

**МИНОБРНАУКИ РОССИИ**

Федеральное государственное бюджетное образовательное учреждение высшего образования

**«МИРЭА – Российский технологический университет»**

|  |
| --- |
| **РТУ МИРЭА** |
|  |
| **Институт кибербезопасности и цифровых технологий (ИКБ)** |
|  |
| КБ-2 «Прикладные информационные технологии» |

**ОТЧЕТ О ВЫПОЛНЕНИИ ИНДИВИДУАЛЬНОГО ЗАДАНИЯ №2**

**В РАМКАХ ДИСЦИПЛИНЫ «БОЛЬШИЕ ДАННЫЕ»**

Выполнил:

Студент 2-ого курса

Учебной группы БИСО-02-22

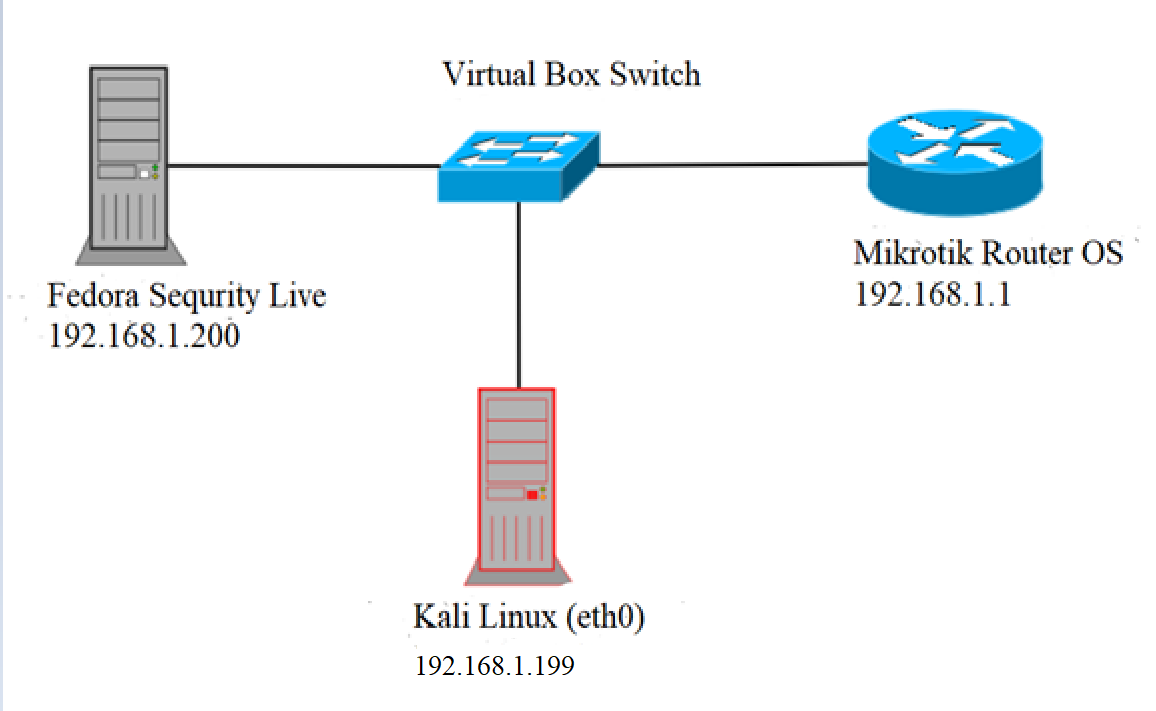
Зубарев В.С.

Оглавление

**Элементы оглавления не найдены.**

# Конфигурация оборудования

Для выполнения практической работы будет использоваться следующая конфигурация



Компьютер злоумышленника – операционная система Kali Linux 2023.4

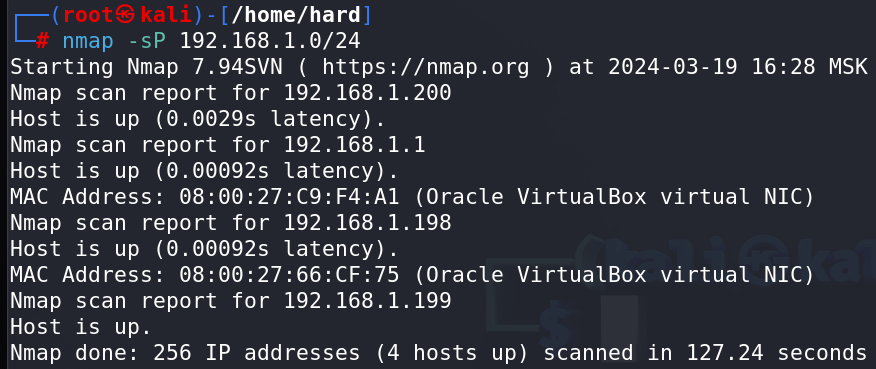
Маршрутиатор – Mikrotik RouterOS

Пользователь локальной сети – Fedora Security Live (FSL)

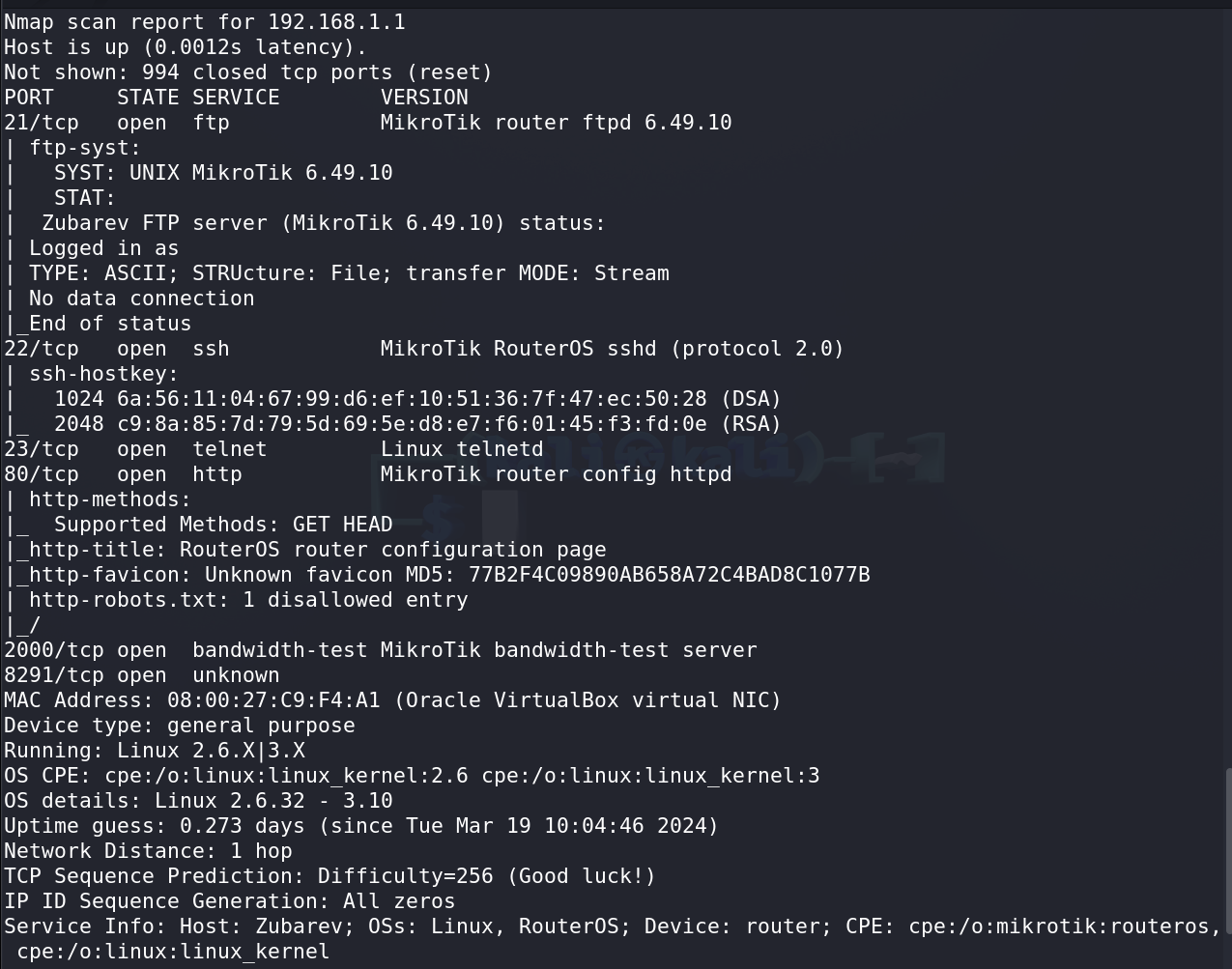
На всех VM сетевые интерфейсы находятся в режиме Internal Net

# Сканирование сети

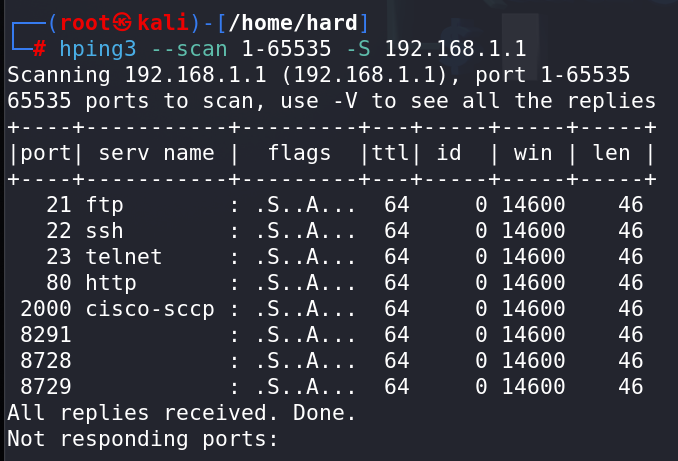
С помощью программы nmap с рабочего места злоумышленника выявите узлы в локальной сети, определите работающие сервисы, их версии. Выявление “живых” хостов в сети с помощью ICMP-сканирования:



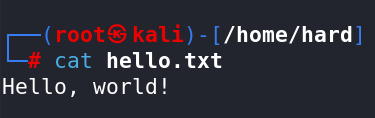
Результаты сканирования сетевых сервисов для узла 192.168.1.1:

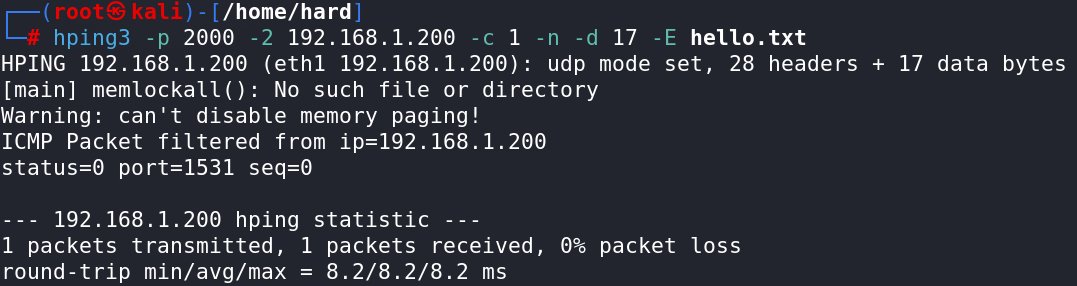


Осуществить SYN-сканирование с помощью утилиты hping3:



С помощью утилиты netcat откроем UDP-порт на узле 192.168.1.199 и проверим с помощью hping3 его работоспособность. Для этого создадим произвольный файл, например, hello.txt Содержимое файла:



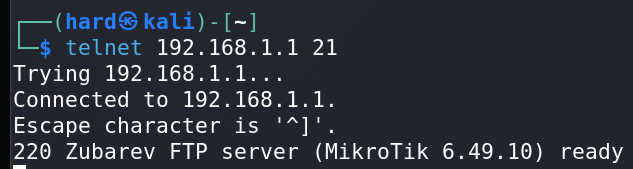




# Осуществление DOS-атаки на сетевой сервис

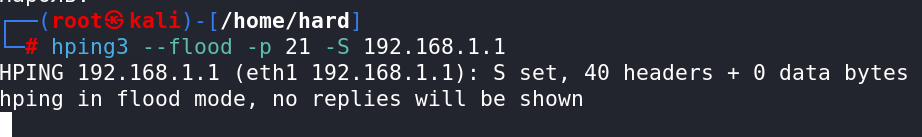
С помощью утилиты hping3 осуществить SYN-flood атаку на FTP-сервис маршрутизатора Mikrotik Исходное состояние – проверить доступность FTP-сервера с TinyCore Linux с помощью telnet:

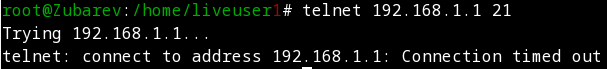
$ telnet 192.168.1.1 21



Запустить DoS-атаку типа SYN-flood:

$ hping3 ­­flood ­p 21 ­S 192.168.1.1





# Выявление и блокирование SYN-flood атаки на устройстве Mikrotik

В Mikrotik добавить правила:

