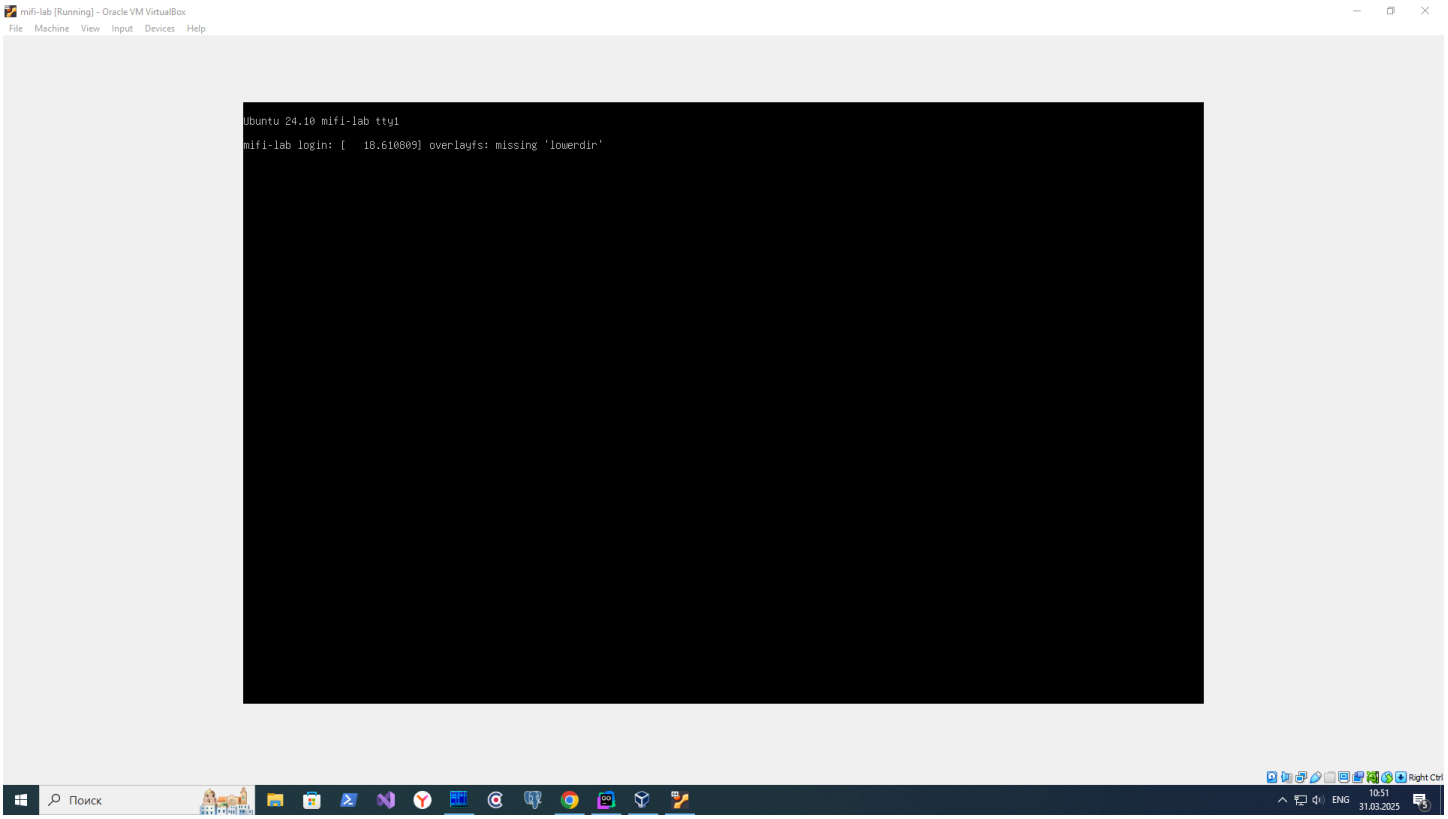
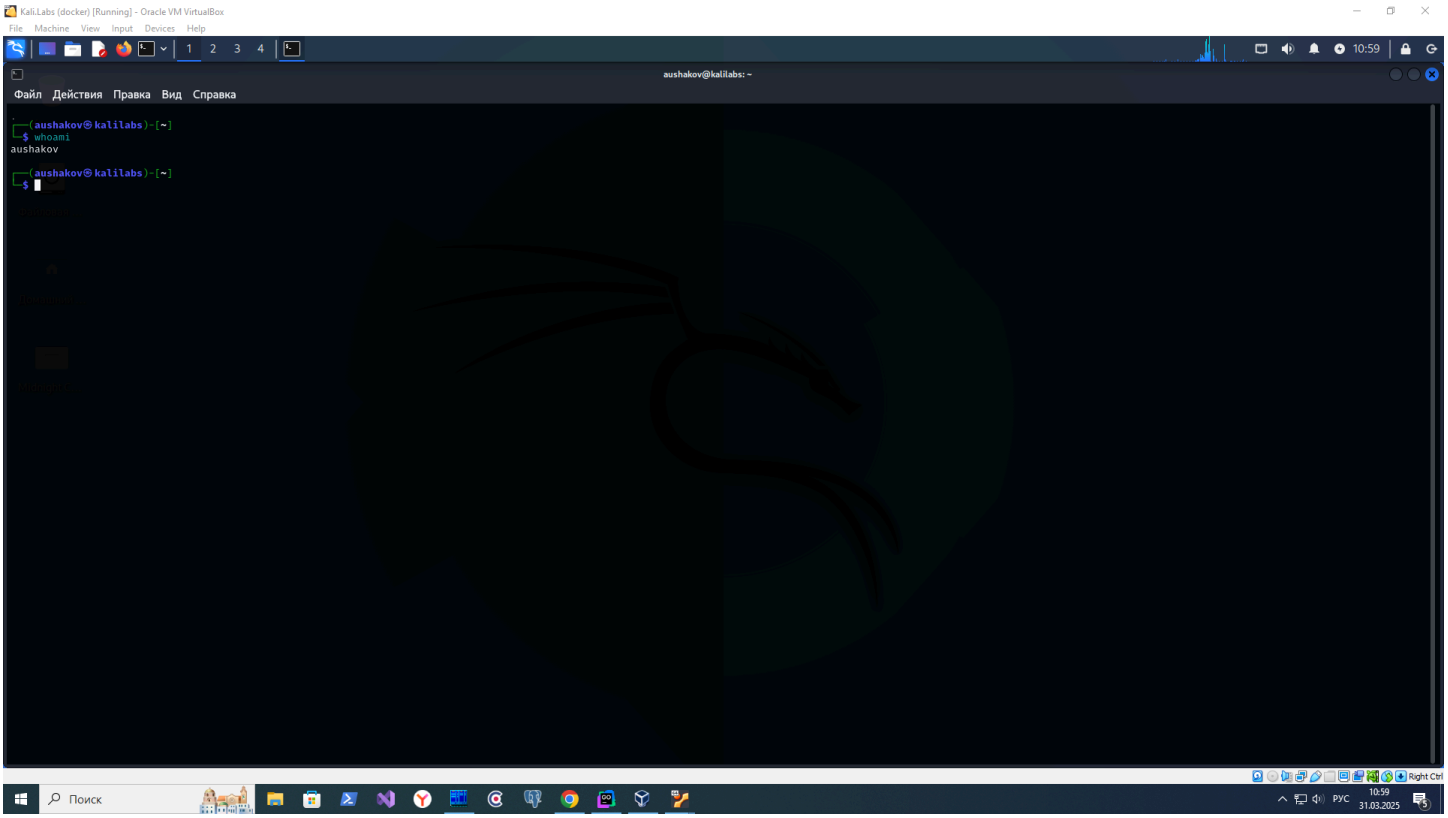
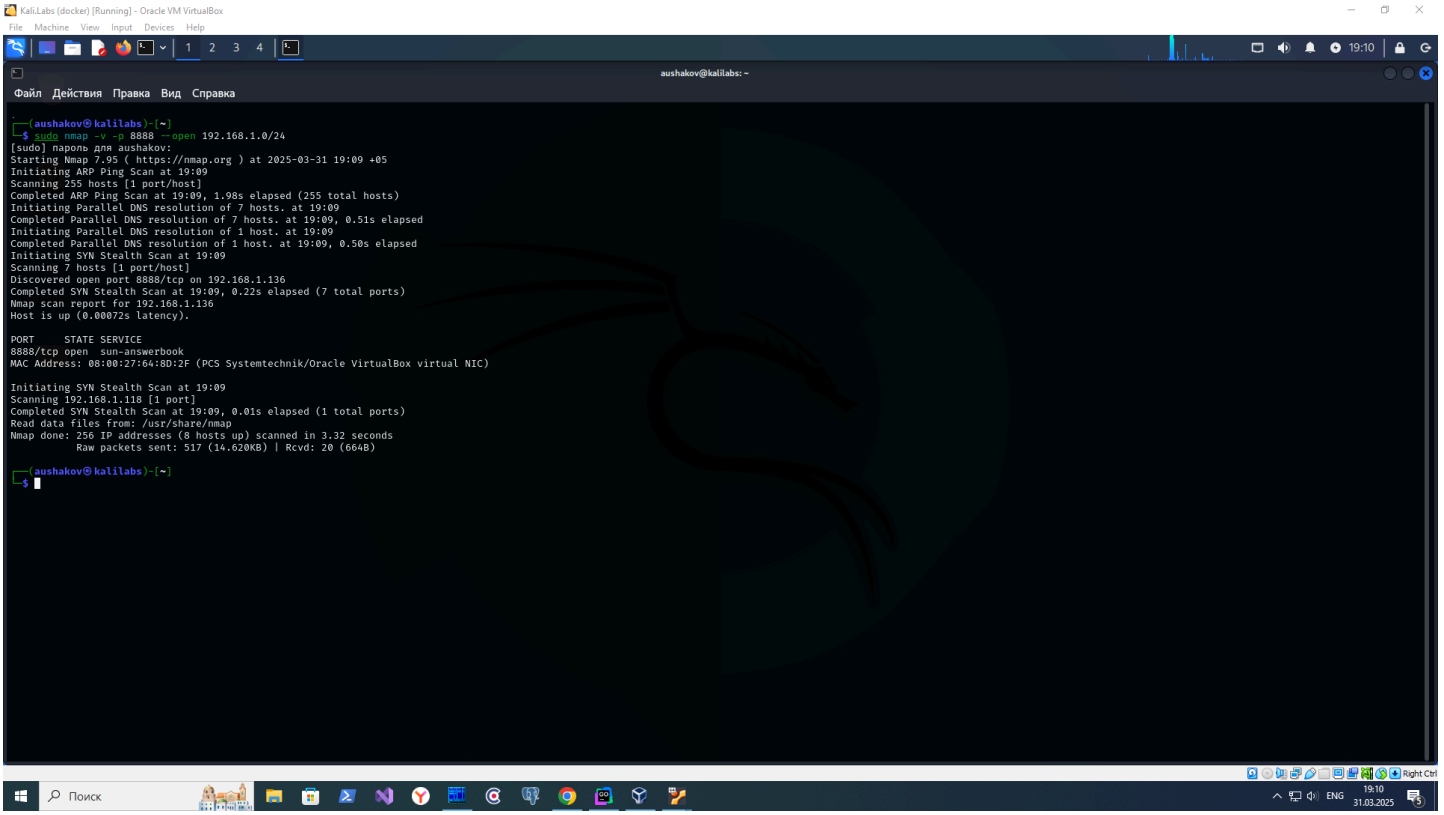
Запустил виртуальную машину с уязвимостями



Создал виртуальную машину с Kali Linux

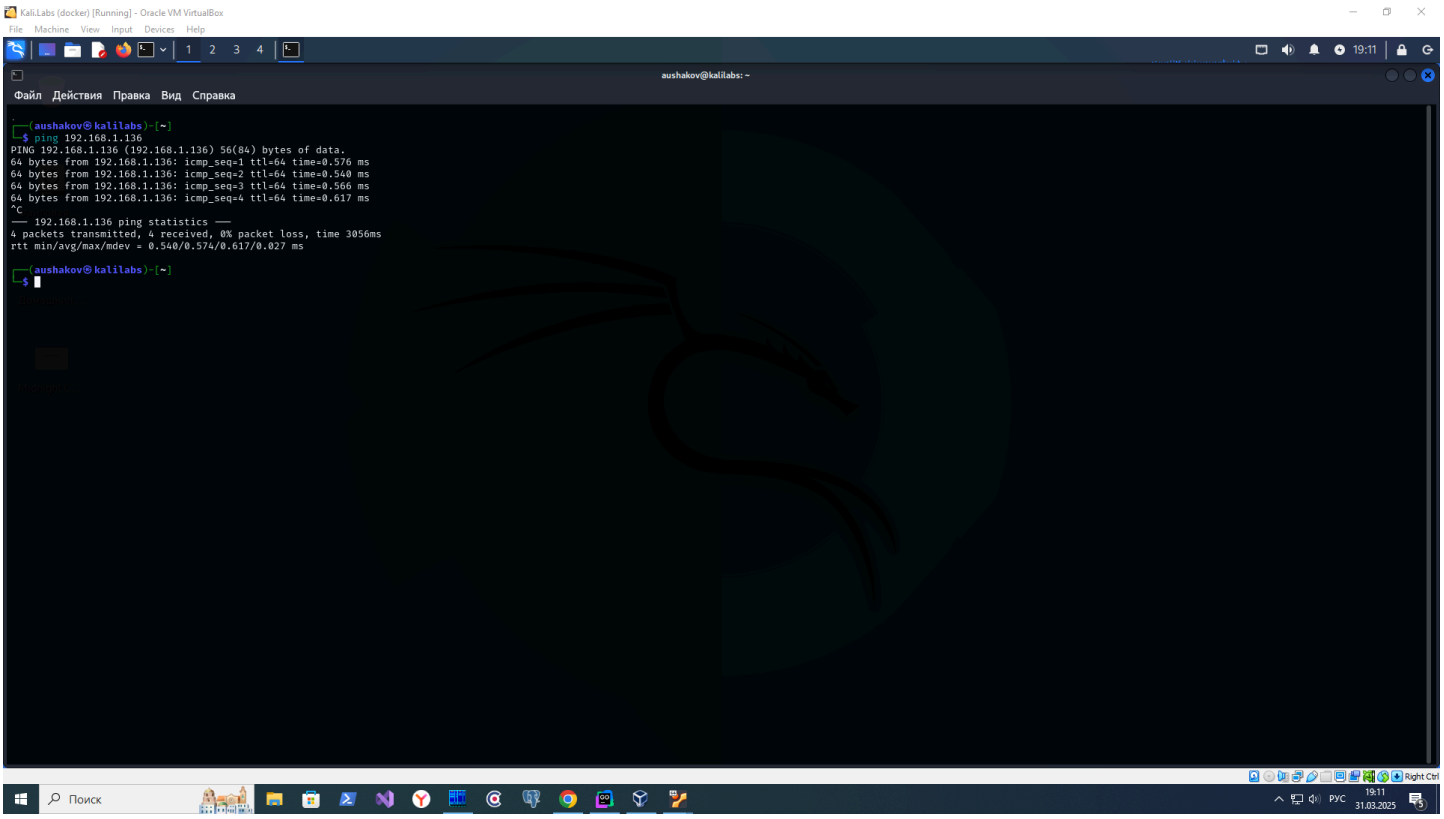


Определяю ip-адрес машины с уязвимостями:

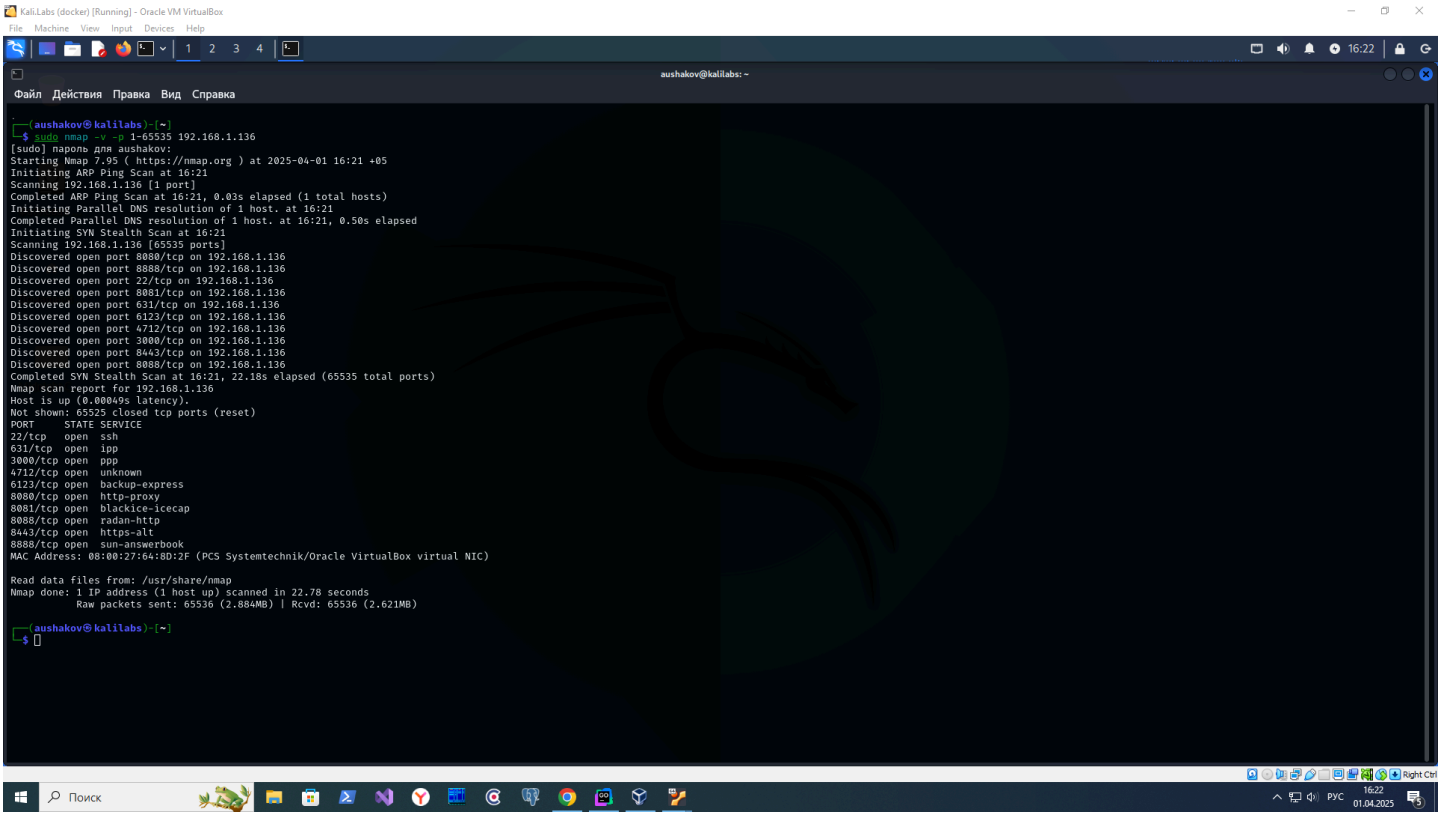


Для этого я использую следующую команду: nmap -v -p 8888 --open 192.168.1.0/24. Видно, что ip-адрес машины с уязвимостями следующий: 192.168.1.136.

Можно еще проверить, что данная машина пингуется:



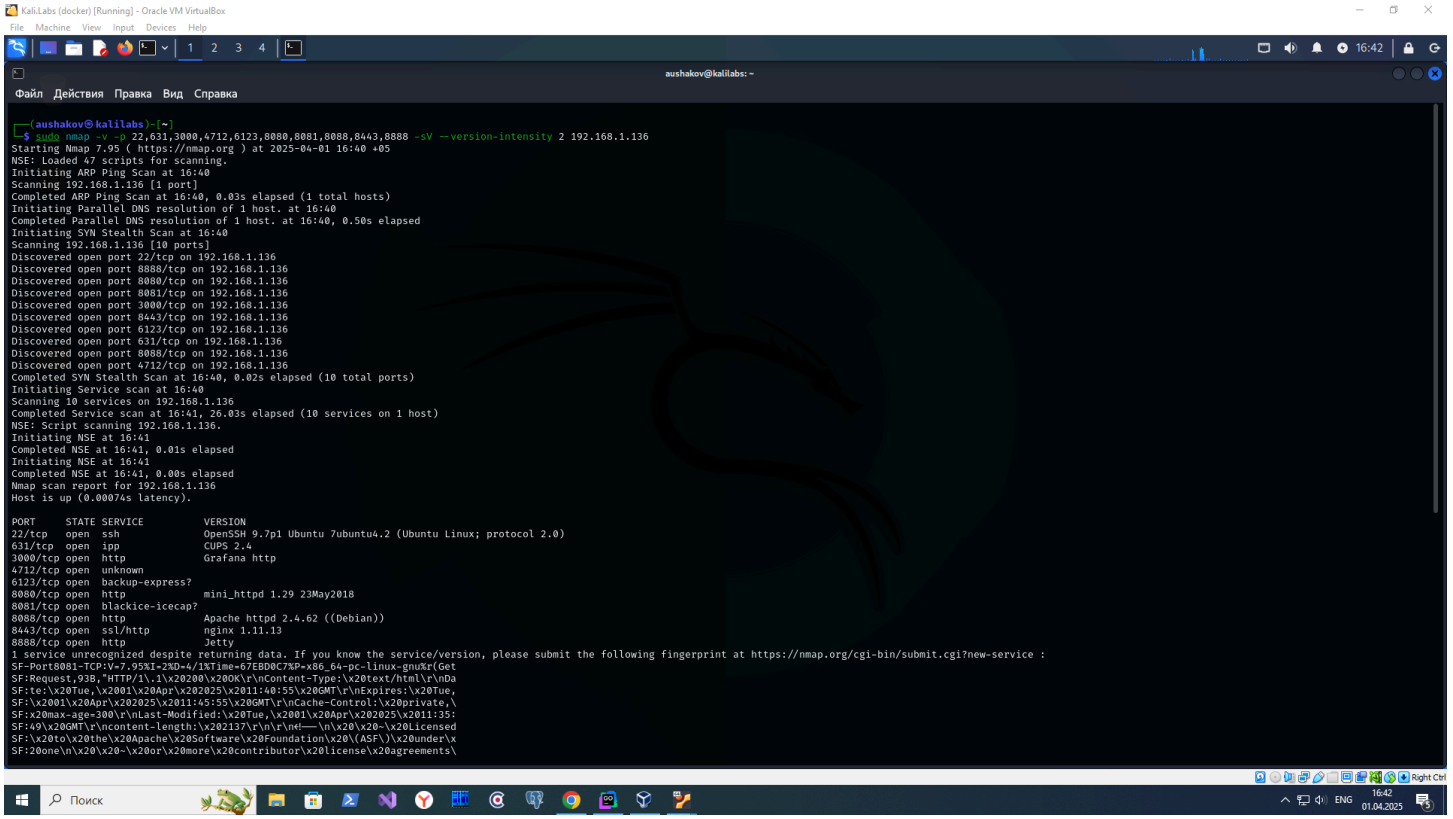
Проверяю с помощью nmap, какие порты открыты с указанием 1-65535 в качестве диапазона проверяемых портов (можно, например, для простоты использовать опцию -F: быстрое сканирование ограниченного количества портов)



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:



Для этого я использую следующую команду:

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

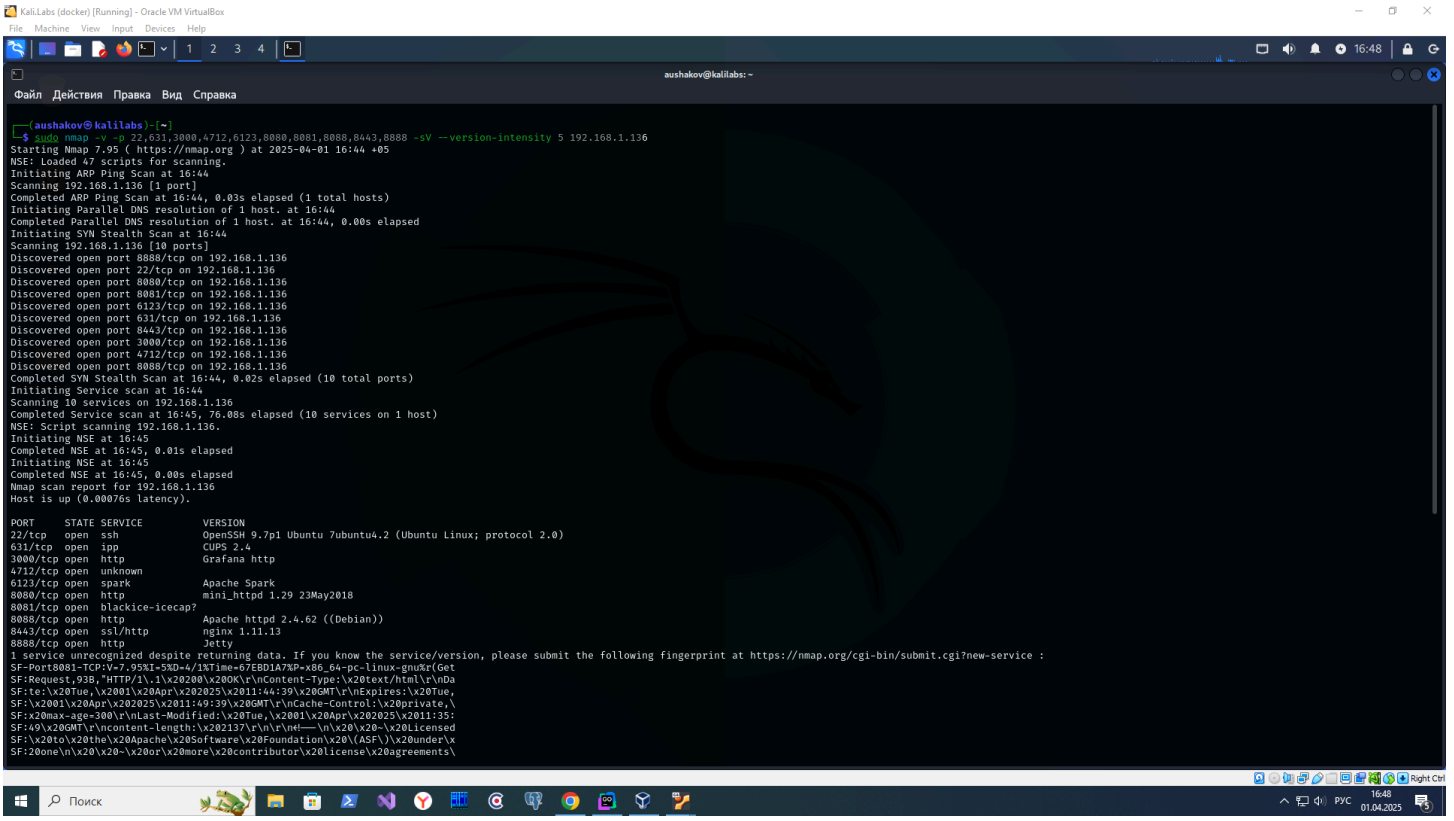
Результаты ее работы следующие (продублировал информацию со скриншота выше):

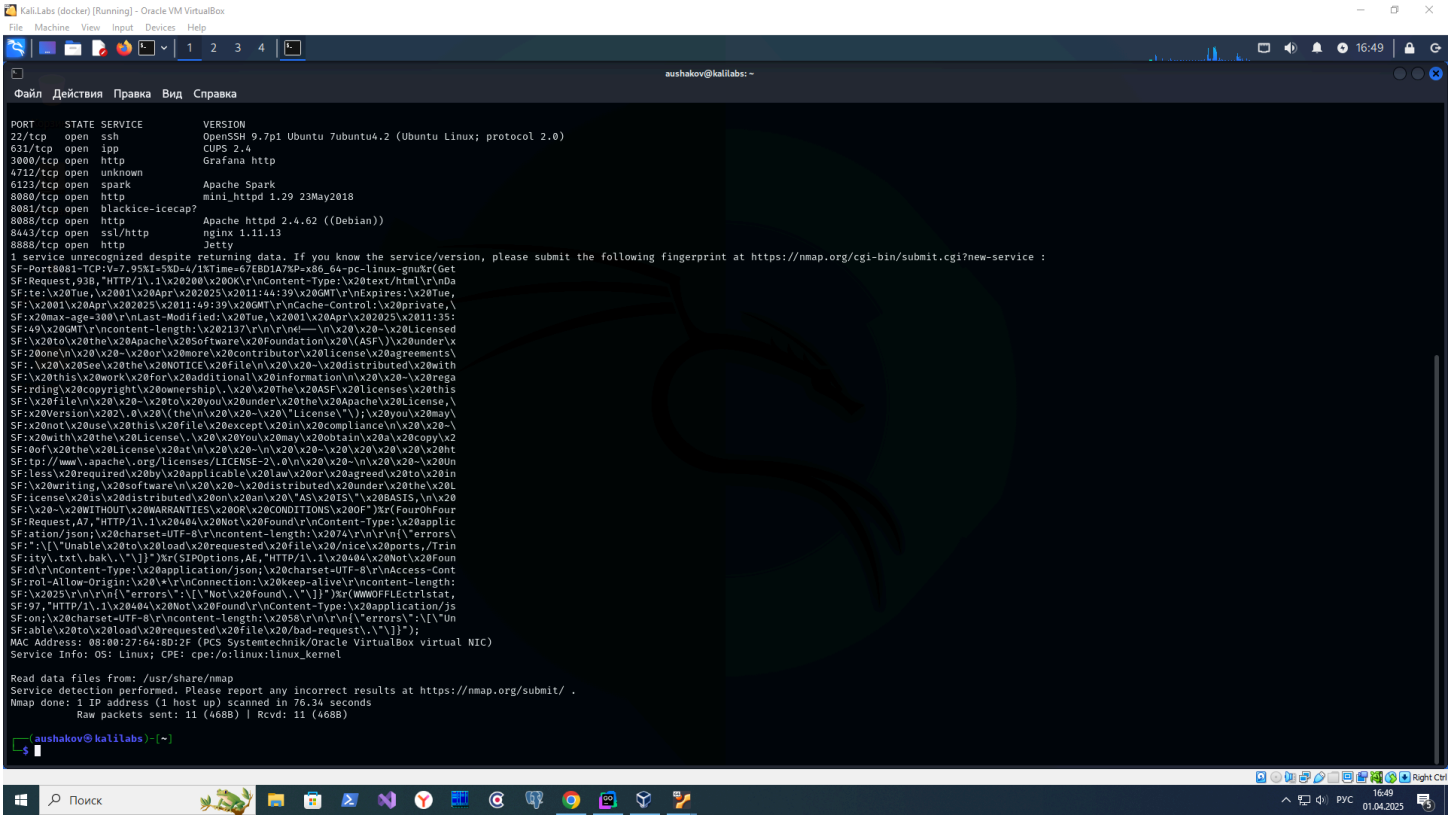
22/tcp open ssh OpenSSH 9.7p1 Ubuntu 7ubuntu4.2 (Ubuntu Linux; protocol 2.0)

631/tcp open ipp CUPS 2.4

3000/tcp open http   Grafana http
4712/tcp open unknown
6123/tcp open 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:





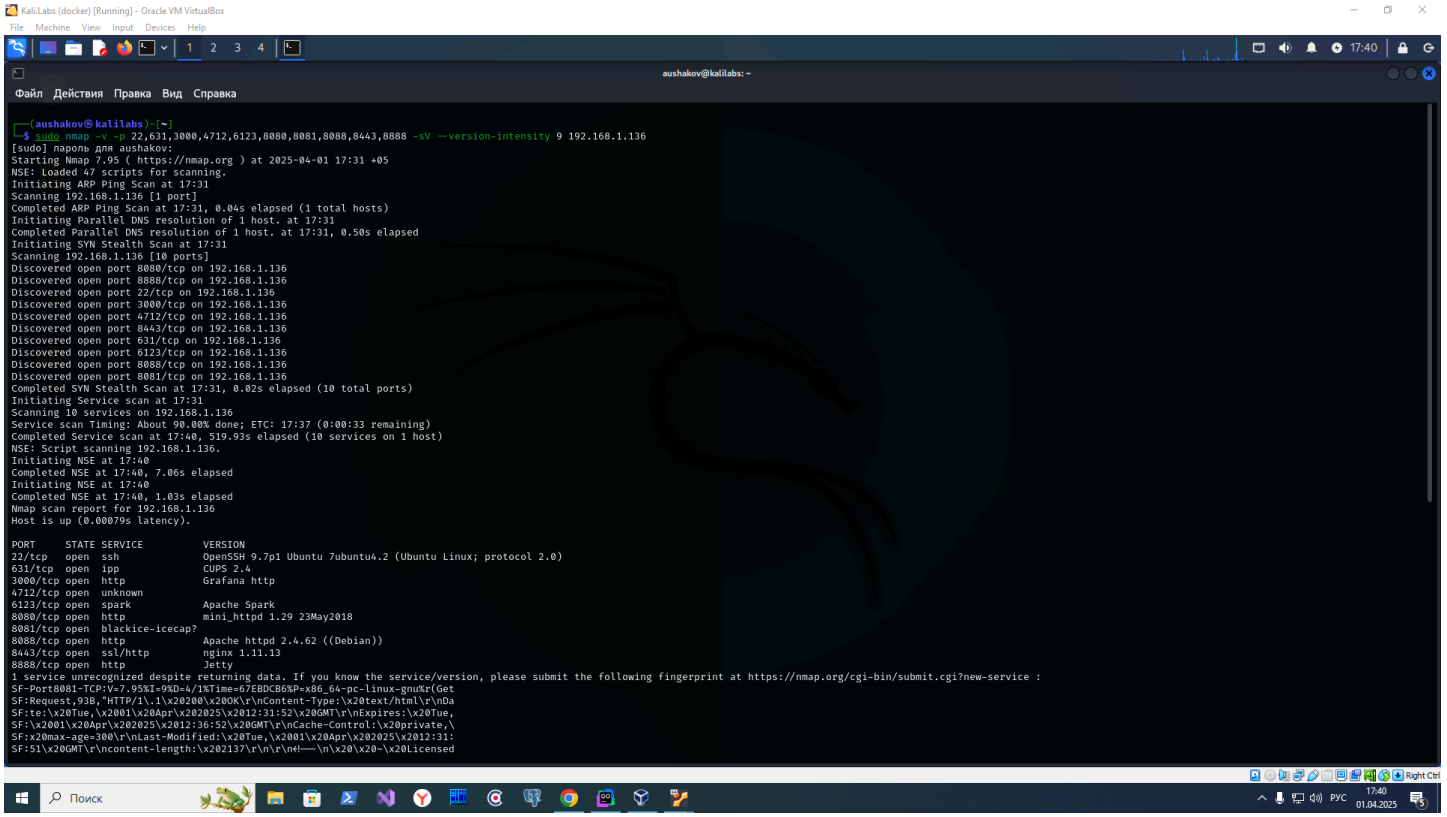
Для этого я использую следующую команду:

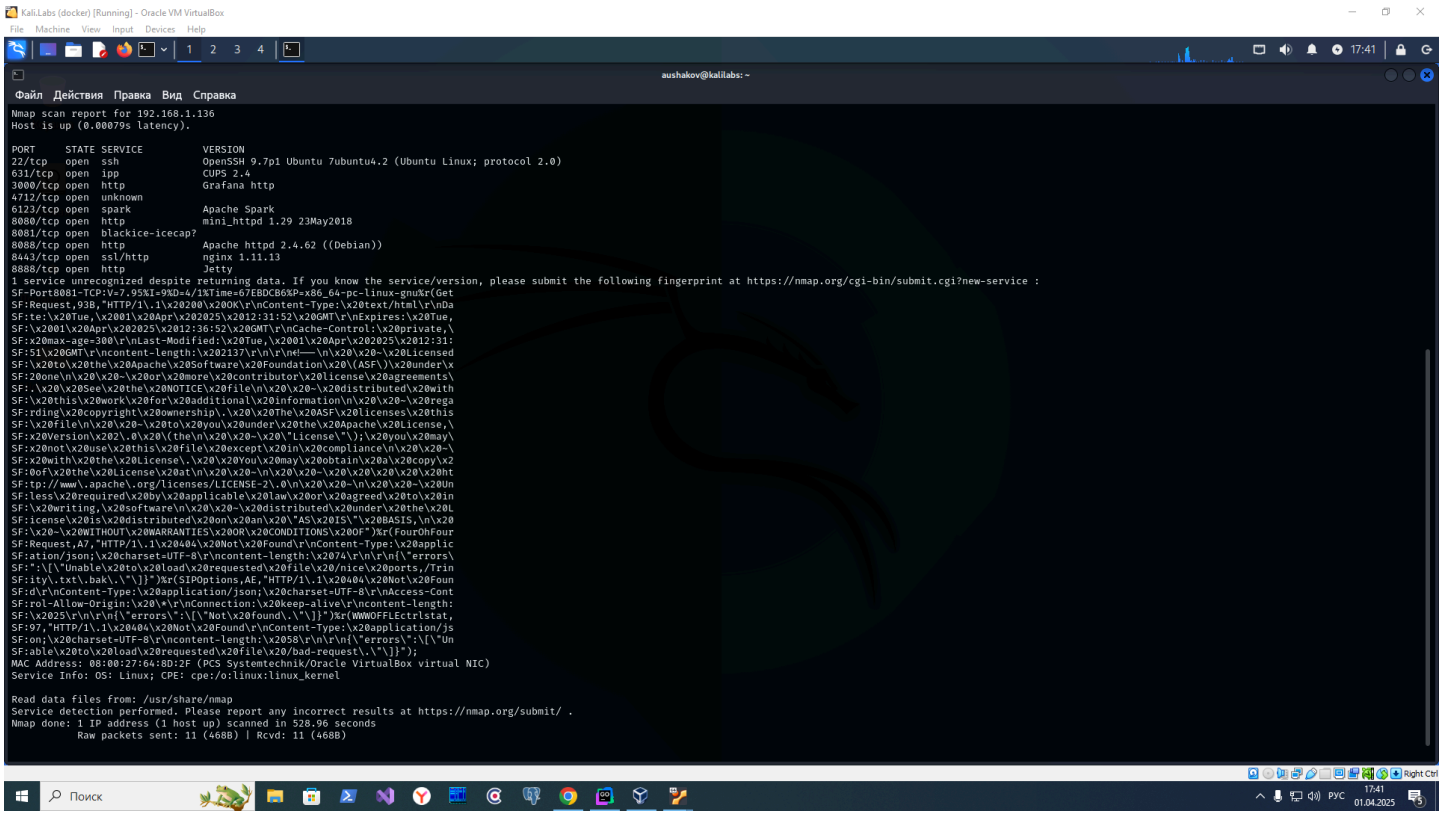
nmap -v -p 22,631,3000,4712,6123,8080,8081,8088,8443,8888 -sV --version-intensity 5 192.168.1.136

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:

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

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.