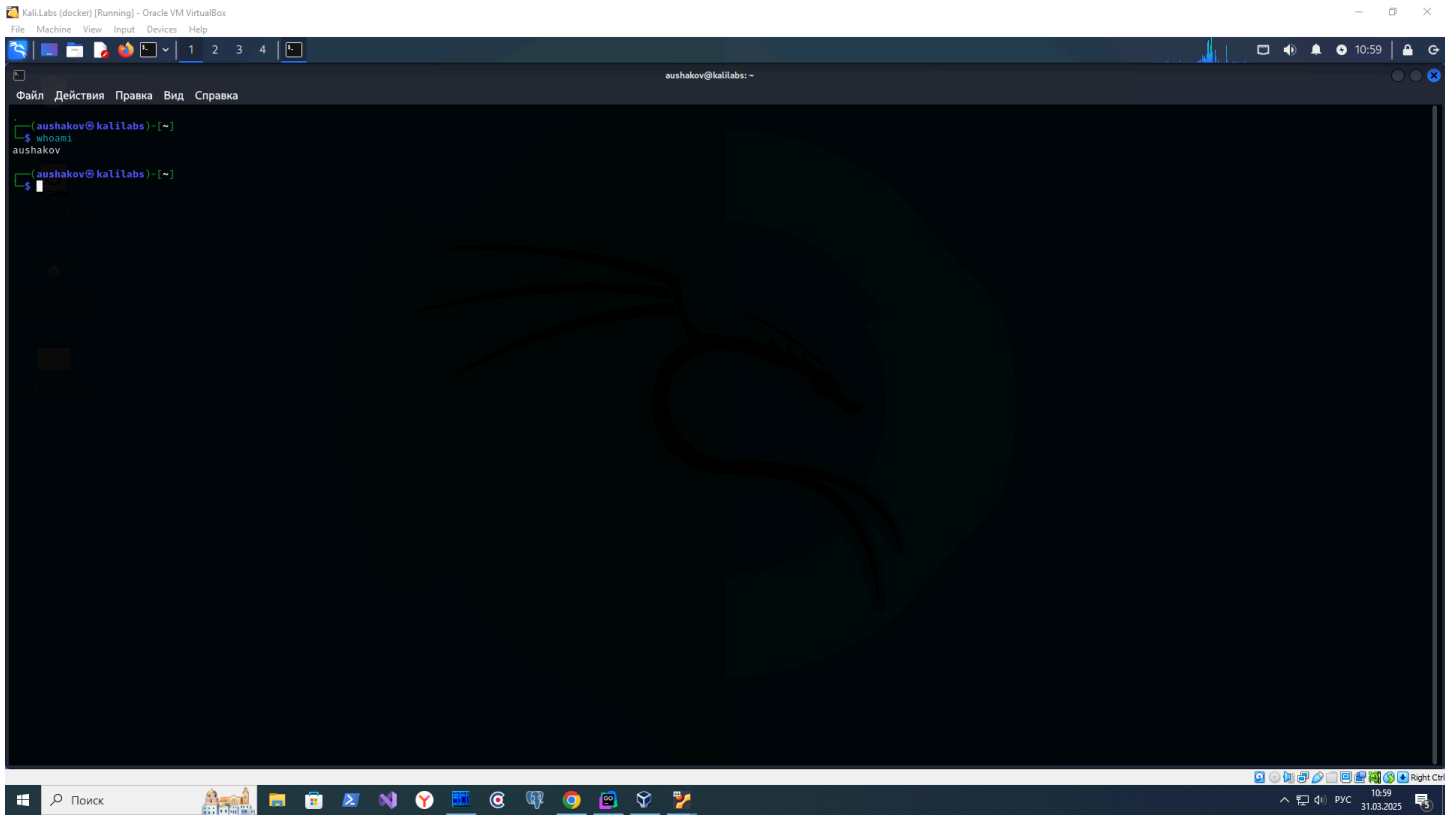


Запустил виртуальную машину с уязвимостями



Создал виртуальную машину с Kali Linux



Определяю ip-адрес машины с уязвимостями:

```
Kali.Labs (docker) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4 5
aushakov@kalilabs: ~
Файл Действия Правка Вид Справка
aushakov@kalilabs:~$ sudo nmap -v -p 8888 --open 192.168.1.0/24
[sudo] пароль для aushakov:
Starting Nmap 7.95 ( 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]
Discovered 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: 08:00:27:64:80:2F (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Initiating SYN Stealth Scan at 19:09
Scanning 192.168.1.118 [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 (14.628KB) | Rcvd: 20 (664B)

aushakov@kalilabs:~$
```

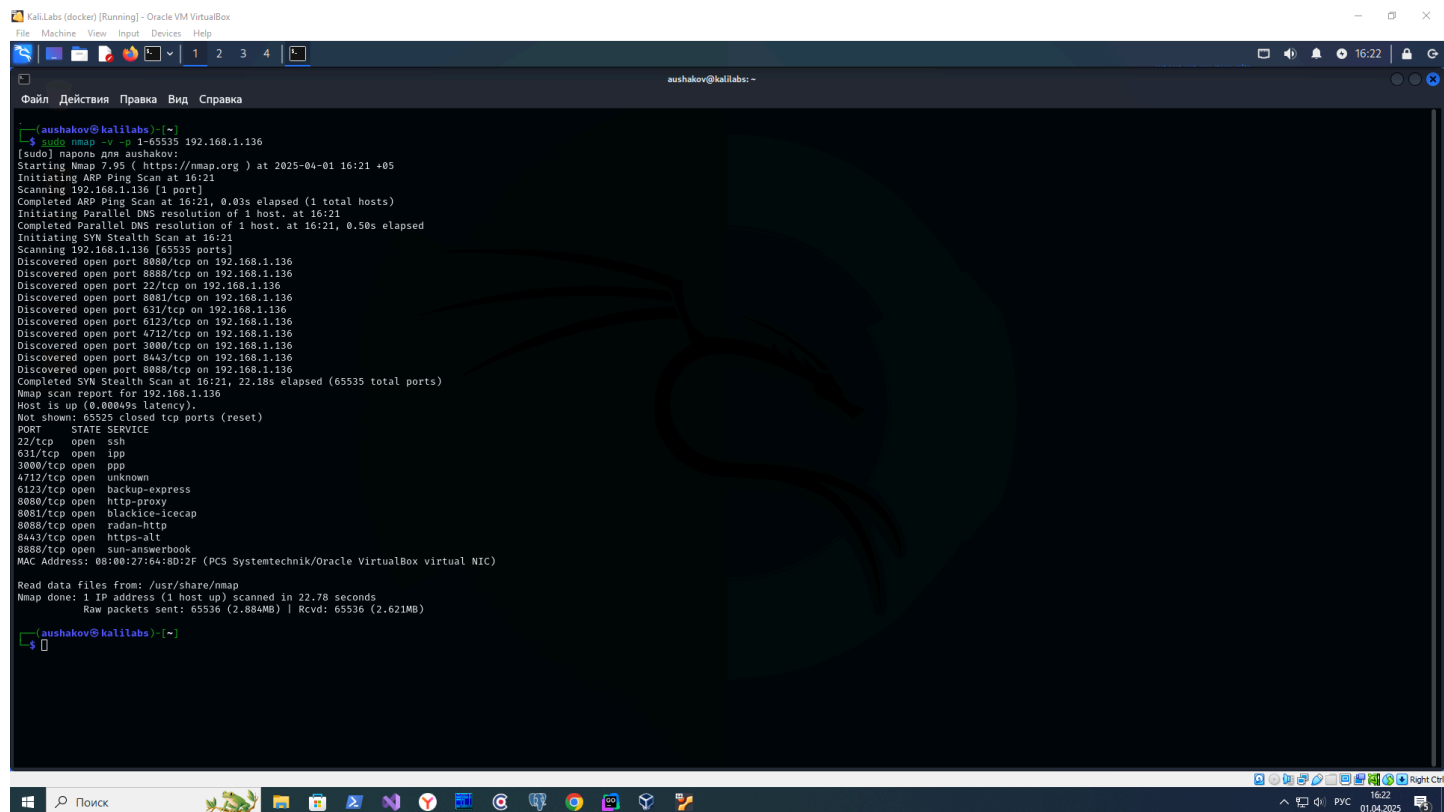
Для этого я использую следующую команду: `nmap -v -p 8888 --open 192.168.1.0/24`. Видно, что ip-адрес машины с уязвимостями следующий: 192.168.1.136.

Можно еще проверить, что данная машина пингуется:

```
Kali.Labs (docker) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4 5
aushakov@kalilabs: ~
Файл Действия Правка Вид Справка
aushakov@kalilabs:~$ 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
^C
--- 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

aushakov@kalilabs:~$
```

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@kali:~$ sudo nmap -v -p 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
Scanning 192.168.1.136 [1 port]
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 8080/tcp on 192.168.1.136
Discovered open port 8888/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 8088/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
8088/tcp  open  radan-http
8443/tcp  open  https-alt
8888/tcp  open  sun-answerbook

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@kali:~$
```

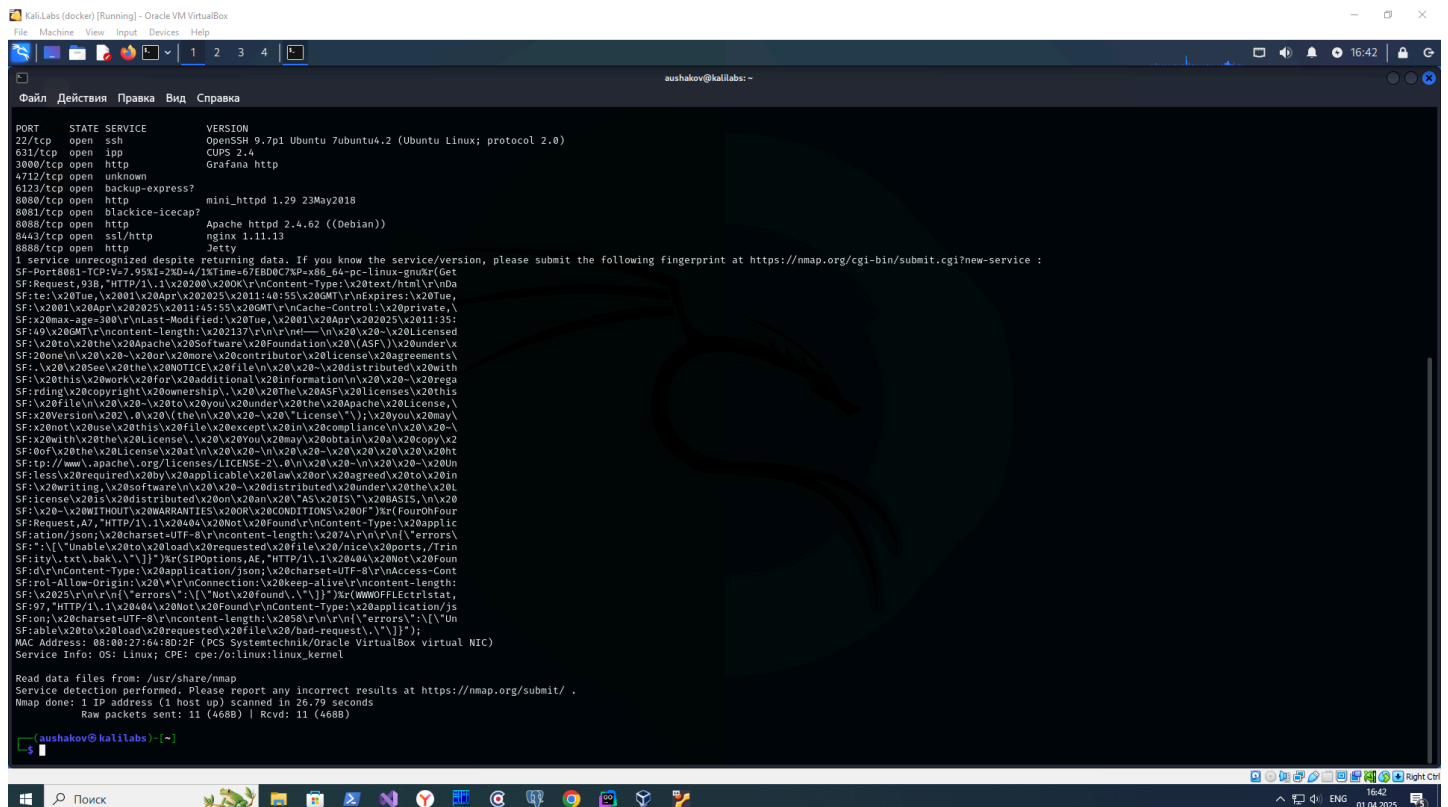
Для этого я использую следующую команду: `nmap -v -p 1-65535 192.168.1.136`

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:



```
nmap -v -p 22,631,3000,4712,6123,8080,8081,8088,8443,8888 -sV --version-intensity 2 192.168.1.136
```

```
22/tcp open  ssh      OpenSSH 9.7p1 Ubuntu 7ubuntu4.2 (Ubuntu Linux; protocol 2.0)
```

CONCLUSIONS

```
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:

Kali Linux (docker) [Running] Oracle VM VirtualBox
File Machine View Input Devices Help

aushakov@kali: ~

Файл Действия Правка Вид Справка

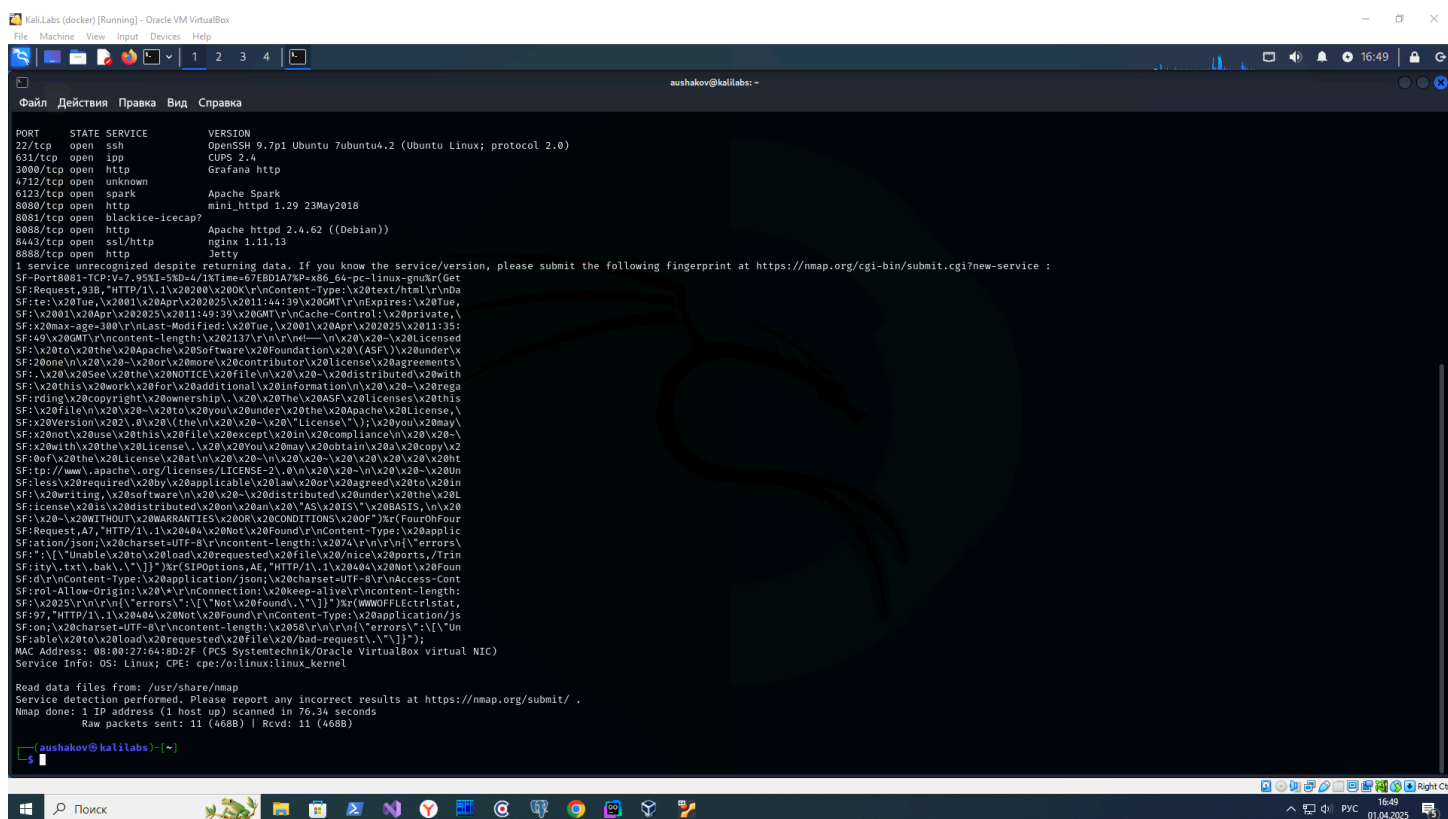
```
aushakov@kali: ~$ sudo nmap -v -p 22,631,3000,4712,6123,8080,8081,8088,8443,8888 -sV --version-intensity 5 192.168.1.136
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-01 16:44 +05
NSE: Loaded 47 scripts for scanning.
Initiating ARP Ping Scan at 16:44
Scanning 192.168.1.136 [1 port]
Completed 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 8088/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 631/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, 0.02s elapsed (10 total ports)
Initiating Service scan at 16:44
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 (0.00076s latency).

PORT      STATE SERVICE
22/tcp    open  ssh
631/tcp   open ipp
3000/tcp  open http
4712/tcp  open unknown
6123/tcp  open spark
8080/tcp  open http
8081/tcp  open blackice-icecap?
8088/tcp  open http
8443/tcp  open ssl/http
8888/tcp  open http

1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF:Port8081-TCP:V=7.95X=540-4/18Time=67EBD1A7P=x86_64-pc-linux-gnuKr(Ge
SF:Request, 920, \x20\x2000\x2000\x20Content-Type:\x20text/html\x20a
SF:te:\x20Tue, \x2001\x20Apr\x202025\x2011:44:39\x20GMT\r\nExpires:\x20Tue,
SF:\x2001\x20Apr\x202025\x2011:49:39\x20GMT\r\nContent-Control:\x20private,\
SF:\x20max-age=300\r\nLast-Modified:\x20Tue, \x2001\x20Apr\x202025\x2011:35:
SF:49\x20GMT\r\nContent-Length:\x202137\r\n\r\n--\x20\x20\x20\x20\x20Licen
SF:\x201\x20the\x20Apache\x20Software\x20Foundation\x20(\x20ASF)\x20Under\x
SF:\x20one\x20of\x20the\x20more\x20contributor\x20license\x20agreements\
```

Поиск

16:48 01.04.2025



```
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
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

I service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port8081-TCP:V=9.5N=5604/I=18Time=67EBD1A7KP=x86_64-pe=linux-gnuR=get
SF:Request,93B,"HTTP/1.1\x20200\x20OK\r\nContent-Type:\x20text/html\r\nnda
SF:te:\x20Tue,\x2001\x20Apr\x202025\x2011:44:39\x20GMT\r\nExpires:\x20Tue,
SF:\x2001\x20Apr\x202025\x2011:49:39\x20GMT\r\nCache-Control:\x20private,\x
SF:\x20max-age=360\r\nLast-Modified:\x20Tue,\x2001\x20Apr\x202025\x2011:35:
SF:49\x20GMT\r\ncontent-length:\x202137\r\n\r\n\x20\x20\x20\x20\x20\x20\x20
SF:\x20to\x20the\x20Apache\x20Software\x20Foundation\x20(ASF)\x20under\x20
SF:\x20the\x20license\x20of\x20the\x20contributor\x20the\x20Apache\x20license,\x
SF:\x20the\x20license\x20of\x20the\x20file\x20the\x20distributed\x20with
SF:\x20this\x20work\x20for\x20additional\x20information\x20\x20\x20\x20\x20regre
SF:ding\x20copyright\x20ownership.\x20\x20The\x20ASF\x20licenses\x20this
SF:\x20file\x20the\x20\x20\x20to\x20you\x20under\x20the\x20Apache\x20license,\x
SF:\x20version\x202.0,\x20of\x20the\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20
SF:\x20not\x20use\x20this\x20file\x20except\x20in\x20compliance\x20\x20\x20\x20
SF:\x20with\x20the\x20license.\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20
SF:00\x20the\x20license\x20of\x20the\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20
SF:tp://www.apache.org/licenses/LICENSE-2.0/\x20\x20\x20\x20\x20\x20\x20\x20
SF:less\x20required\x20by\x20applicable\x20law\x20or\x20agreed\x20to\x20in
SF:\x20writing,\x20software\x20\x20\x20\x20\x20distributed\x20under\x20the\x20
SF:license\x20of\x20the\x20distributed\x20on\x20an\x20ASL\x202018.\x20\x20\x20
SF:\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20
SF:Request,47,"HTTP/1.1\x20404\x20Not\x20Found\r\nContent-Type:\x20applic
SF:ation/json;\x20charset=UTF-8\r\ncontent-length:\x2074\r\n\r\n{"errors\
SF:":{"unable\x20to\x20load\x20requested\x20file\x20nice\x20ports,/trin
SF:ity\,txt\,bak\,\x20}}\x20(SIPoptions,4E,"HTTP/1.1\x20404\x20Not\x20Found
SF:d\r\nContent-Type:\x20application/json;\x20charset=UTF-8\r\nAccess-Cont
SF:rol-allow-Origin:\x20*\r\nConnection:\x20keep-alive\r\ncontent-length:
SF:\x20253\r\n\r\n{"errors":{"not\x20found\,\x20}}\x20(wwwOffEctrIstat,
SF:97,"HTTP/1.1\x20404\x20Not\x20Found\r\nContent-Type:\x20application/js
SF:on;\x20charset=UTF-8\r\ncontent-length:\x2058\r\n\r\n{"errors":{"Un
SF:able\x20to\x20load\x20requested\x20file\x20bad-request\,\x20}}");
MAC Address: 08:00:27:64:8D:2F (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Read data files from: /usr/share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 76.34 seconds
Raw packets sent: 11 (4688) | Rcvd: 11 (4688)
```

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:

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:

1. С помощью nmap мы нашли 10 открытых портов
2. С помощью nmap определили сервисы и их версии.
3. 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.
4. nmap не смог уверенно определить один сервис: который слушает на порту 8081/tcp
5. 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).
6. Для всех остальных сервисов nmap смог определить и его тип и его версию.