|  |
| --- |
|  |
| МИНОБРНАУКИ РОССИИ |
| Федеральное государственное бюджетное образовательное учреждение  высшего образования  **«МИРЭА – Российский технологический университет»**  **РТУ МИРЭА** |

Институт кибербезопасности и цифровых технологий

КБ-4 «Интеллектуальные системы информационной безопасности»

Отчет по практической работе №7

по дисциплине: «Управление информационной безопасностью»

**Выполнил**:

Студент группы ББМО-02-22

Кузьмин Владимир Дмитриевич

**Проверил**:

Пимонов Роман Владимирович

Москва 2023

Содержание

[Задание на практическую работу 3](#_Toc154149314)

[1. Сканирование сети с помощью Nmap 4](#_Toc154149315)

[2. Сканирование сети с помощью OpenVAS 7](#_Toc154149316)

[3. Анализ безопасности системы с помощью Metasploit 9](#_Toc154149317)

[Заключение 13](#_Toc154149318)

# Задание на практическую работу

**Цель работы**: Активное тестирование защищенности информационных систем.

**Задачи**:

1. Сканирование сети с помощью Nmap;
2. Сканирование сети с помощью OpenVAS;
3. Анализ безопасности системы с помощью Metasploit.

# 1. Сканирование сети с помощью Nmap

Проведем операции по сканированию сети. Начнем с поиска узлов в подсети (рисунок 1).

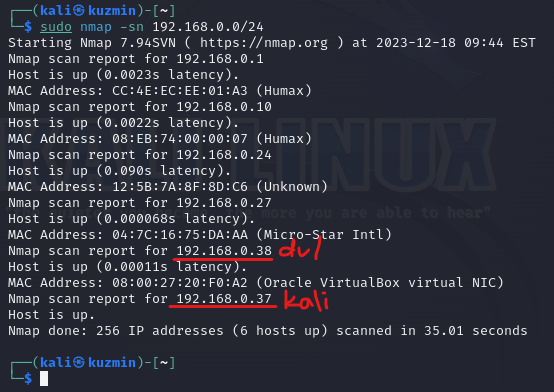


Рисунок 1 – Поиск узлов

Затем просканируем конкретный узел с целью выявления рабочих сервисов и портов, по которым они выходят наружу (рисунок 2), а также с целью определения операционной системы узла (рисунок 3).

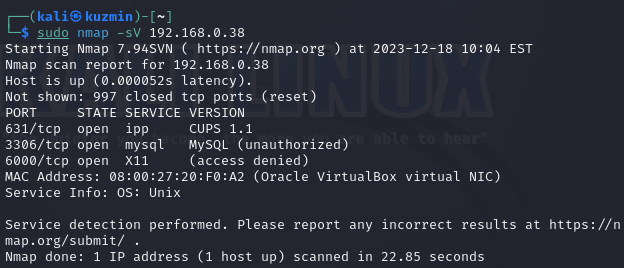


Рисунок 2 – Запрос по сервисам

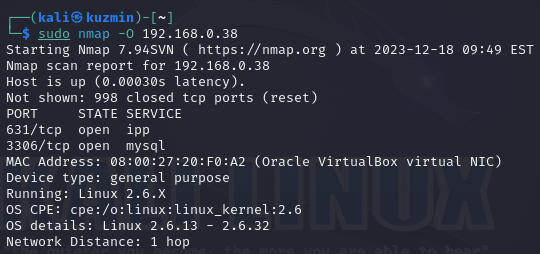


Рисунок 3 – Запрос по операционной системе

После чего попробуем просканировать узел на наличие потенциальных угроз безопасности (рисунок 4).

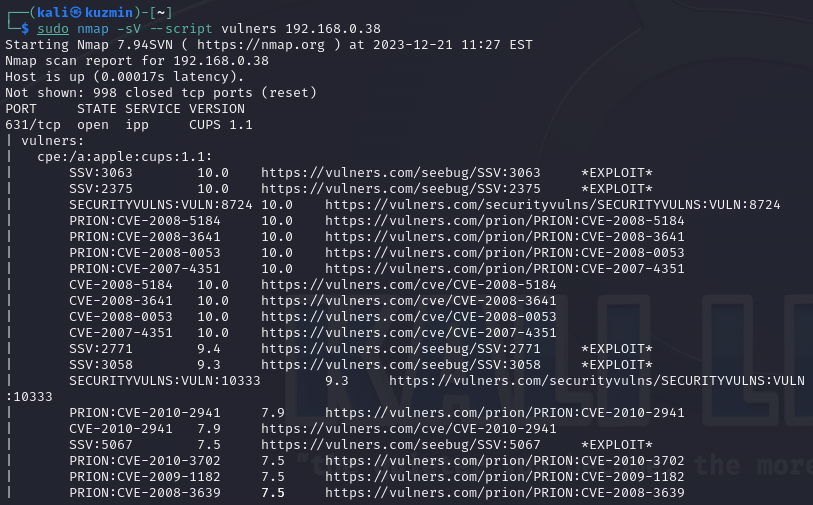


Рисунок 4 – Поиск уязвимостей

# 2. Сканирование сети с помощью OpenVAS

Проведем операции по сканированию сети. Создадим задачу на сканирование нашего целевого узла (рисунок 5).

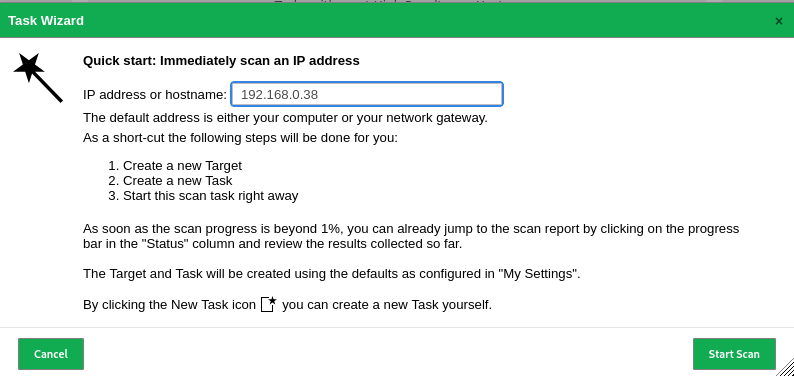


Рисунок 5 – Создание задачи

Посмотрим, что мы получили в отчете по итогам сканирования узла (рисунки 6-7).

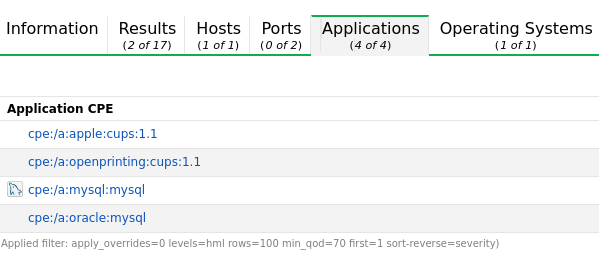


Рисунок 6 – Обнаруженные приложения на узле

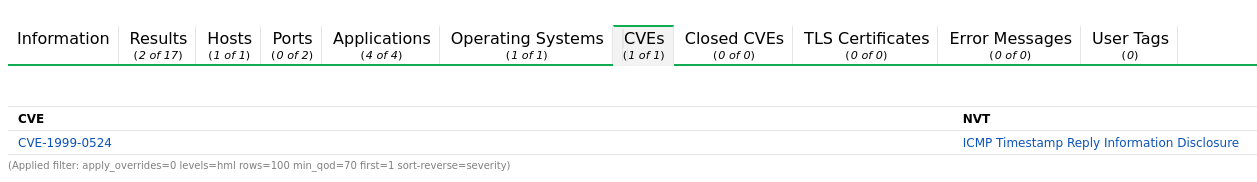


Рисунок 7 – Обнаруженные CVE на узле

Посмотрим описание найденной уязвимости в представлении NVT (рисунок 8).



Рисунок 8 – Сводка по найденной уязвимости

В сравнении с nmap, OpenVAS нашел гораздо меньше уязвимостей, что связанно, в первую очередь, с базовым скриптом и базовой базой уязвимостей, которые участвуют в сканировании. Преимуществом OpenVAS, в данном случае, является функционал по визуализации и настройки расписания сканирований, что будет полезным при постоянном мониторинге узлов в сети на предмет возможных уязвимостей.

# 3. Анализ безопасности системы с помощью Metasploit

Первым делом поднимем сервис SSH, с целью повышения количества возможных уязвимостей (рисунок 9).

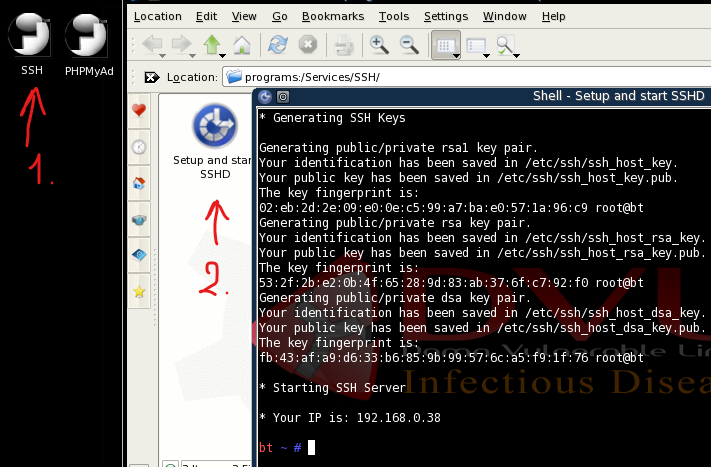


Рисунок 9 – Запуск сервиса SSH

Затем запустим консоль утилиты Metasploit, предварительно обновив базу знаний утилиты (рисунок 10).

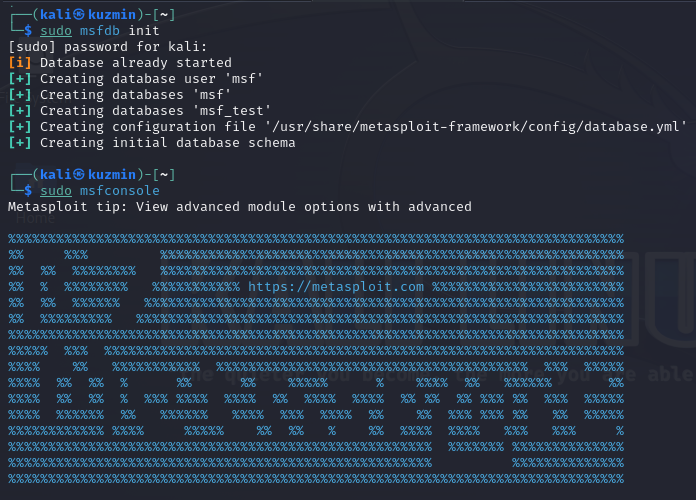


Рисунок 10 – Обновление и запуск

Посмотрим какие функциональные возможности нам предлагает утилита в отношении SSH (рисунок 11).

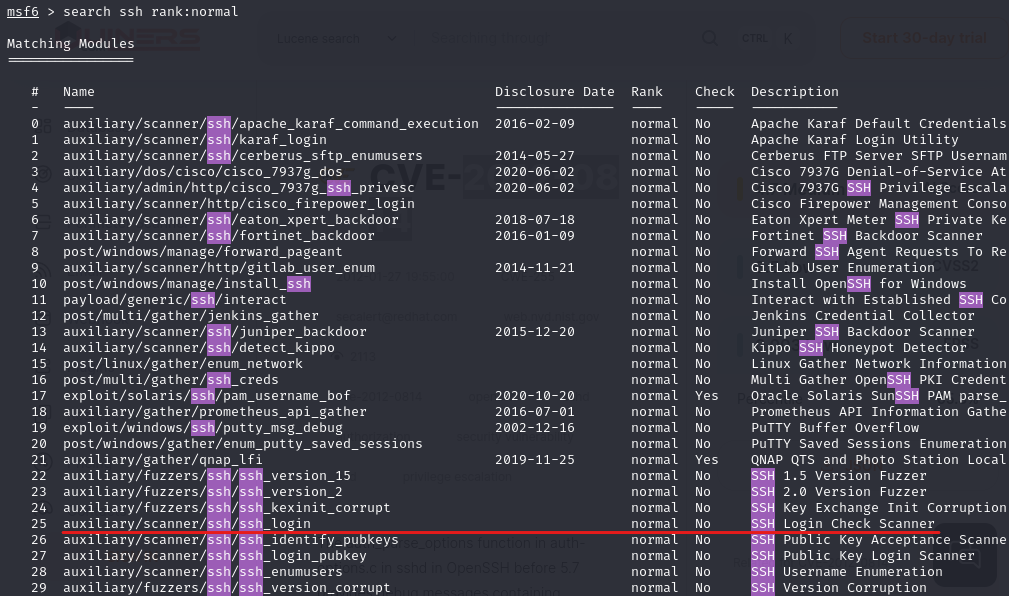


Рисунок 11 – Поиск вектора

Остановимся на самом простейшем варианте – сканере логина. Посмотрим описание данной функции (рисунок 12).

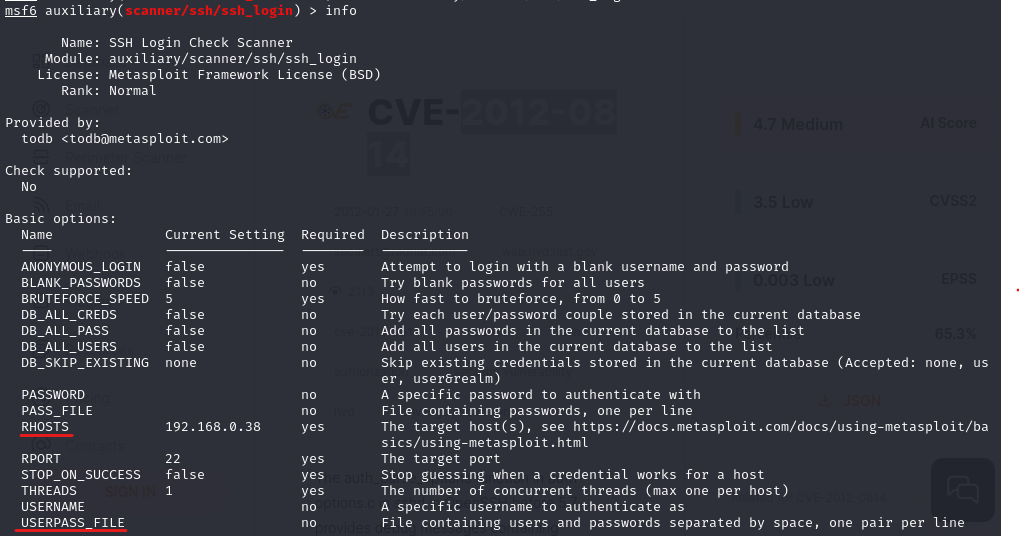


Рисунок 12 – Описание

Из представляемых функцией опций нам потребуется только указание целевого узла и подключение словаря в формате «логин пароль». Укажем необходимые опции и запустим (рисунок 13).

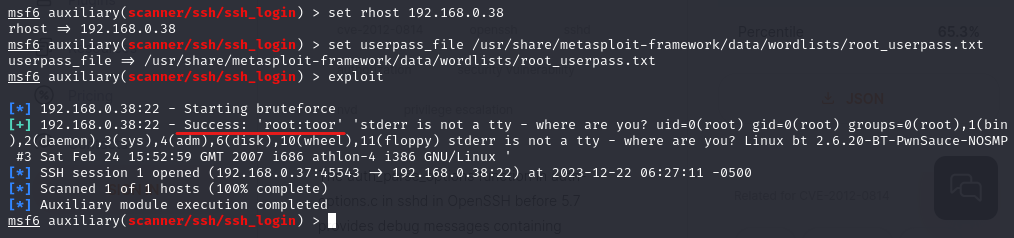


Рисунок 13 – Подготовка и запуск

В мгновение ока было получено совпадение с кредами целевого узла для подключения по SSH. Данная уязвимость имеет идентификатор CVE-1999-0502 и подразумевает, что для сервиса SSH установлена учетная запись Unix, которая имеет пароль по умолчанию, нулевой, пустой или отсутствующий.

CVE-1999-0502 относится к уязвимости в протоколе управления передачей (TCP) стека протоколов TCP/IP, которая также может привести к отказу в обслуживании (DoS). Уязвимость связана с возможностью переполнения буфера в функции recv() в коде BSD.

Рекомендации по устранению этой уязвимости следующие:

1. Отключите учетную запись root или задайте ей сложный пароль.
2. Используйте авторизацию по приватному ключу.
3. Используйте двухфакторную аутентификацию для SSH.
4. Убедитесь, что на вашем сервере и клиентских машинах установлены последние обновления безопасности для операционной системы и приложений.
5. Обновите программное обеспечение, использующее уязвимые функции, до последних версий, в которых уязвимость была исправлена.
6. Если это невозможно, отключите использование уязвимых функций или измените конфигурацию, чтобы избежать их использования. Например, если уязвимость связана с функцией recv(), можно попробовать использовать альтернативные функции для чтения данных.
7. Ограничьте доступ к уязвимым функциям или службам, которые их используют, только для доверенных источников и пользователей.
8. Используйте системы предотвращения вторжений и брандмауэры для защиты от возможных атак, использующих уязвимость.
9. Постоянно следите за обновлениями безопасности и новыми угрозами, связанными с этой уязвимостью, и своевременно применяйте необходимые исправления.

# Заключение

В ходе выполнения практической работы были выполнены необходимые задачи, а именно:

1. Сканирование сети с помощью Nmap;

2. Сканирование сети с помощью OpenVAS;

3. Анализ безопасности системы с помощью Metasploit.

Соответственно, цель работы – настройка параметров системы обнаружения атак, была достигнута.