Министерство науки и высшего образования Российской Федерации Федеральное государственное бюджетное образовательное учреждение высшего образования «Тульский государственный университет»

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

**\БАЗОВЫЕ МЕТОДЫ АКТИВНОГО СБОРА ИНФОРМАЦИИ ОБ УЯЗВИМОСТЯХ ОБЪЕКТА ЗАЩИТЫ**

отчет о   
лабораторной работе №3

по дисциплине

*ПРОГРАММНЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ*

***ВАРИАНТ 13***

|  |  |  |
| --- | --- | --- |
| Выполнила: | ст. гр. 230711 | Павлова В.С. |
| Проверил: | асс. каф. ИБ | Греков М.М. |

Тула, 2023 г.

# **ЦЕЛЬ РАБОТЫ**

**Цель:** ознакомиться с основными методами сканирования сети защищаемых или анализируемых объектов с использованием специализированных средств.

# **ЗАДАНИЕ НА РАБОТУ**

1. Установить NMap или ZenMap.
2. Изучить документацию по базовым опциям NMap, опциям имитации разрыва соединения.
3. Просканировать сайт scanme.org с использованием различных опций NMap.
4. Поискать уязвимости на сайте scanme.org с использованием скриптового движка NMap и базы данных.
5. Найти субдомены сайта scanme.org с использованием скрипта dns-brute.
6. При наличии такой возможности, постараться использовать опции подмены адреса и опции управления пакетами данных, встроенные в среду NMap.

# **ХОД РАБОТЫ**

1. После установки ZenMap отображается следующее окно:

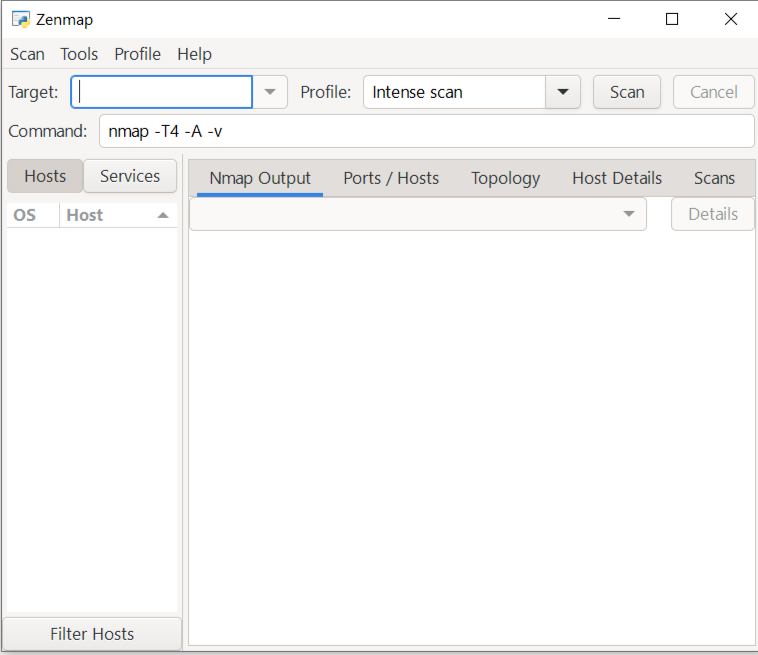
****

Рисунок 1 – Установка программы

1. Результат сканирования ресурса scanme.org

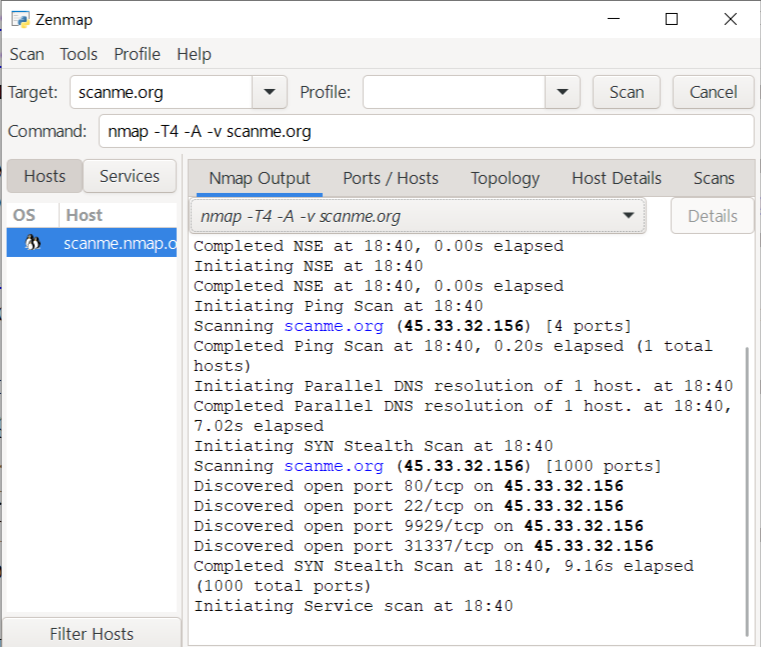


Рисунок 2 – Результат сканирования

1. Поиск уязвимостей на сайте scanme.nmap.org:

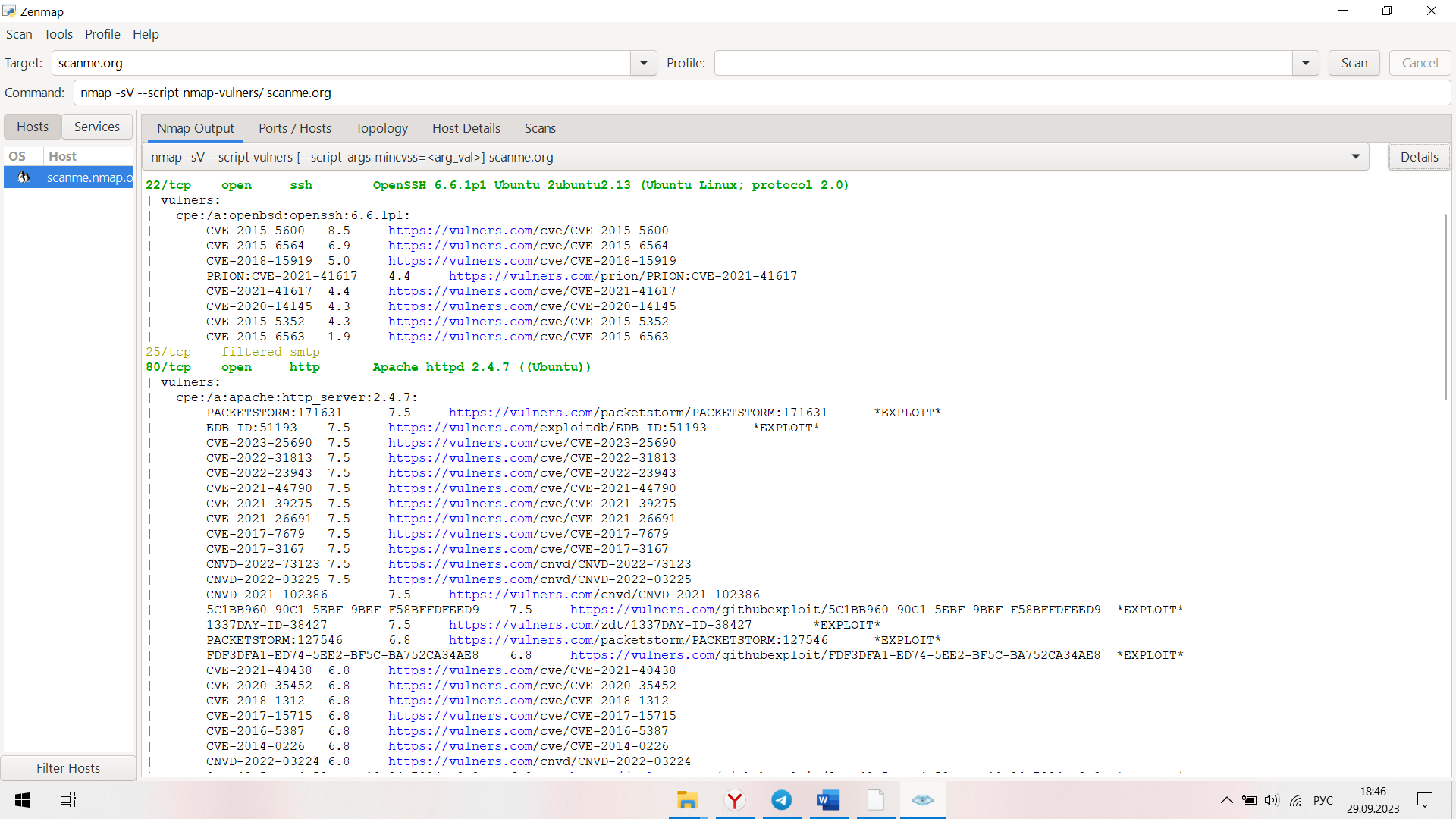


Рисунок 3 – Результат поиска уязвимостей с помощью Nmap-vulners

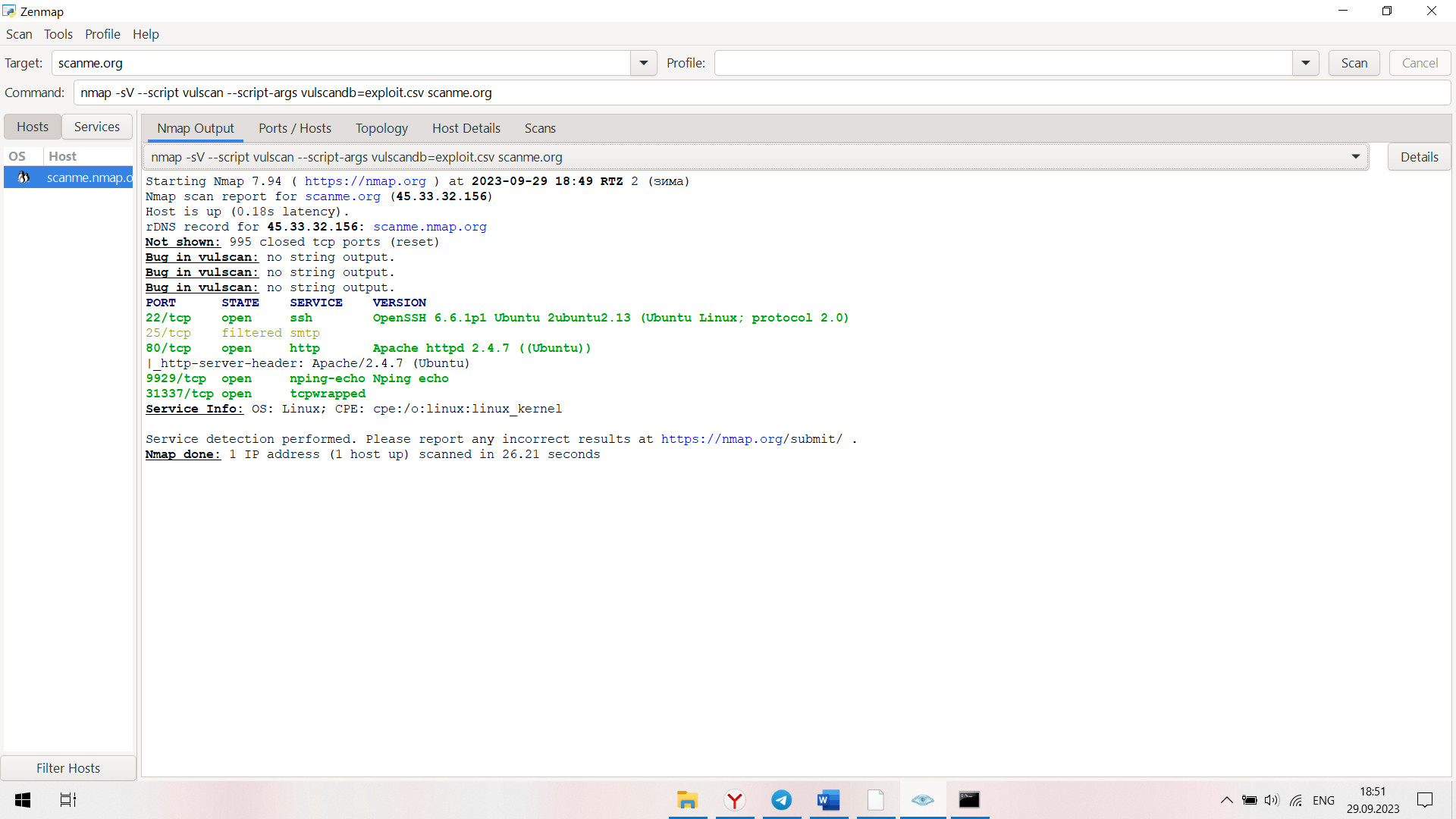


Рисунок 4 – Результат поиска уязвимостей с помощью Nmap-vulscan

1. Результат поиска субдоменов сайта scanme.org с использованием скрипта dns-brute:

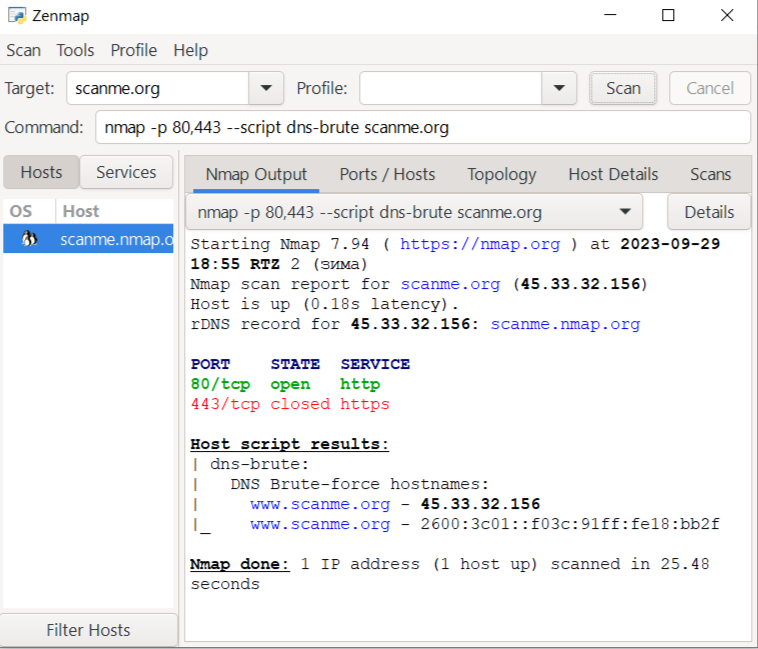


Рисунок 5 – Поиск субдоменов

1. Подмена MAC-адреса с помощью nmap:

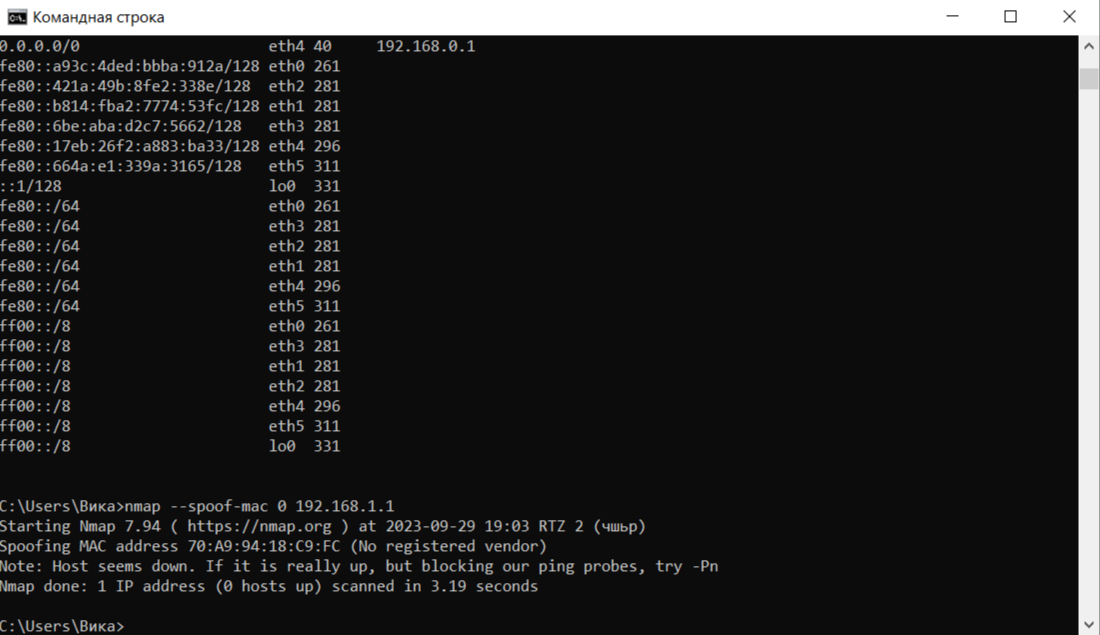


Рисунок 6 – Подмена MAC-адреса

# **ВЫВОД**

В ходе выполнения данной лабораторной работы я ознакомилась с основными методами сканирования сети защищаемых или анализируемых объектов с использованием специализированных средств.