|  |
| --- |
|  |
| 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 №3.2

по дисциплине: «Управление информационной безопасностью»

**Выполнил**:

Студент группы ББМО-01-22

Загороднов Е.А.

**Проверил**:

Пимонов Р.В.

Москва 2023

**СОДЕРЖАНИЕ**

[ЗАДАНИЕ 3](#_Toc154603020)

[1. Сканирование сети с помощью Nmap 4](#_Toc154603021)

[2. Сканирование сети с помощью OpenVAS 7](#_Toc154603022)

[3. Анализ безопасности системы с помощью Metasploit 10](#_Toc154603023)

[РЕКОМЕНДАЦИИ 14](#_Toc154603024)

[ЗАКЛЮЧЕНИЕ 16](#_Toc154603025)

# **ЗАДАНИЕ**

**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;
4. Составить рекомендации по устранению выявленной уязвимости.

# **1. Сканирование сети с помощью Nmap**

Давайте выполним процедуры по сканированию сети, начиная с выявления узлов в пределах подсети. Этот этап позволит нам обнаружить активные устройства и определить их характеристики. Затем мы сможем провести более глубокий анализ структуры сети, выявив ее топологию и потенциальные уязвимости. В целом, эти операции по сканированию сети предоставят ценную информацию о состоянии и безопасности сетевой инфраструктуры. Процесс поиска узлов показан на рисунке 1

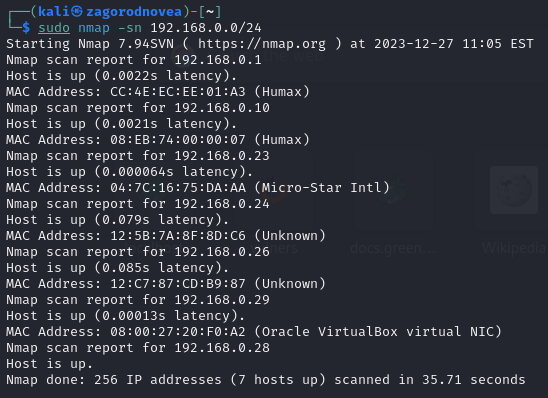


Рисунок 1 – Поиск узлов

После этого мы проведем сканирование определенного узла с целью выявления активных сервисов и портов, через которые они взаимодействуют с внешней средой. Сканирование узла с целью выявления активных сервисов и портов показано на рисунке 2.

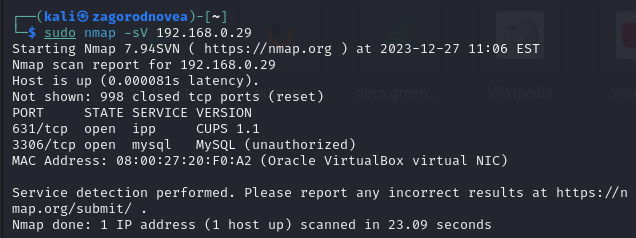


Рисунок 2 – Сканирование узла с целью выявления активных сервисов и портов

Также проведем сканирование с целью определения операционной системы, работающей на данном узле . Этот этап анализа позволит более детально изучить функциональные характеристики узла, что важно для определения его роли и возможных уязвимостей. Полученная информация будет полезна при разработке стратегий управления и обеспечения безопасности в сети. Сканирования с целью определения операционной системы показано на рисунке 3.

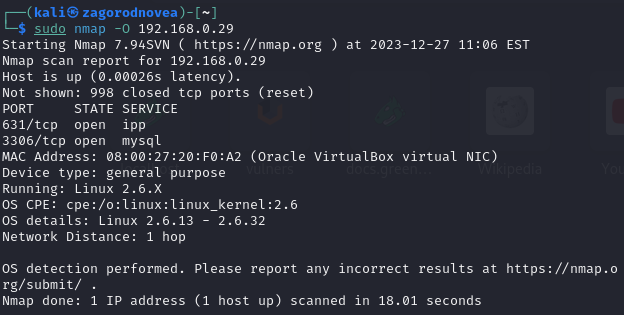


Рисунок 3 – Сканирования с целью определения операционной системы

Затем мы предпримем попытку провести сканирование узла для выявления возможных угроз безопасности. Попытка проведения сканирование узла для выявления возможных угроз безопасности показана на рисунке 4.

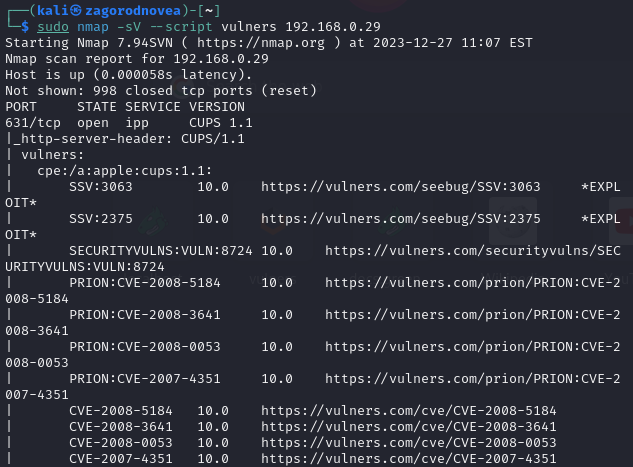


Рисунок 4 – Cканирование узла для выявления возможных угроз безопасности

Этот этап необходим для идентификации потенциальных уязвимостей в сетевой инфраструктуре, что позволит разработать соответствующие меры по их предотвращению или устранению. Анализ безопасности узла является ключевым шагом в обеспечении целостности и защиты сетевой среды от возможных атак или несанкционированного доступа.

# **2. Сканирование сети с помощью OpenVAS**

Давайте выполним процедуры по сканированию сети и инициируем задачу на сканирование выбранного целевого узла. Этот шаг позволит нам систематически изучить структуру сети, выявив ее компоненты и параметры. Задача на сканирование узла также обеспечит более детальное исследование его характеристик, включая активные порты, сервисы и другие важные параметры, необходимые для полного понимания его роли в сети. В результате мы получим ценные данные, которые могут быть использованы для оптимизации и улучшения безопасности сетевой инфраструктуры. Процесс создания задачи показан на рисунке 5.

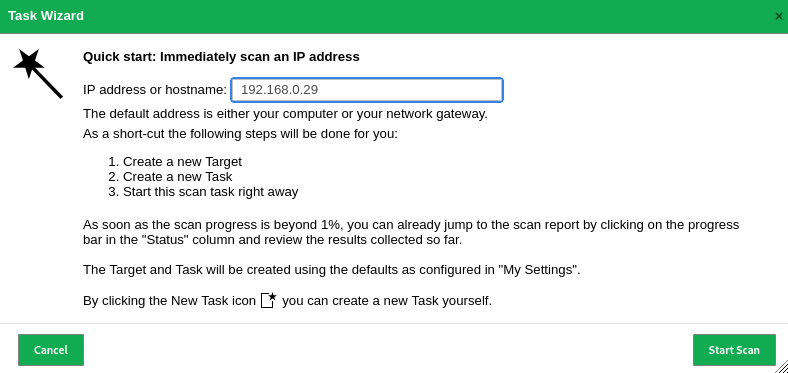


Рисунок 5 – Создание задачи

Давайте ознакомимся с содержанием отчета, который был сформирован в результате сканирования данного узла. Список сканирований показан на рисунке 6. Обнаруженные CVE на узле показаны на рисунке 7.

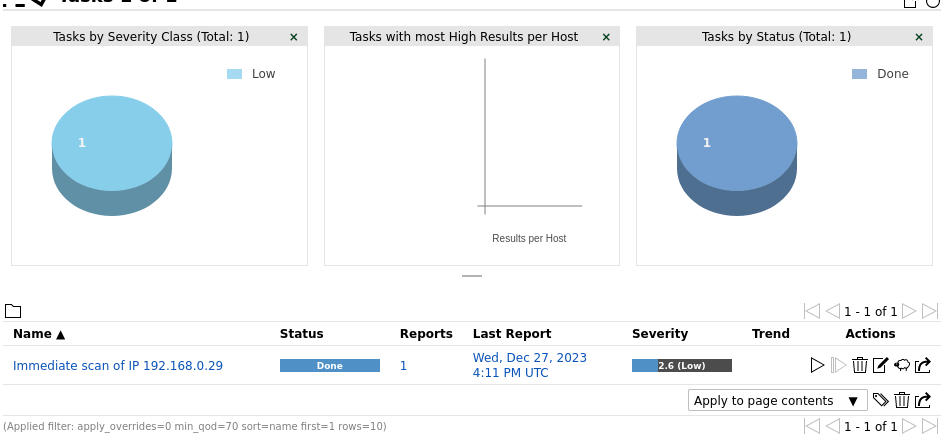


Рисунок 6 – Список сканирований

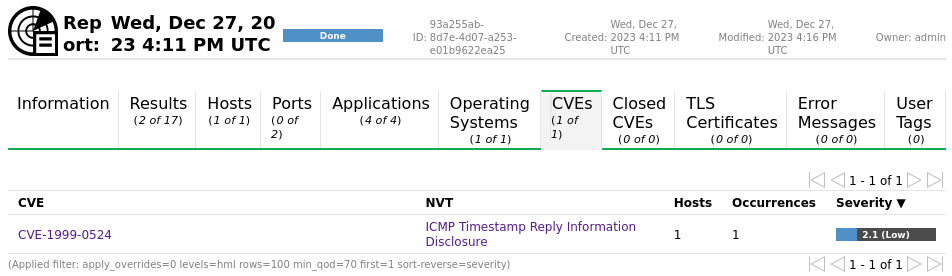


Рисунок 7 – Обнаруженные CVE на узле

Давайте рассмотрим подробности о выявленной уязвимости, представленные в формате NVT (Network Vulnerability Test) на рисунке 8. Анализ представления NVT является важным шагом в обеспечении безопасности сети, позволяя эффективно реагировать на потенциальные риски и повышать общий уровень защиты. Этот этап анализа даст нам информацию о характере и степени серьезности уязвимости, а также предложит рекомендации по ее устранению или смягчению.

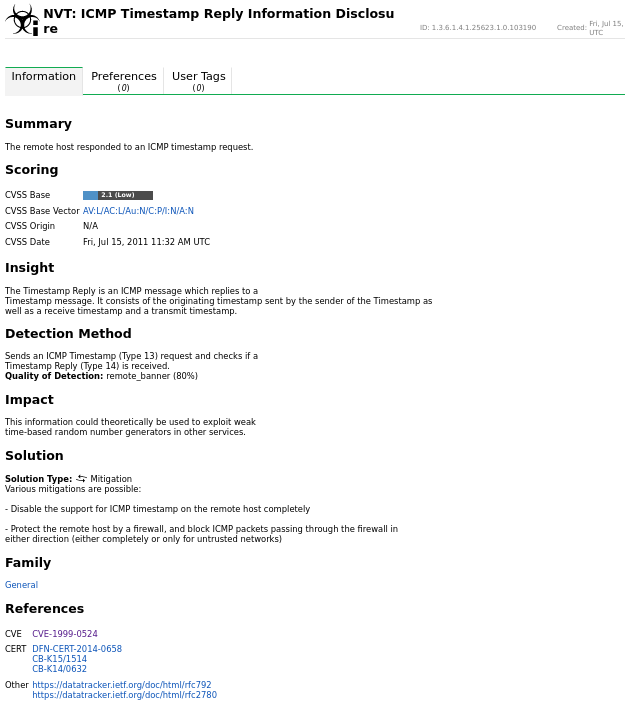


Рисунок 8 – Подробности о выявленной уязвимости

По сравнению с nmap, OpenVAS выявил значительно меньше уязвимостей, что обусловлено в первую очередь ограниченными скриптами и базой данных уязвимостей, используемыми при сканировании. Однако преимуществом OpenVAS в данном случае является наличие функционала по визуализации и настройке расписания сканирований.

Эти возможности будут полезны при постоянном мониторинге узлов в сети с целью выявления и управления потенциальными уязвимостями. Таким образом, хотя количество обнаруженных уязвимостей меньше, функциональные особенности OpenVAS делают его ценным инструментом для систематического контроля безопасности в сетевой инфраструктуре.

# **3. Анализ безопасности системы с помощью Metasploit**

Для начала активируем сервис SSH с целью увеличения числа потенциальных уязвимостей. Этот шаг предусматривает осознанное включение службы SSH, что может создать дополнительные точки входа для потенциальных атак. Увеличивая количество сценариев угроз, мы сможем более тщательно оценить уровень безопасности системы и разработать соответствующие стратегии по ее укреплению. Активация сервиса SSH показана на рисунке 9.

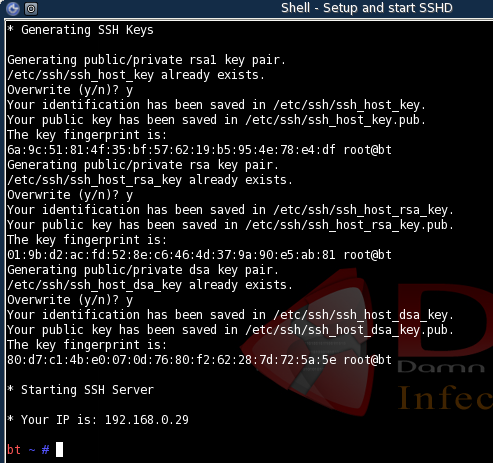


Рисунок 9 – Активация сервиса SSH

После этого выполним запуск командной консоли утилиты Metasploit, предварительно проведя обновление базы данных инструмента Этот шаг включает в себя активацию Metasploit и обновление его информационных ресурсов, что обеспечит доступ к актуальным данным о методах атак и известных уязвимостях. Запуск командной консоли утилиты Metasploit и ее обновление показаны на рисунке 10.

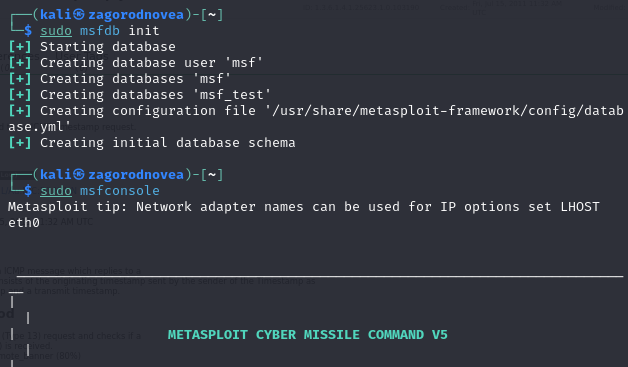


Рисунок 10 – Запуск и обновление командной консоли утилиты Metasploit

Давайте рассмотрим, какие функциональные возможности предоставляет утилита в отношении протокола SSH. Анализ функционала утилиты в контексте SSH даст нам полезные инсайты для оптимизации безопасности этого сервиса и предотвращения возможных угроз. Функциональные возможности утилиты показаны на рисунке 11.

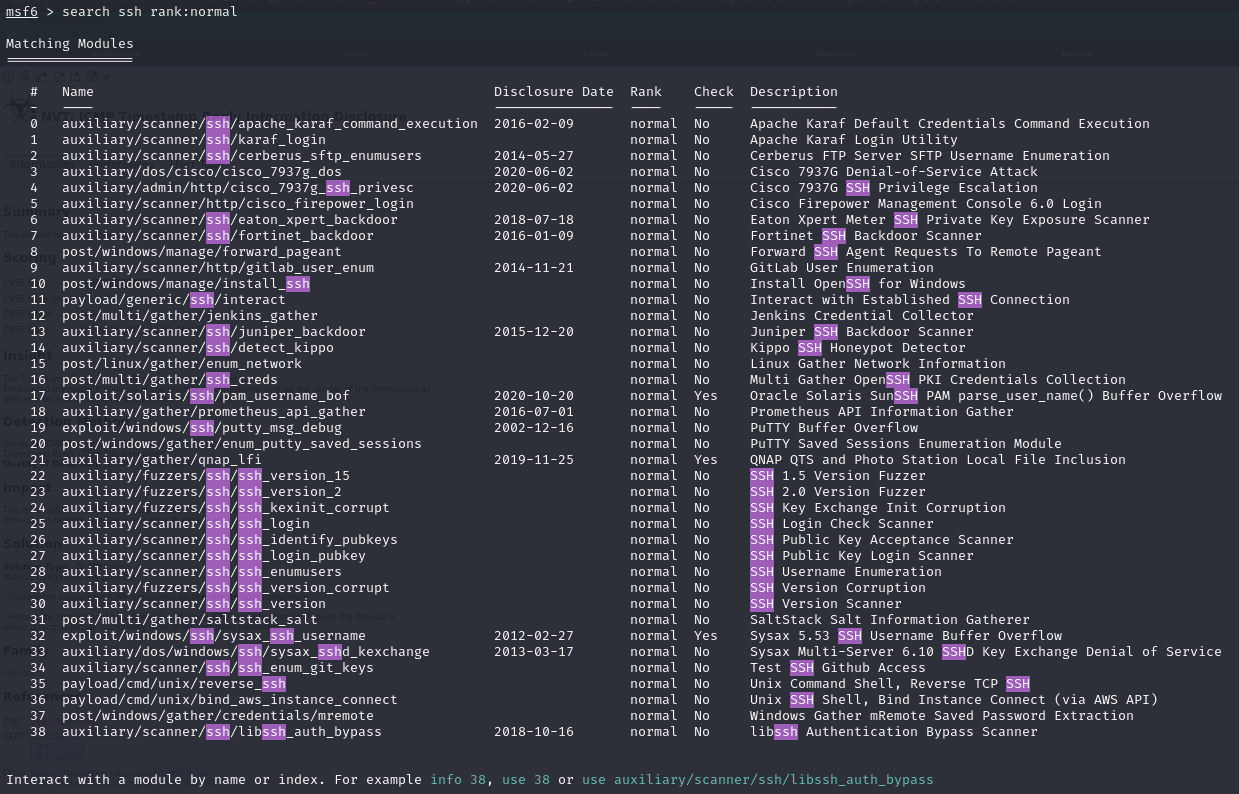


Рисунок 11 – Функциональные возможности утилиты

Обратим внимание на наивно простой вариант - сканер логина. Давайте рассмотрим подробное описание этой функции.

Для использования данной опции нам достаточно указать целевой узел и подключить словарь в формате "логин-пароль". После указания необходимых опций мы запустим процесс сканирования. Этот этап позволит нам оценить простейшие методы атаки на логин и пароль для улучшения общей безопасности системы. Подготовка и запуск процесс сканирования показан на рисунке 12.

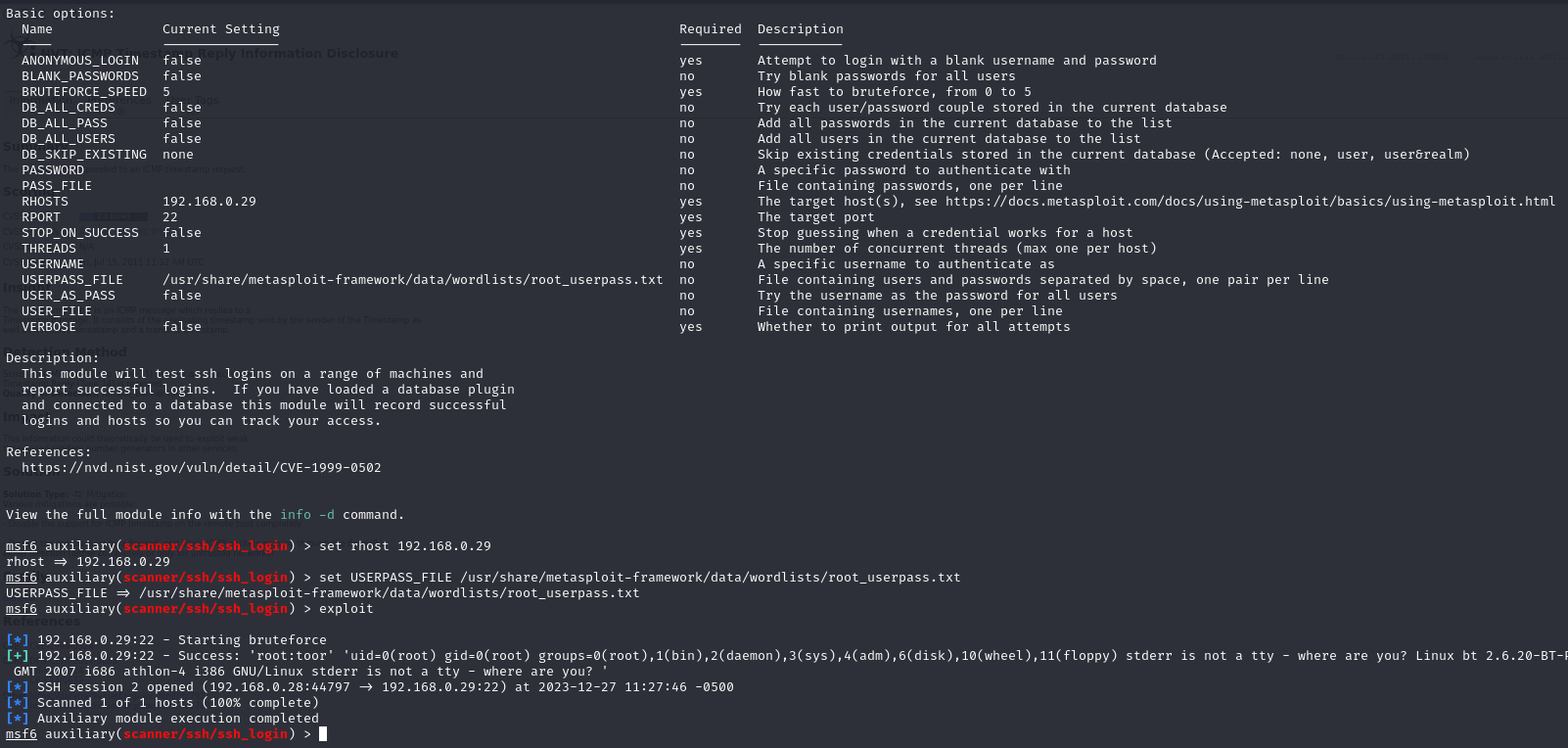


Рисунок 12 – Подготовка и запуск сканирования

В тот же момент мы обнаружили совпадение с учетными данными для доступа к целевому узлу по протоколу SSH. Эта уязвимость идентифицирована под кодом CVE-1999-0502 и предполагает наличие учетной записи Unix для сервиса SSH с паролем, установленным по умолчанию, равным нулю, пустым или отсутствующим.

CVE-1999-0502 связана с уязвимостью в протоколе управления передачей (TCP) стека протоколов TCP/IP и может привести к отказу в обслуживании (DoS). Эта уязвимость связана с возможностью переполнения буфера в функции recv() в коде BSD, что подчеркивает серьезность потенциальных атак и требует немедленных мер по ее устранению.

# **РЕКОМЕНДАЦИИ**

Рекомендации по устранению этой уязвимости следующие:

1. Отключить или изменить пароль учетной записи root на сложный, не поддаваемый легкому подбору. Использовать авторизацию по приватному ключу.
2. Перейти на аутентификацию с использованием приватных ключей, что повысит безопасность процесса входа в систему.Убедитесь, что на вашем сервере и клиентских машинах установлены последние обновления безопасности для операционной системы и приложений.
3. Включить двухфакторную аутентификацию для усиления защиты доступа к SSH.
4. Убедиться, что операционная система и все приложения на сервере и клиентских машинах обновлены до последних версий с учетом патчей безопасности. Ограничить доступ к уязвимым функциям или службам, которые их используют, только для доверенных источников и пользователей.
5. Актуализировать программное обеспечение, использующее уязвимые функции, до последних версий, в которых уязвимость была исправлена.
6. При необходимости отключить использование уязвимых функций или измените конфигурацию, чтобы предотвратить их использование.
7. Внедрить системы предотвращения вторжений и брандмауэры для активной защиты от потенциальных атак.
8. Следить за обновлениями безопасности и новыми угрозами, связанными с данной уязвимостью, и оперативно внедряйте необходимые исправления.
9. Установить политику регулярной смены паролей для всех учетных записей, включая ту, которая используется для службы SSH, для уменьшения риска компрометации.
10. Проводить обучение сотрудников, особенно тех, кто управляет системами, по базовым принципам безопасности, чтобы уменьшить риск человеческого фактора в безопасности системы.
11. Регулярно анализировать сетевой трафик для выявления подозрительной активности и атак, связанных с уязвимостью, и реагируйте на них немедленно.
12. Реализовать систему резервного копирования данных и процедуры восстановления, чтобы в случае успешной атаки была возможность восстановить систему и данные.

# **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;

4. Составить рекомендации по устранению выявленной уязвимости.

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