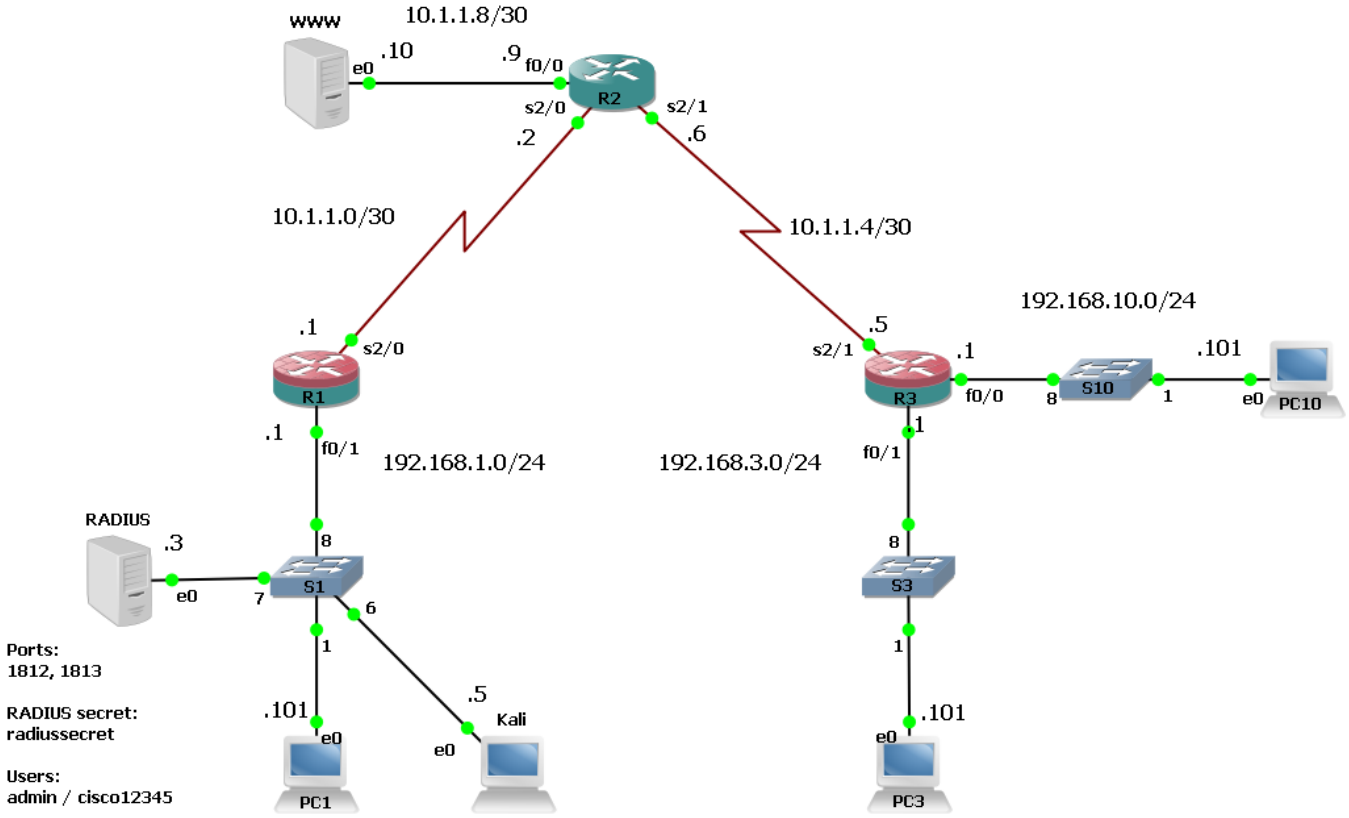
CCNA Security

Лабораторная работа 2

Сканирование сети и узлов

Топология



Описание

Nmap – популярный и мощный инструмент для сканирования сетей и узлов. Nmap работает в режиме командной строки, но для простоты вы будете использовать графическую оболочку zenmap. Вы проведёте базовое сканирование сети и узнаете, какие узлы есть в сети 192.168.1.0/24. Затем вы проведёте более глубокое сканирование маршрутизатора R1.

Если вас заинтересует nmap, то полную документацию всегда можно найти на сайте проекта https://nmap.org/

Также в этой работе вы используете Kali Linux, одну из самых популярных «хакерских ОС».

Если вас заинтересует Kali Linux, то всю информацию можно найти на сайте проекта https://www.kali.org/

Таблица адресации

Устройство	Интерфейс	IPv4-адрес/Маска подсети	Шлюз по умолчанию	Описание
R1	Fa0/1	192.168.1.1/24	-	LAN interface
	Se2/0	10.1.1.1/30	-	WAN interface (To R2)
R2	Se2/0	10.1.1.2/30	-	To R1
	Se2/1	10.1.1.6/30	-	To R3
	Fa0/0	10.1.1.9/30	-	To WWW server
R3	Fa0/1	192.168.3.1/24	-	LAN interface
	Fa0/0	192.168.10.1/24	-	Conference Room
	Se2/1	10.1.1.5/30	-	WAN interface (To R2)
PC1	NIC	192.168.1.101/24	192.168.1.1	-
PC2	NIC	192.168.3.101/24	192.168.3.1	-
PC10	NIC	192.168.10.101/24	192.168.10.1	-
Kali	NIC	192.168.1.5/24	192.168.1.1	-
RADIUS	NIC	192.168.1.3/24	192.168.1.1	-
WWW	NIC	10.1.1.10/24	10.1.1.9	-

Имена пользователей и пароли

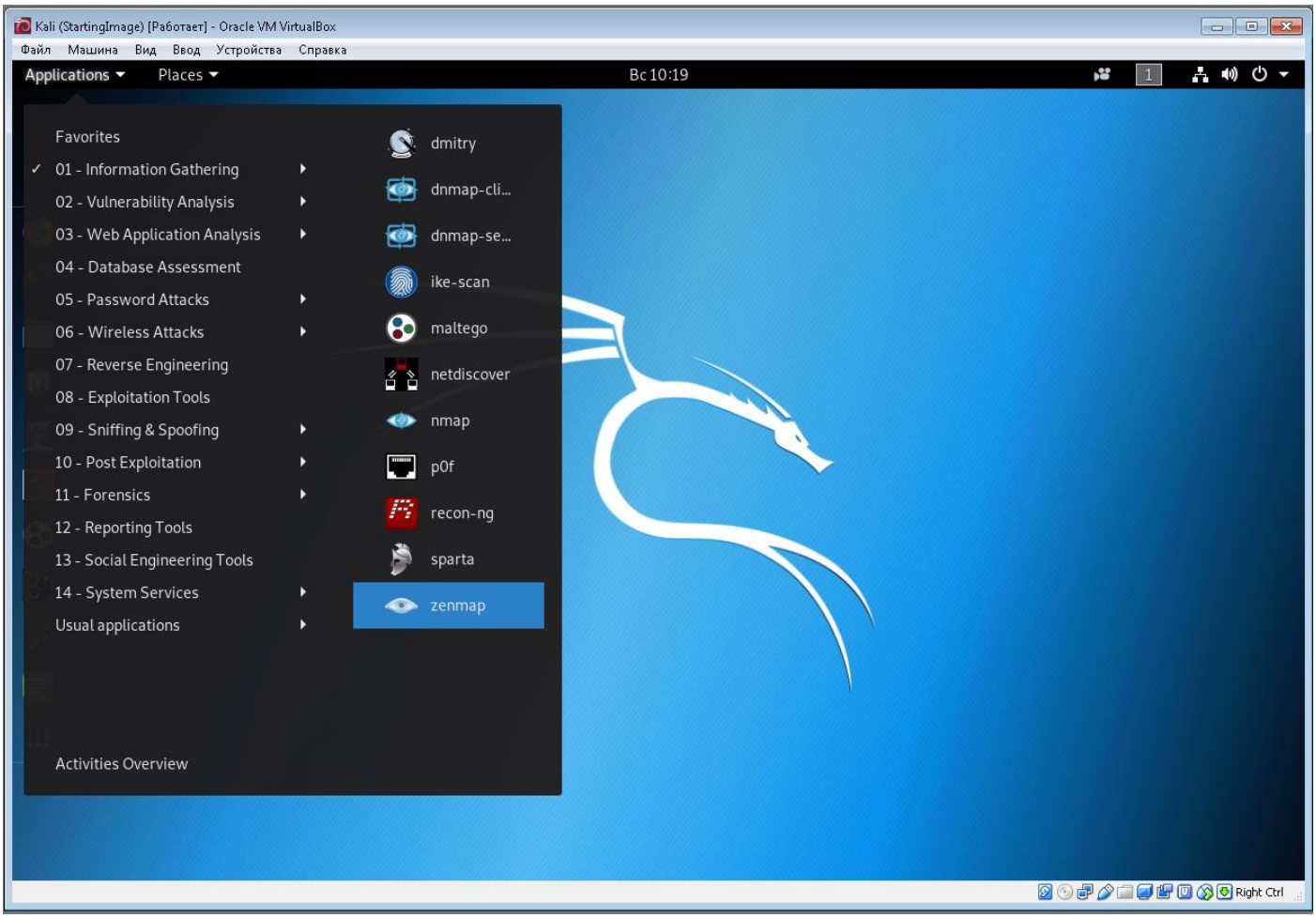
	Console		VTY		Enable
Устройство	Имя пользователя	Пароль	Имя пользователя	Пароль	Пароль
R1	-	-	-	-	-
R2	-	-	-	-	-
R3	-	-	-	-	-

Устройство	Имя пользователя	Пароль
PC1	Student1	1
PC2	Student1	1
PC10	Student1	1
Kali	root	toor

Часть 1: Сканирование сети

1. Войдите в виртуальную машину Kali.

2. Откройте **zenmap** (**Applications -> 01 – Information Gathering -> zenmap**).

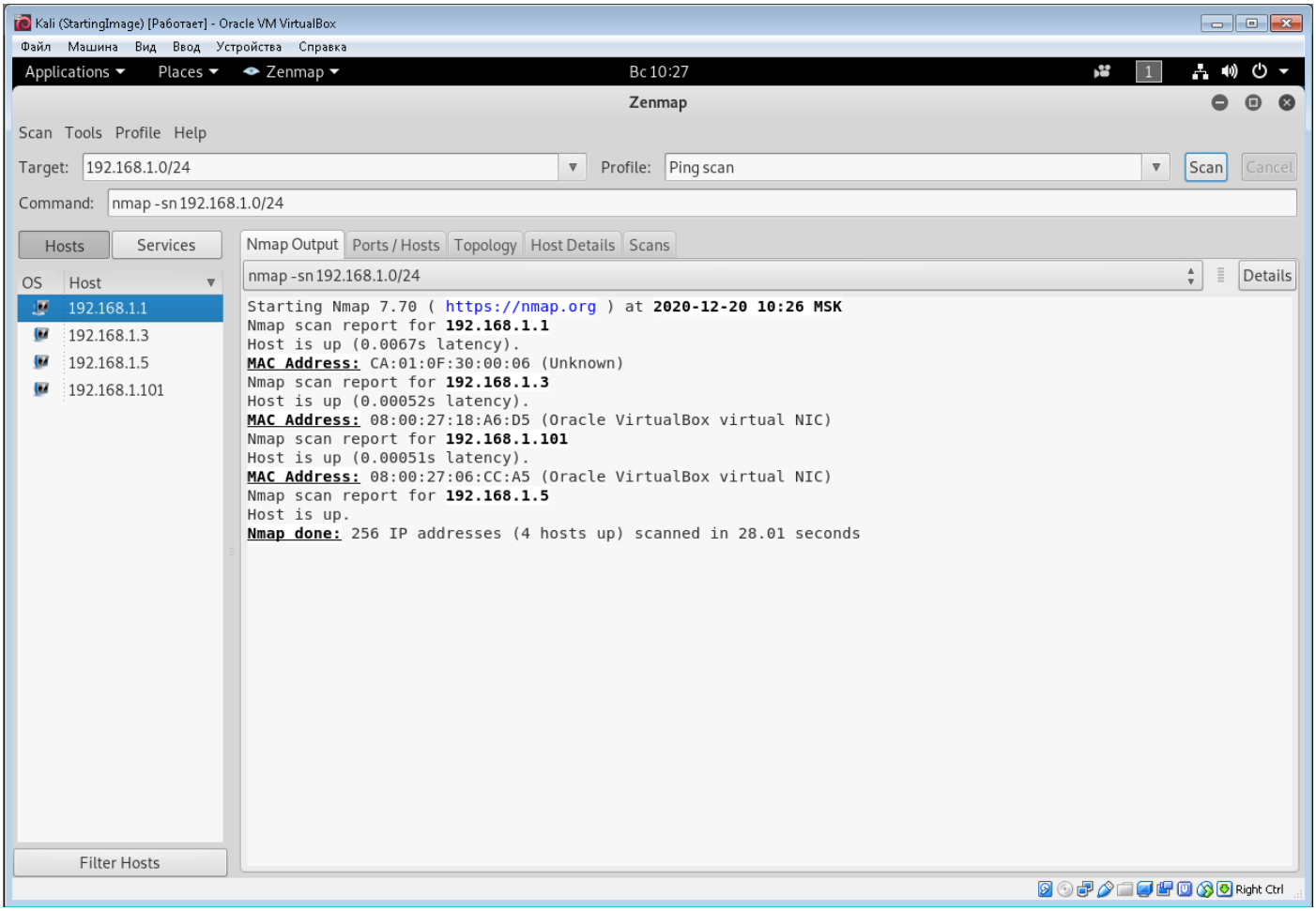


3. Заполните следующие поля

   Target: **192.168.1.0/24**
   Profile: **Ping scan**

4. Нажмите **Scan** и дождитесь результатов сканирования (в средней части окна появится надпись «**Nmap done**»). Сканирование займёт менее минуты.

5. Осмотрите результаты сканирования. Какие узлы были обнаружены помимо самой машины Kali?



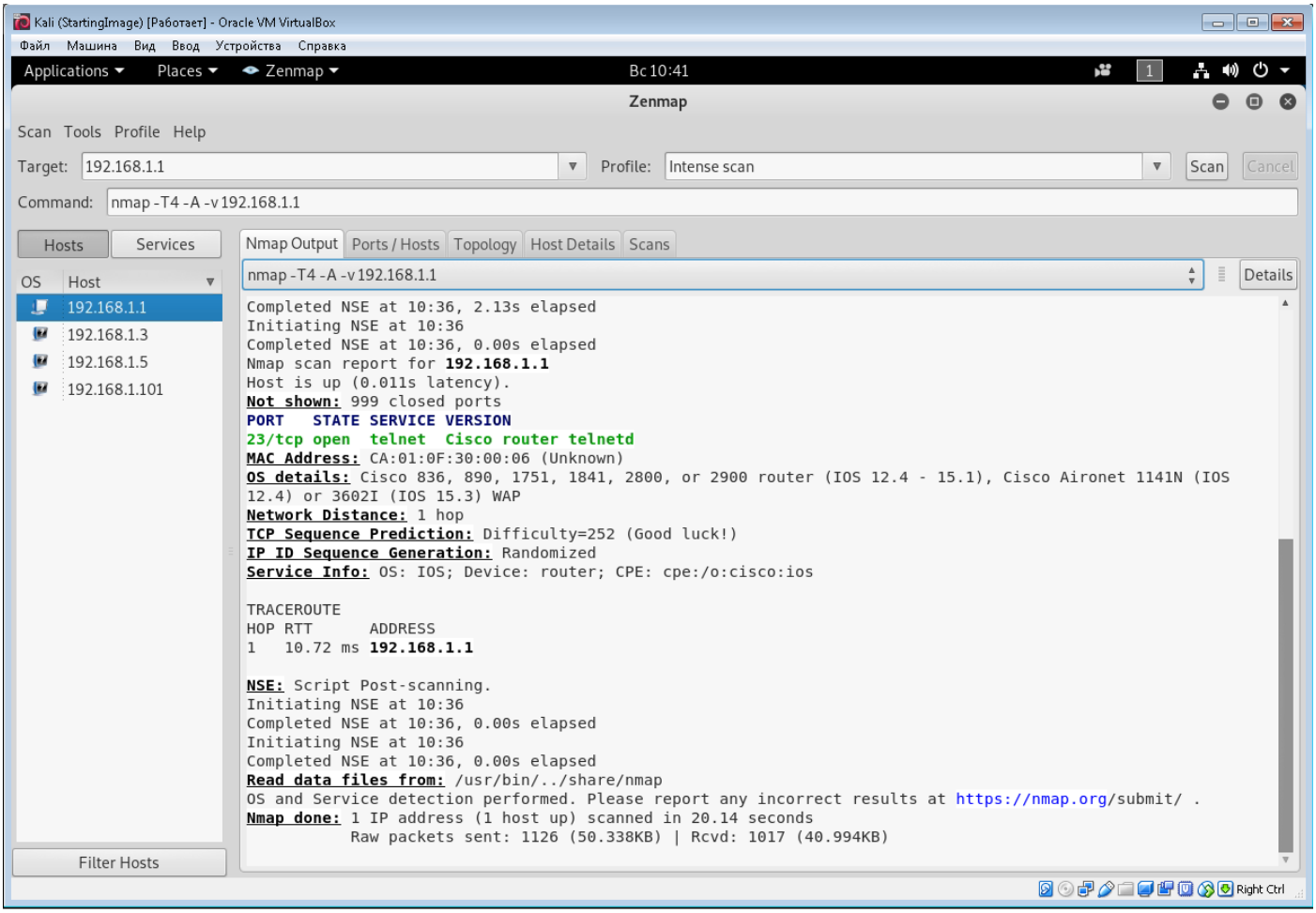
Часть 2: Сканирование узла

Вас заинтересовал узел 192.168.1.1. Выполните более глубокое сканирование именно этого узла. При интенсивном сканировании nmap просканирует 1000 самых распространённых портов протокола TCP и попытается определить название и версию операционной системы на устройстве.

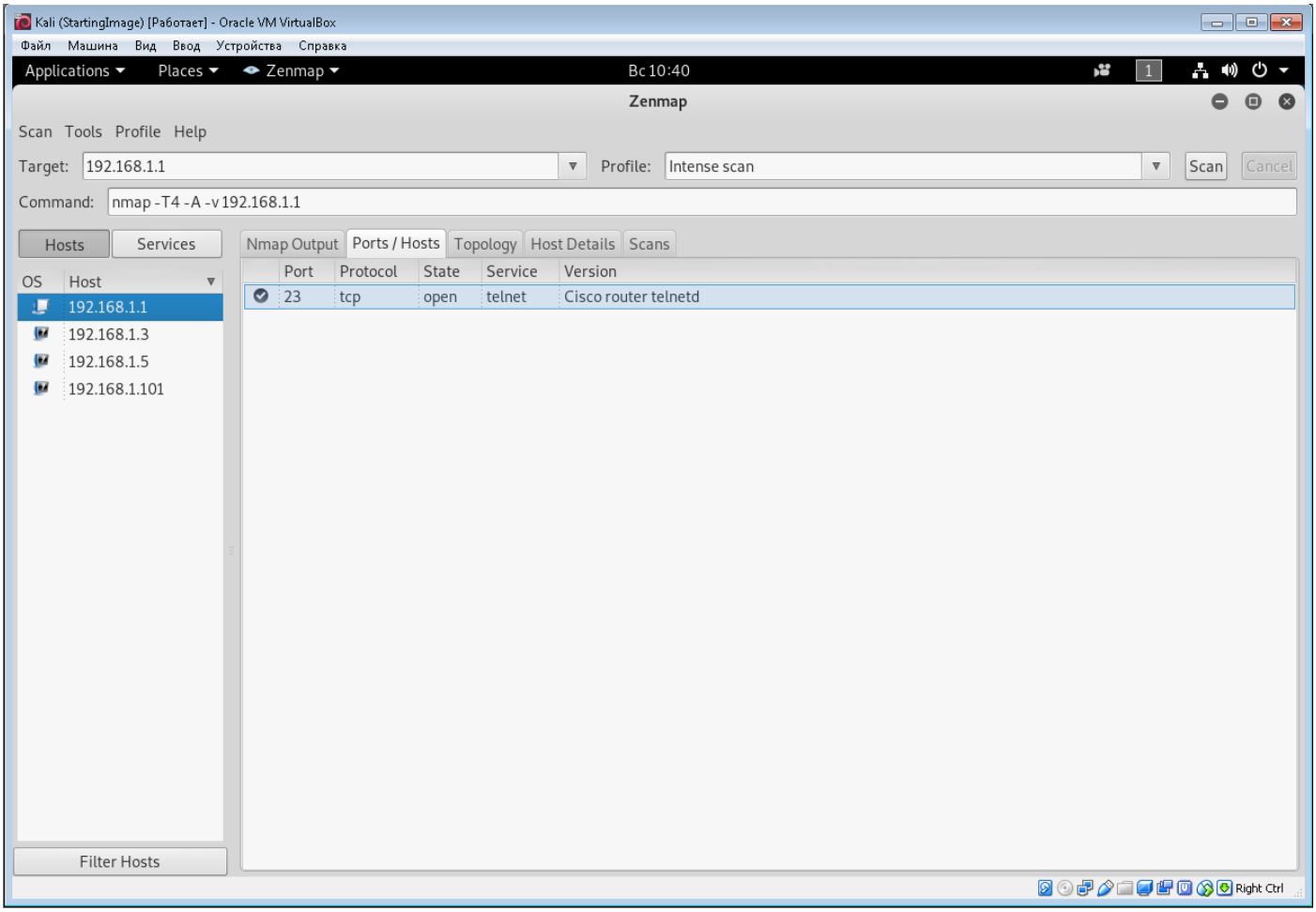
1. Заполните следующие поля

   Target: **192.168.1.1**
   Profile: **Intense scan**

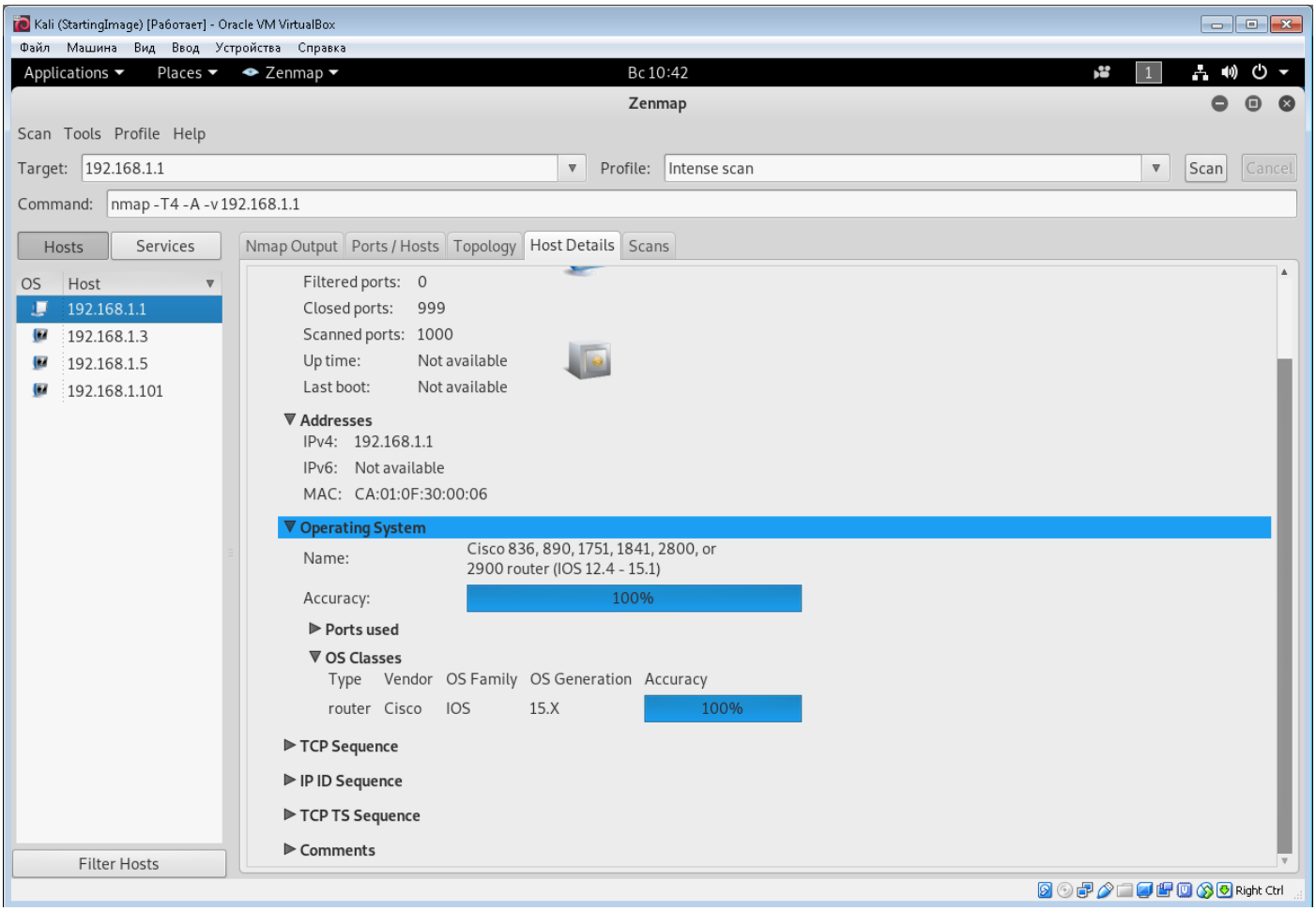
2. Нажмите **Scan** и дождитесь результатов сканирования. Сканирование займёт менее минуты.



3. Перейдите на вкладку **Ports/Hosts**. Какие открытые порты были обнаружены?



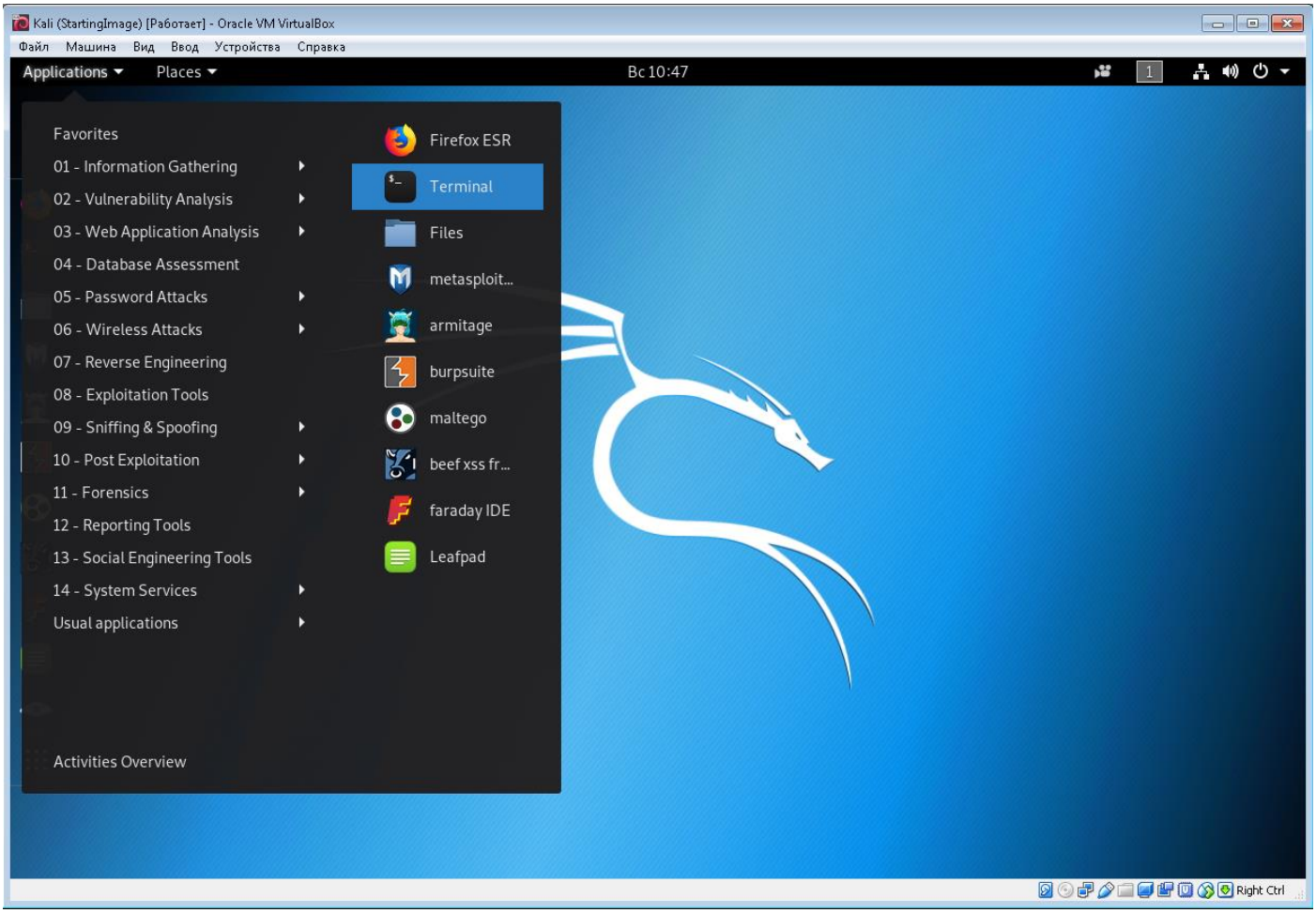
4. Перейдите на вкладку **Host Details**. Какая операционная система была обнаружена? Соответствует ли это действительности?



Часть 3: Попытка входа на устройство по протоколу Telnet

В результате сканирования вы обнаружили на устройстве 192.168.1.1 открытый порт 23 протокола TCP. Это стандартный порт протокола Telnet. Попробуйте подключиться к устройству.

1. Откройте **Terminal (Applications -> Favorites -> Terminal)**.



2. Введите команду **telnet 192.168.1.1**

```
root@kali:~# telnet 192.168.1.1
Trying 192.168.1.1...
Connected to 192.168.1.1.
Escape character is '^]'.
Password required, but none set
Connection closed by foreign host.
```

3. Порт открыт, но подключение не успешно, так как на маршрутизаторе R1 не установлен пароль для vty-линий. Что ж, по крайней мере вы попытались. По умолчанию на устройствах Cisco запрещены удалённые подключения любого рода, однако в нашей лабораторной работе порт протокола Telnet был сознательно открыт.

4. Закройте zenmap и Terminal.