|  |
| --- |
|  |
| 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»

Выполнила:

Студентка группы ББМО-02-22

Бардасова И.А.

Проверил:

Пимонов Р.В.

Москва, 2023

Содержание

[Введение 3](#_Toc155242641)

[1 Развёртывание и настройка 4](#_Toc155242642)

[Шаг 1. Установка Kali Linux 4](#_Toc155242643)

[Шаг 2. Установка Damn Vulnerable Linux 4](#_Toc155242644)

[2 Анализ защищённости 12](#_Toc155242645)

[2.1 Сканирование сети и уязвимостей 12](#_Toc155242646)

[Шаг 3. Инструмент OpenVas 12](#_Toc155242647)

[Шаг 4. Инструмент Nmap 21](#_Toc155242648)

[3 Анализ безопасности системы 24](#_Toc155242649)

[3.1 Инструмент Metasploit 24](#_Toc155242650)

[Заключение 29](#_Toc155242651)

**Введение**

**Цель работы**: Провести активное тестирование защищенности информационных систем. Развернуть две ВМ.

**Задачи**:

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

# 1 Развёртывание и настройка

# Шаг 1. Установка Kali Linux

Kali уже был установлен заранее, представлен на рисунке 1.

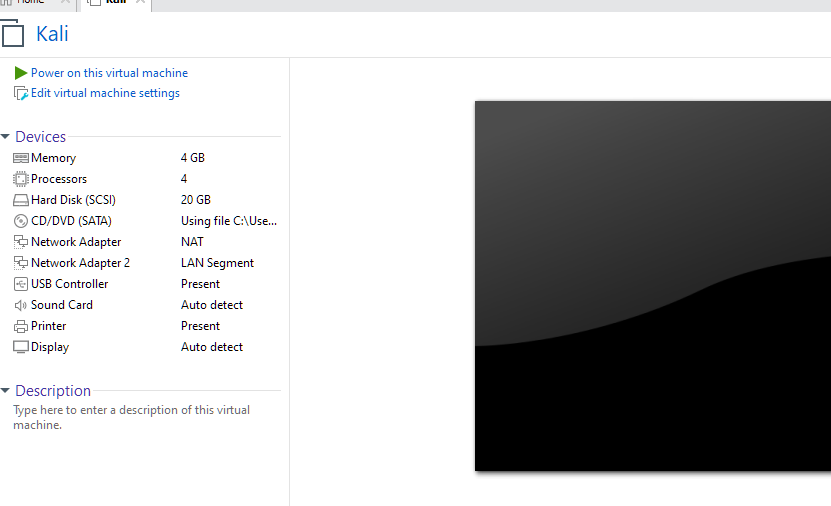


Рисунок 1 – Kali Linux

# Шаг 2. Установка Damn Vulnerable Linux

Установка DVL на отдельной виртуальной машине, настройка для тестирования безопасности.

Скачаем DVL образ диска и выполним установку образа в VMWare (рис. 2).

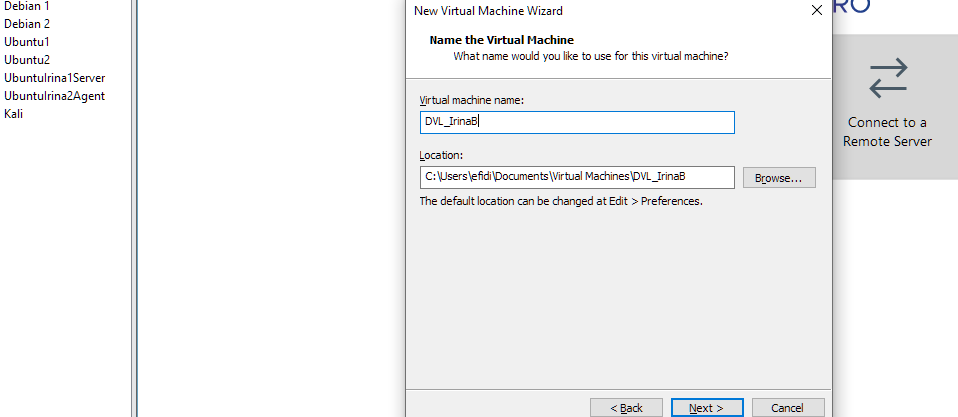


Рисунок 2 – Установка образа

Выполняется загрузка ВМ.

Теперь выполним авторизацию (рис. 3):

Логин: root

Пароль: toor



Рисунок 3 – Авторизация

Определим, какой диск форматировать (/dev/sda) (рис. 4).

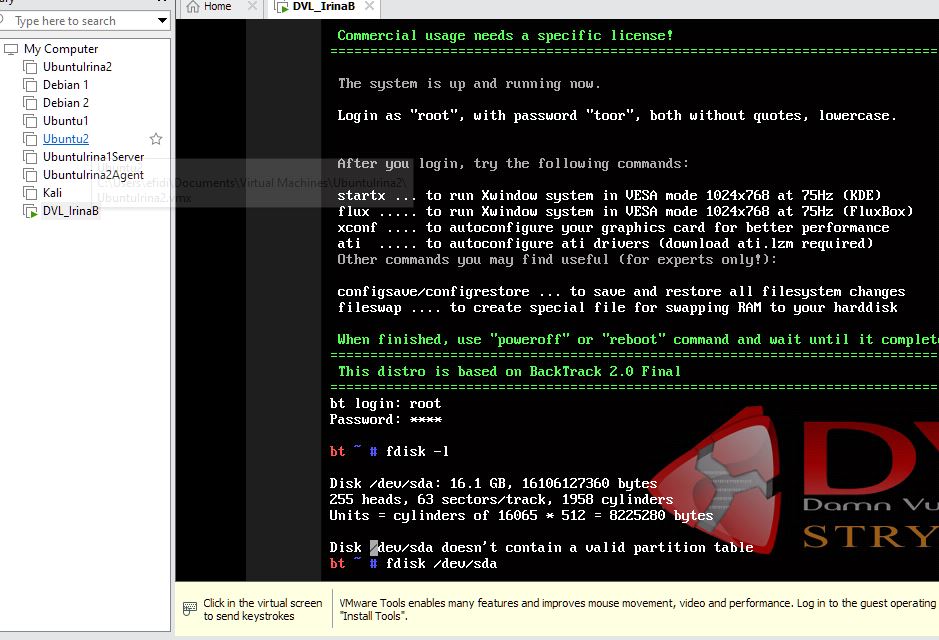


Рисунок 4 – Диск (/dev/sda)

Выберем диск для разбиения на разделы (рис. 5).

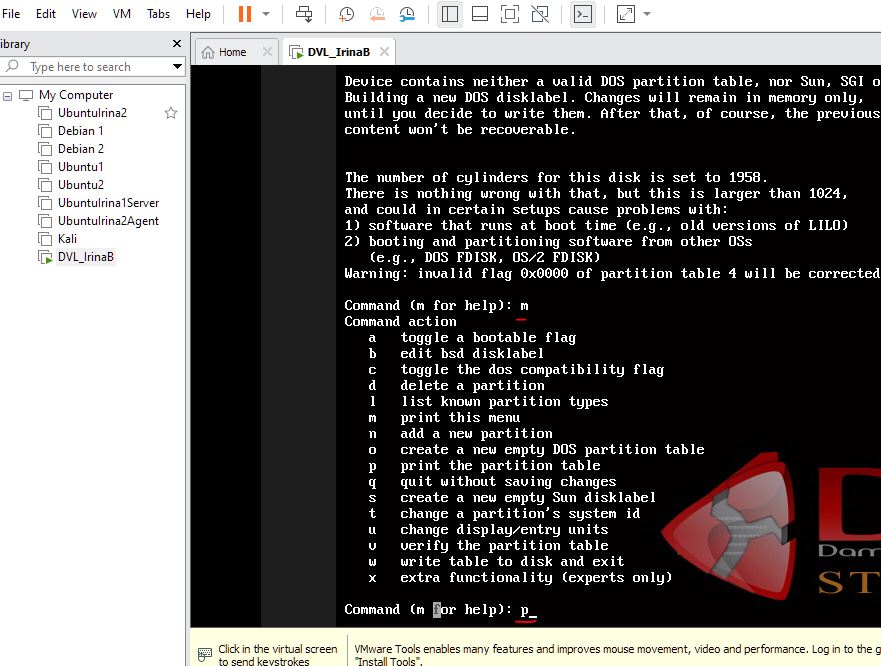


Рисунок 5 – Диск для разбиения

Посмотрим таблицу разделов. Имеется 1958 цилиндра (рис. 6).

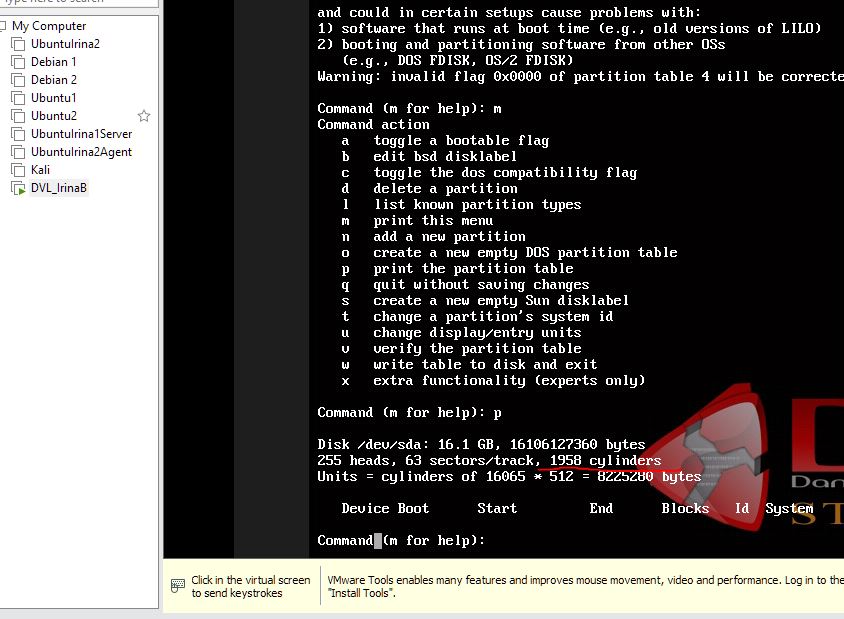


Рисунок 6 – Таблица разделов

Добавим новый раздел (рис. 7).

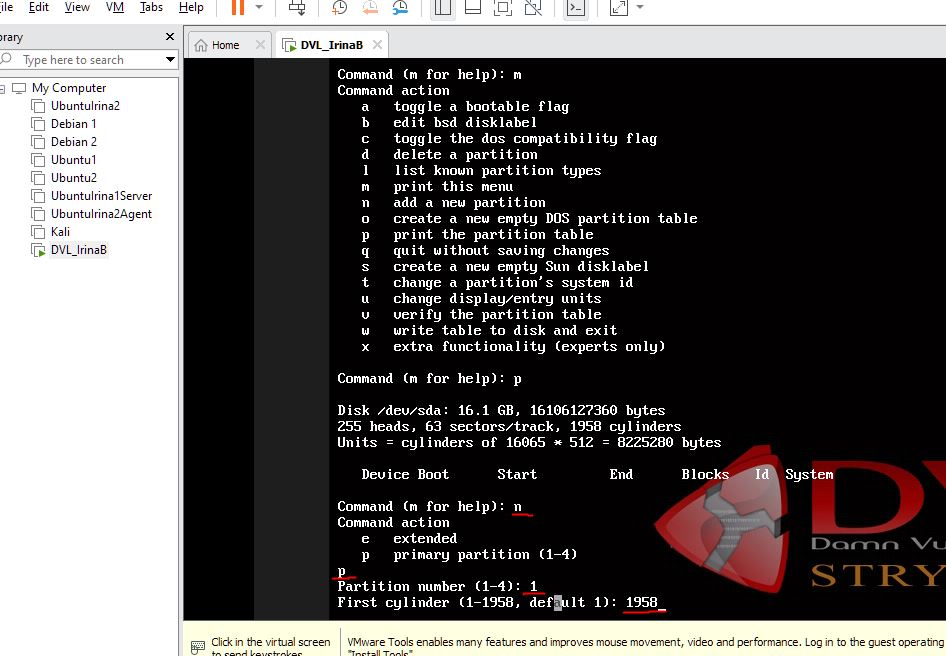


Рисунок 7 – Добавление раздела

Посмотрим на созданный раздел (рис. 8).

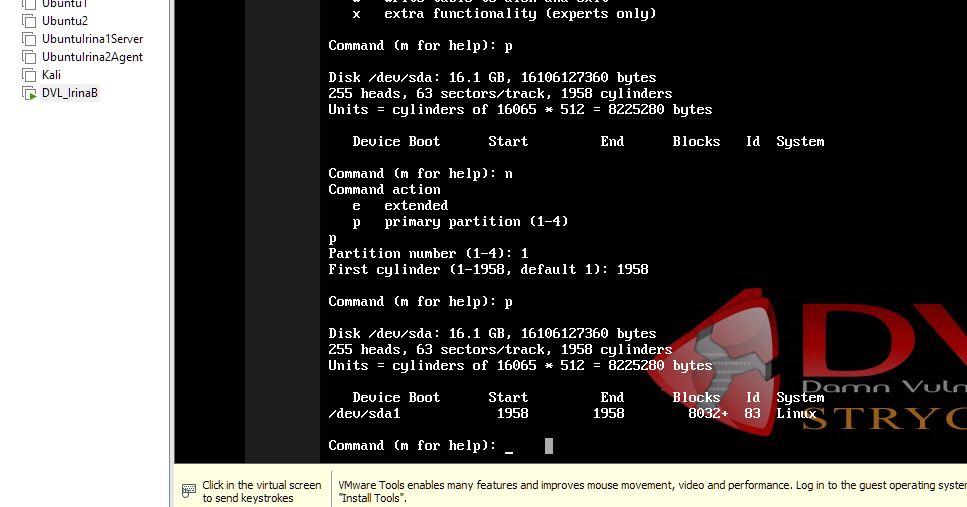


Рисунок 8 – Созданный раздел

Сохраним новый раздел и отформатируем раздел /dev/sda (рис. 9).

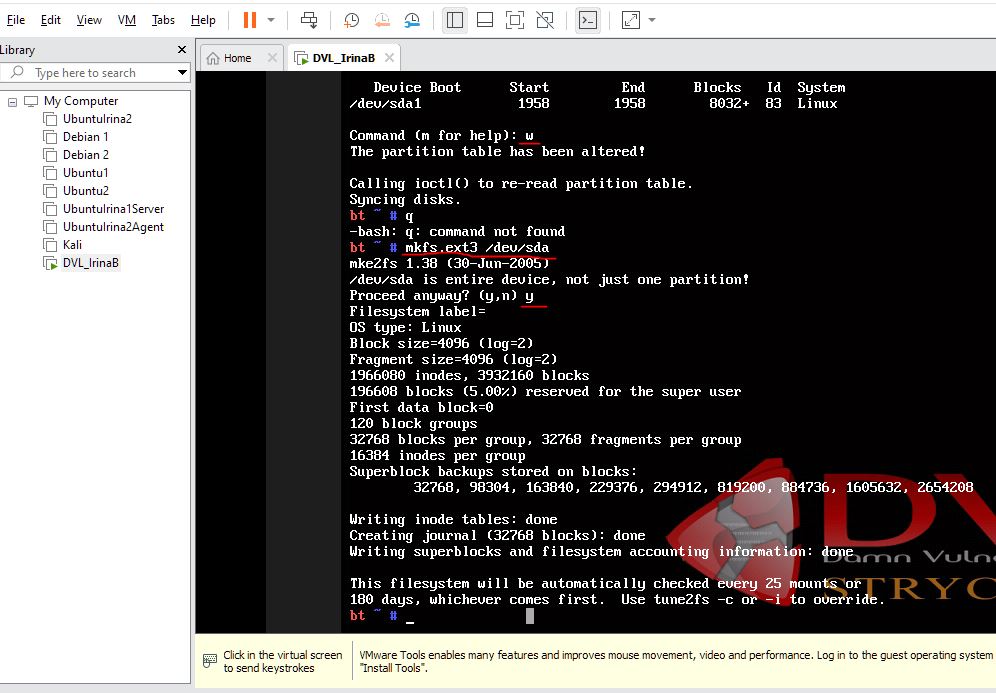


Рисунок 9 – Сохранение раздела

Создадим папку для монтирования раздела. Подключим жесткий диск к каталогу /mnt/dvl. Выполним перезагрузку (рис. 10).

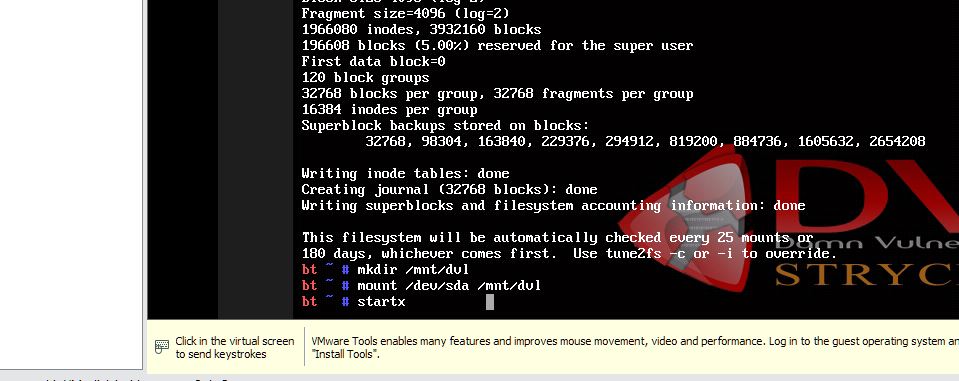


Рисунок 10 – Папка для монтирования раздела, перезагрузка

Настроим установщик BackTrack (рис. 11).

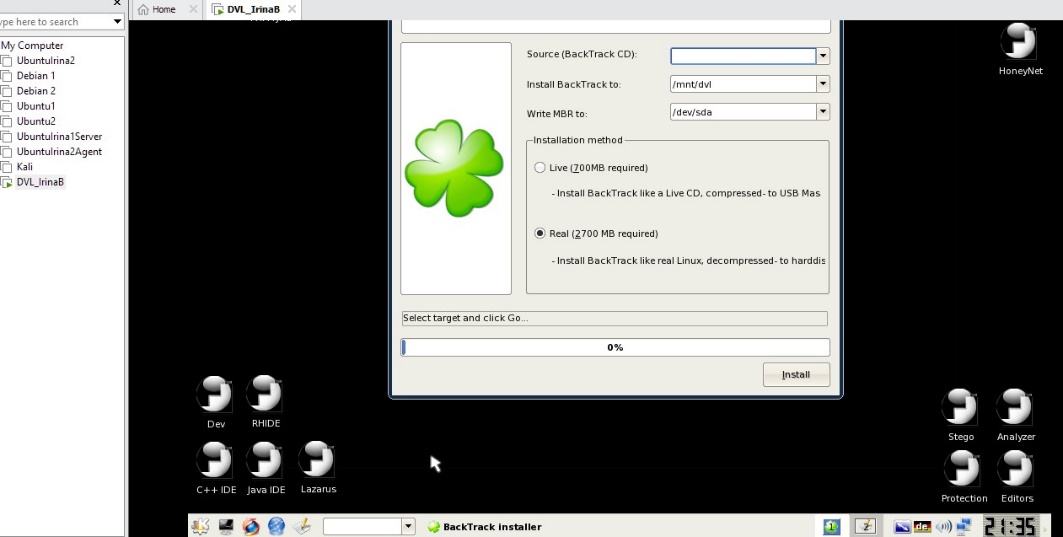


Рисунок 11 – Установщик BackTrack

Ждём завершения (рис. 12).

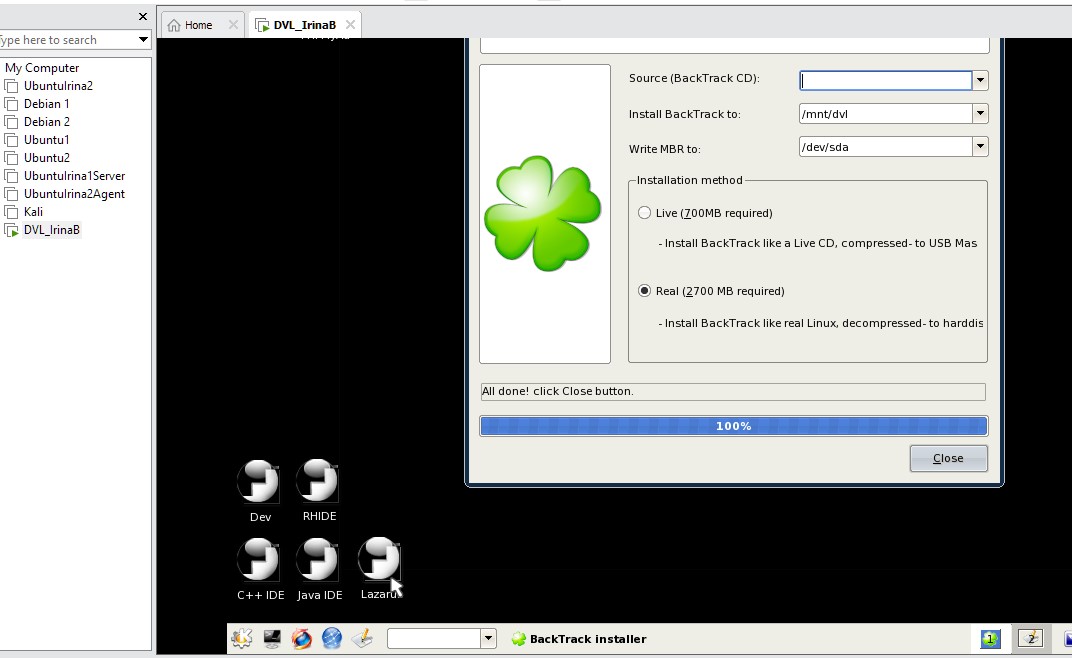


Рисунок 12 – Установщик BackTrack, выполнение

Установим загрузчик (рис. 13).

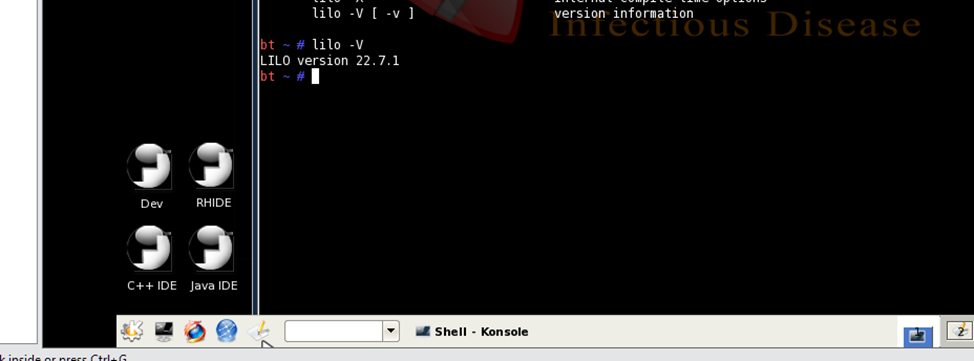


Рисунок 13 – Загрузчик

Наши готовые ВМ (рис. 14-15):

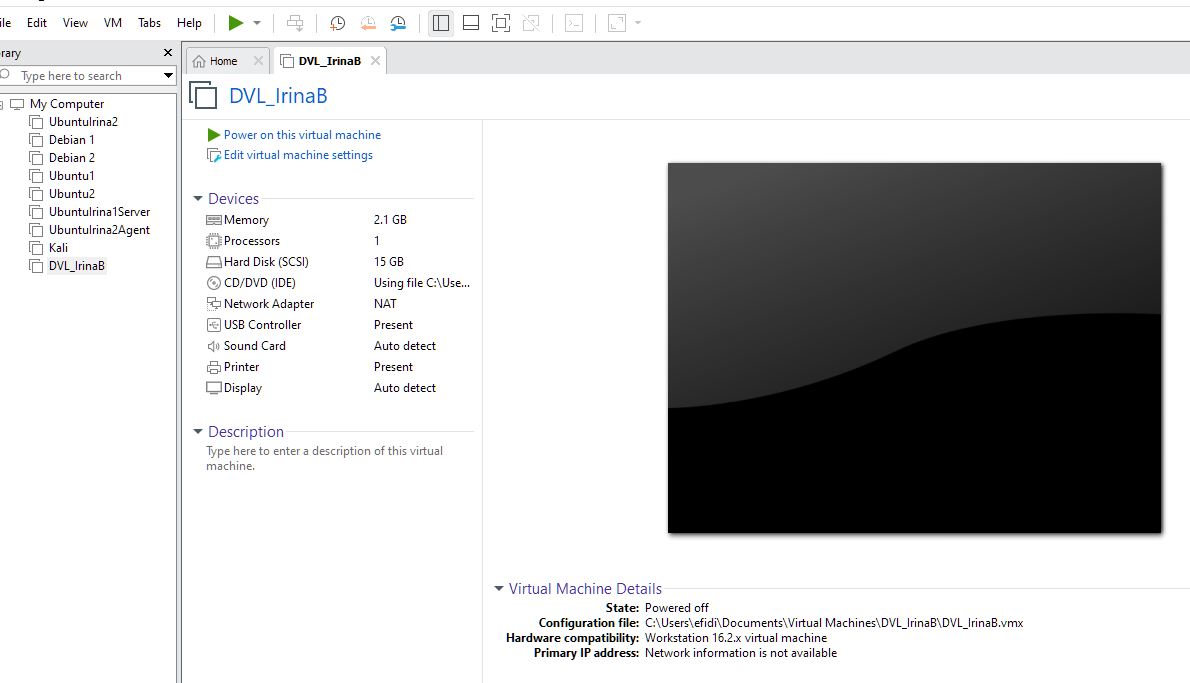


Рисунок 14 – DVL\_IrinaB

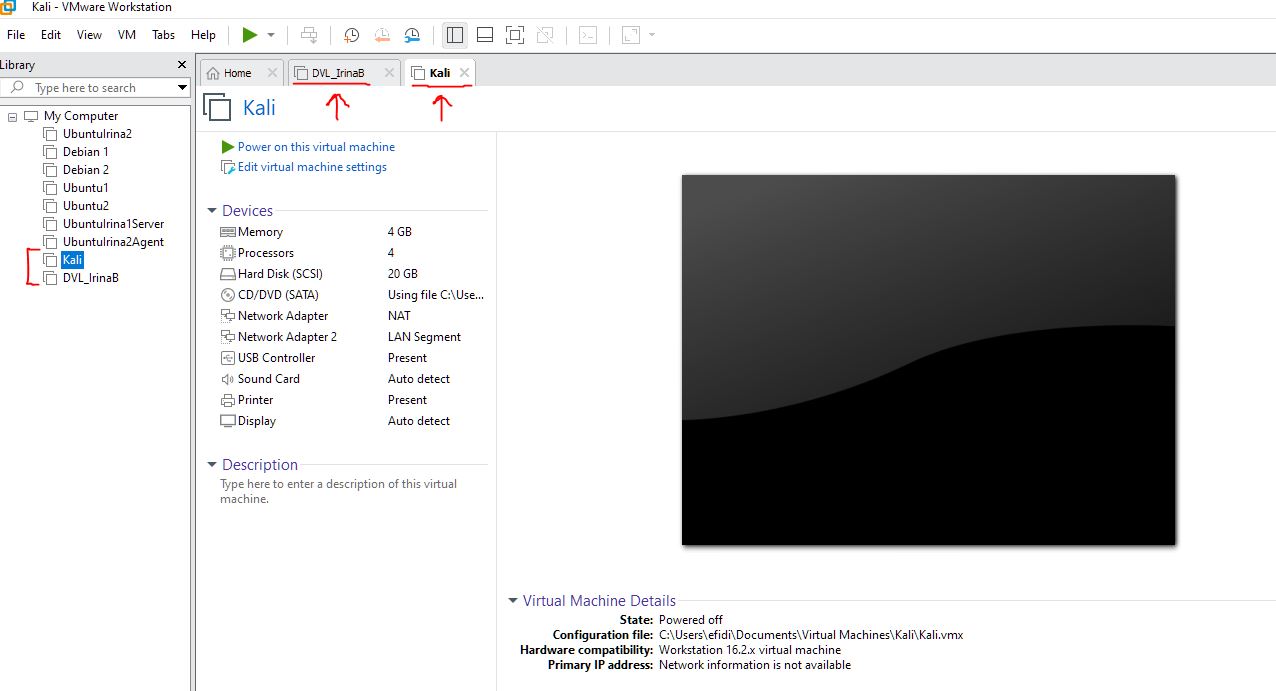


Рисунок 15 – Kali Linux

Узнаем ip-адреса и проверим связь между ними (рис. 16-17):

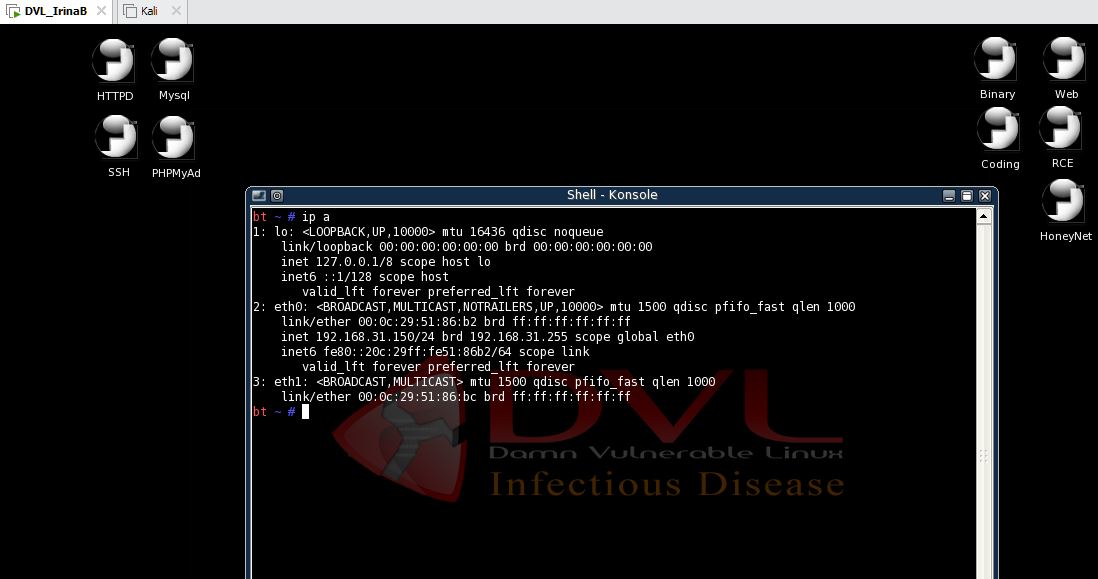


Рисунок 16 – Ip-адрес DVL

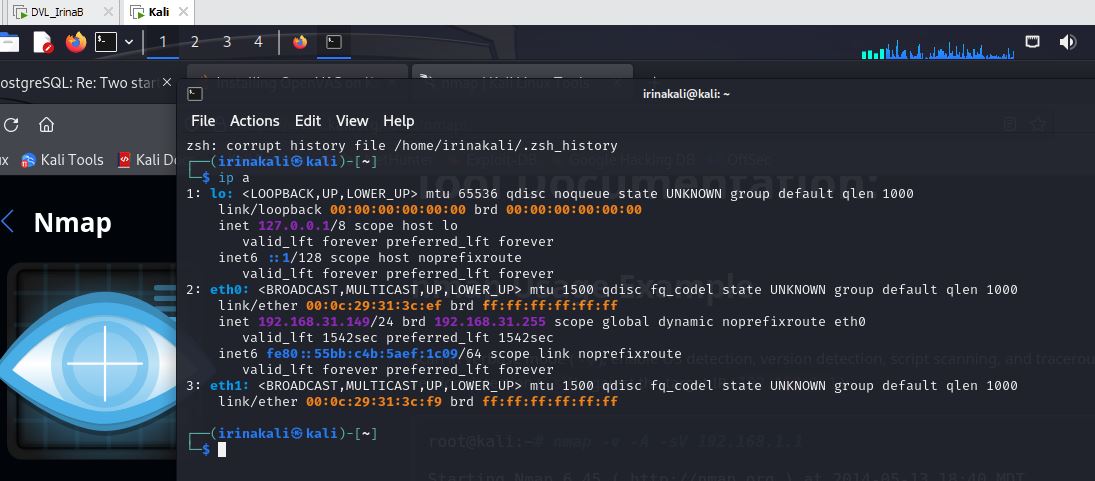


Рисунок 17 – Ip-адрес Kali

Отобразим доступность узлов друг для друга командой ping (рис. 18-19).

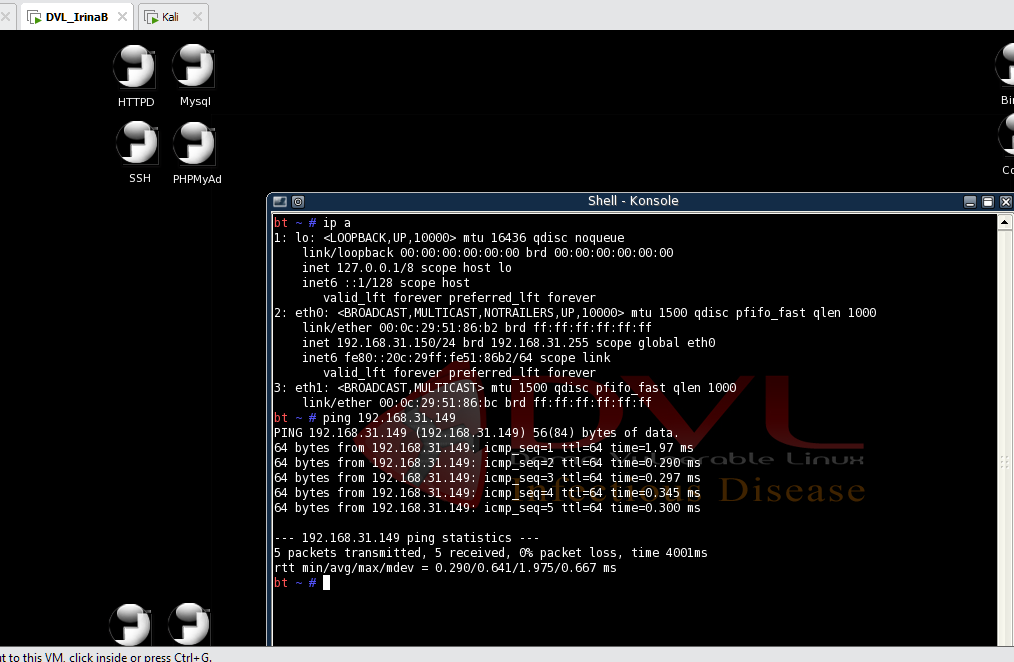


Рисунок 18 – Ping Kali

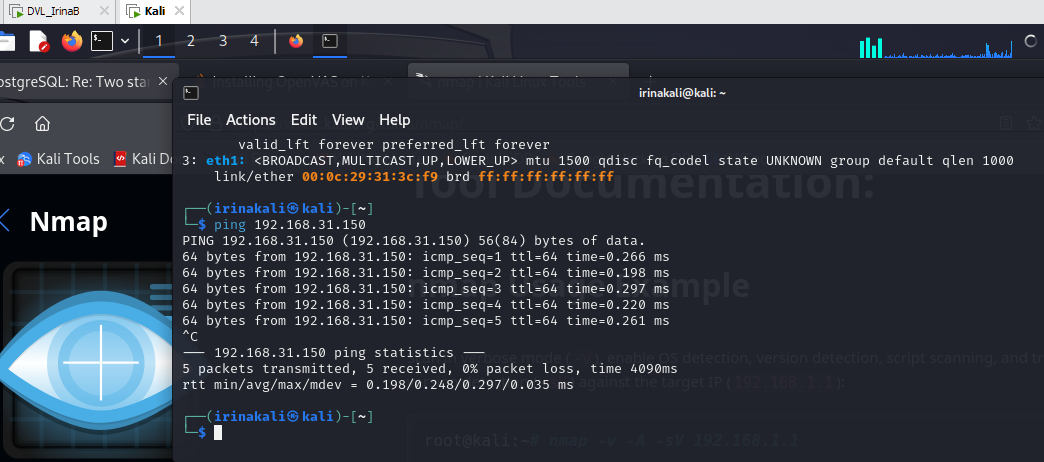


Рисунок 19 – Ping DVL

# 2 Анализ защищённости

# 2.1 Сканирование сети и уязвимостей

# Шаг 3. Инструмент OpenVas

Установим OpenVas на уже имеющуюся ВМ Kali Linux (рис. 20).

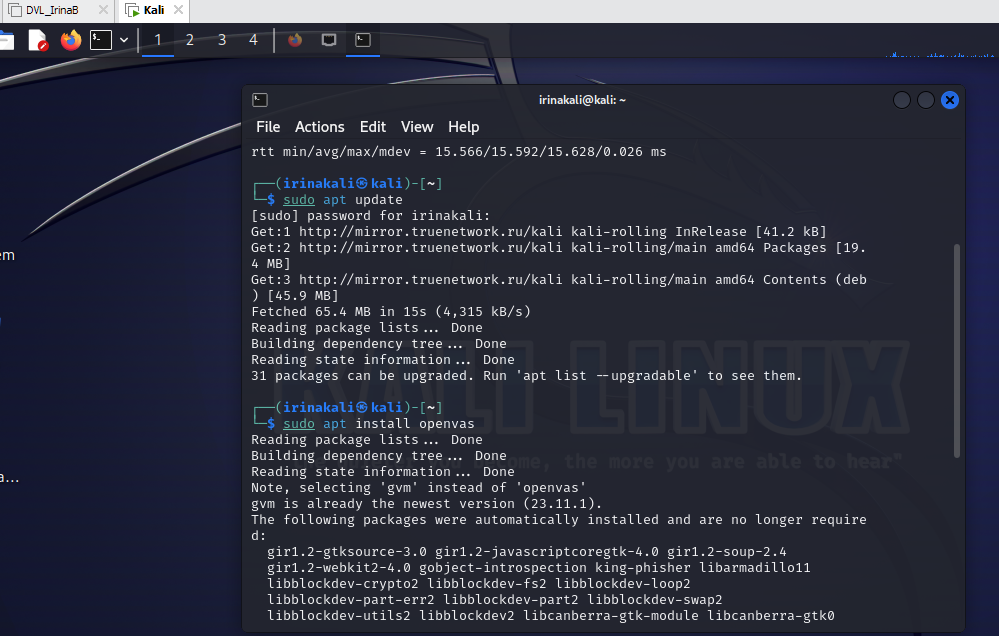


Рисунок 20 – Установка OpenVas

OpenVAS поставляется с собственной службой Redis для Kali GNU/Linux. Убедимся, что сервис Redis настроен для корректной работы с OpenVAS командой «systemctl status redisserver@openvas.service» (рис. 21).

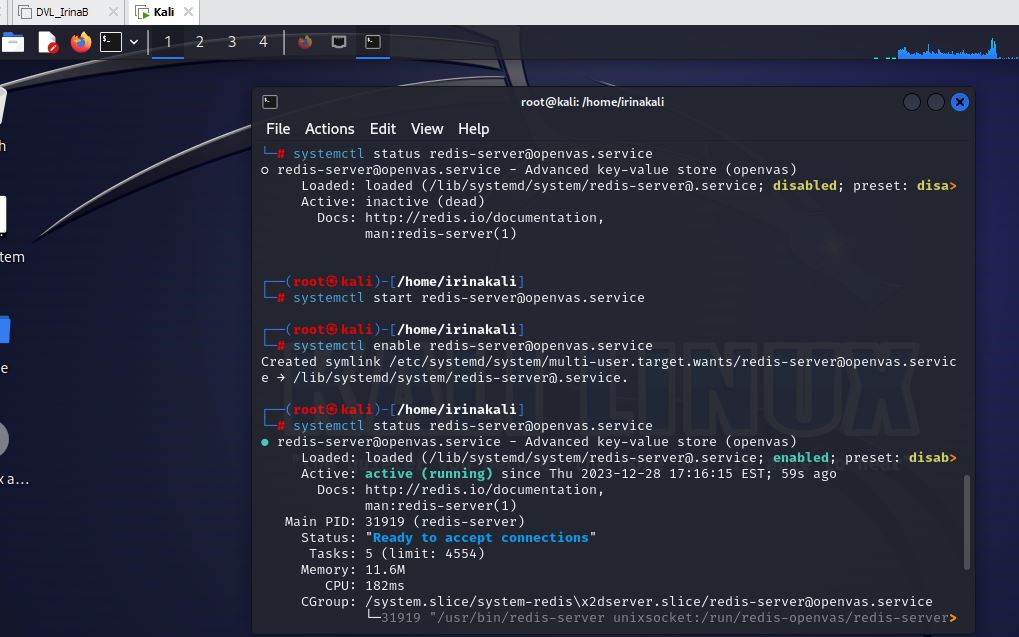


Рисунок 21 – Статус Redis

При попытке запустить настройку сервиса, получаем ошибку о версии СУБД (рис. 22).



Рисунок 22 – Ошибка версии

Для решения данной проблемы необходимо заменить порт необходимой версии на 5432 (рис. 24). Не забудем перезапустить сервис СУБД командой «sudo systemctl restart postgresql» (рис. 23).

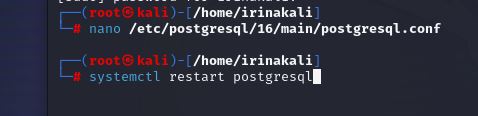


Рисунок 23 – Перезапуск

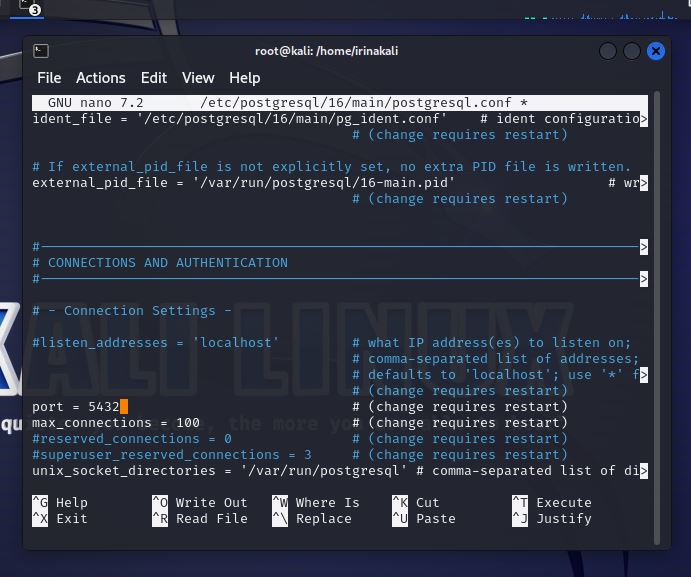


Рисунок 24 – Замена порта СУБД

Но возникла новая проблема, версии не совпадали (рис. 25).

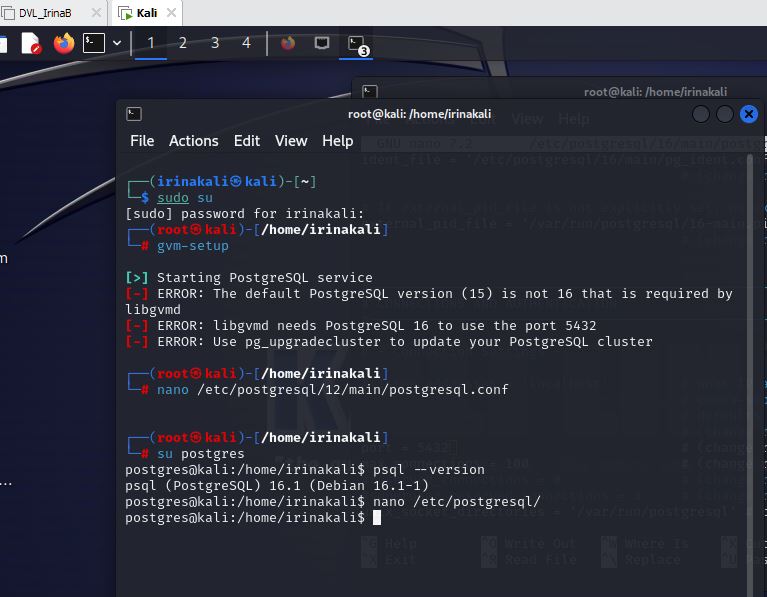


Рисунок 25 – Очередная ошибка

Для решения уже этой проблемы, необходимо было прописать команду «ALTER DATABASE template1 REFRESH COLLATION VERSION;» и перезапустить (рис. 26-27). Мы изменили версии с 2.36 на 2.37.

Повторяем попытку запуска настройки сервиса командой «sudo gvm-setup» (рис. 28-30).

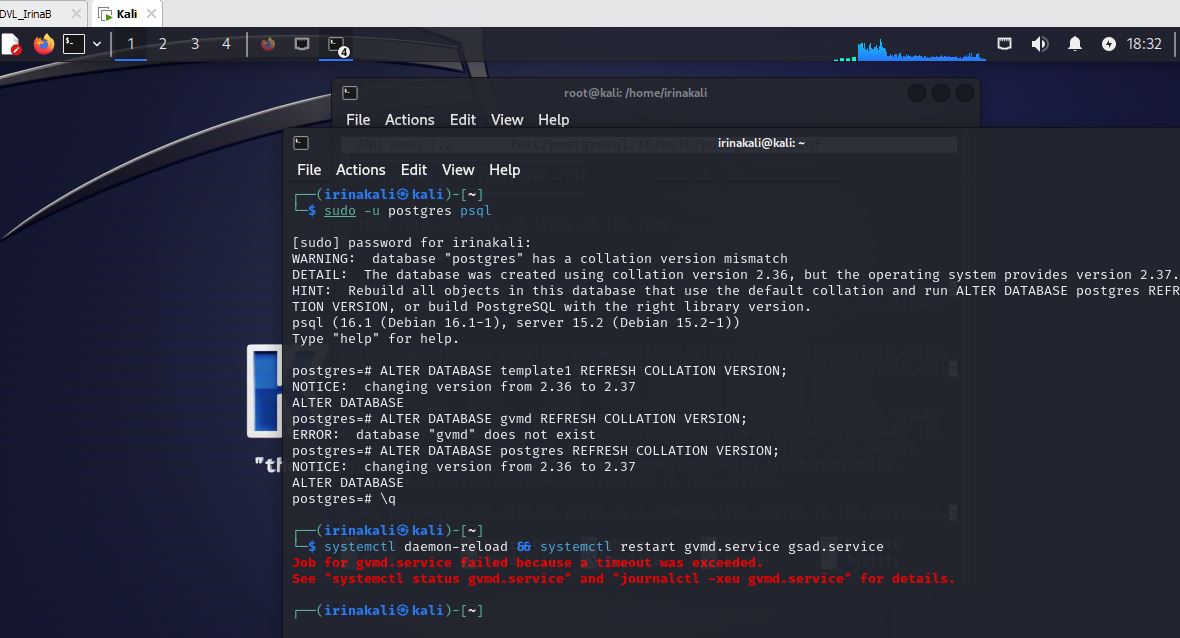


Рисунок 26 – Решение проблемы

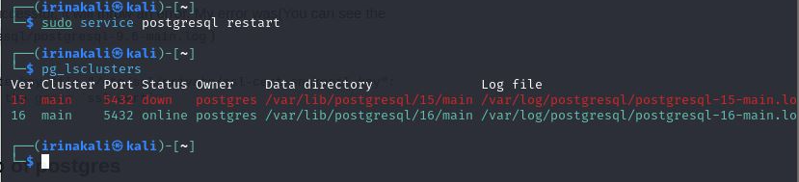


Рисунок 27 – Перезапуск

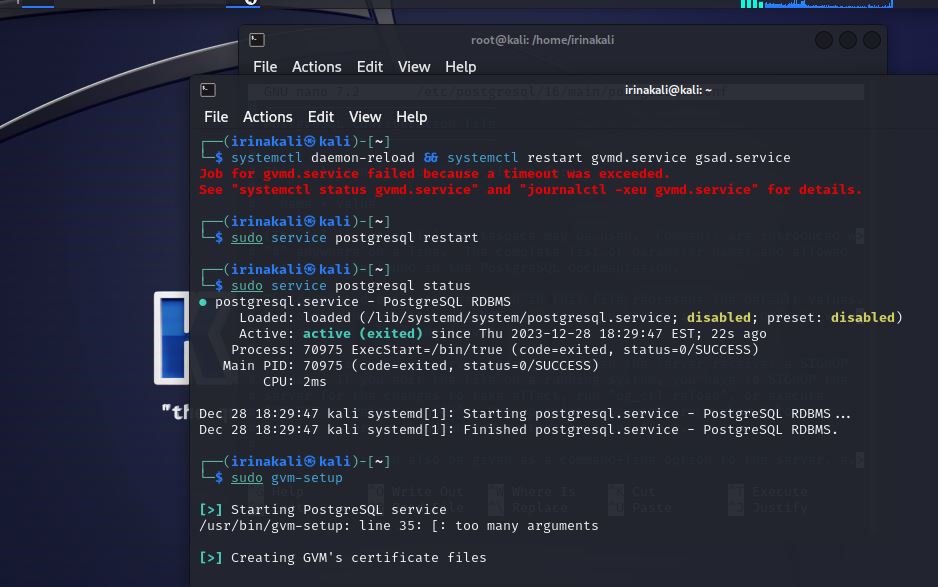


Рисунок 28 – Запуск

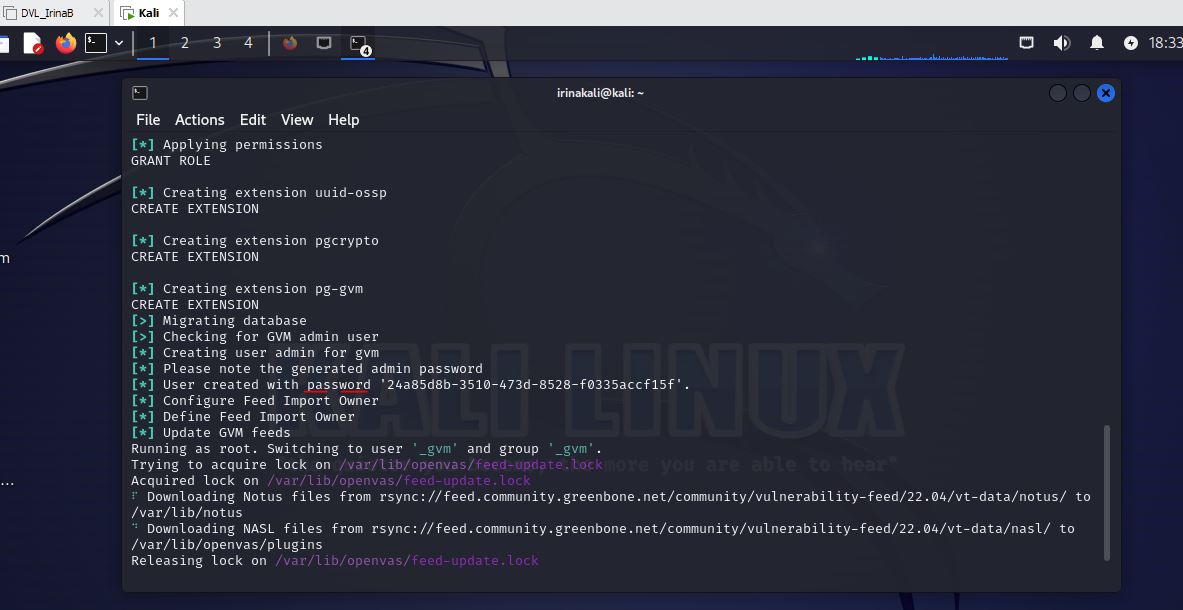


Рисунок 29 – Первичная настройка сервиса

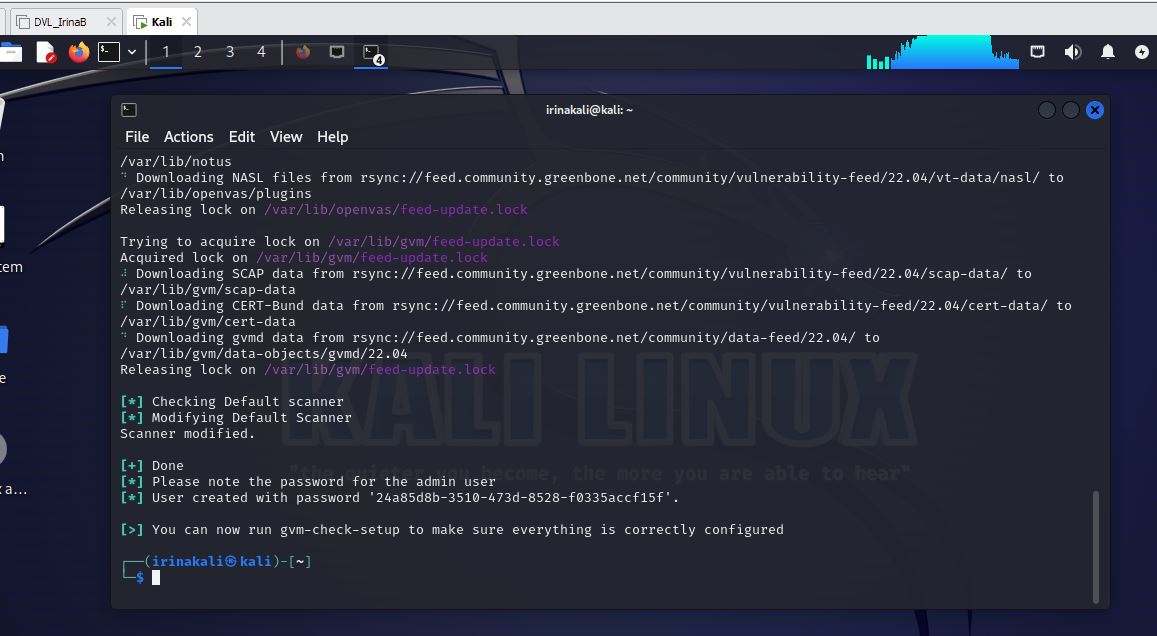


Рисунок 30 – Результат

Дождемся конца установки. По окончанию настройки проверим успешность установки командой «sudo gvm-check-setup», но у нас возникает ошибка (рис. 31).

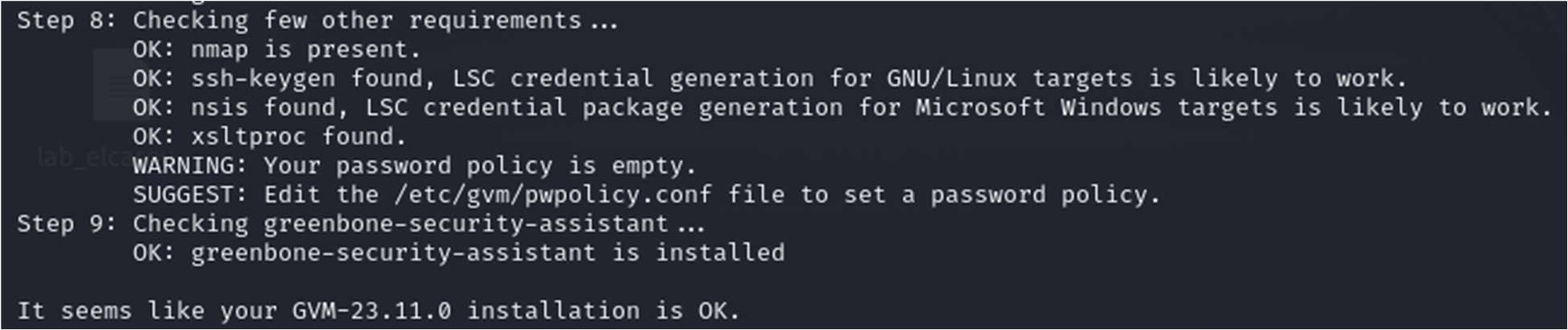


Рисунок 31– Проверка установки

Настройка OpenVAS.

Настроим сервис gvmd и обновим базу OpenVAS, включим сервис gvmd (рис. 32).



Рисунок 32 – Обновление базы

Переходим в веб-интерфейс по адресу https://localhost:9392/. Вводим учетные данные пользователя и сразу попадаем на главную страницу (рис. 33-34).

Данные для входа:

Please note the generated admin password

[\*] User created with password '24a85d8b-3510-473d-8528-f0335accf15f '.

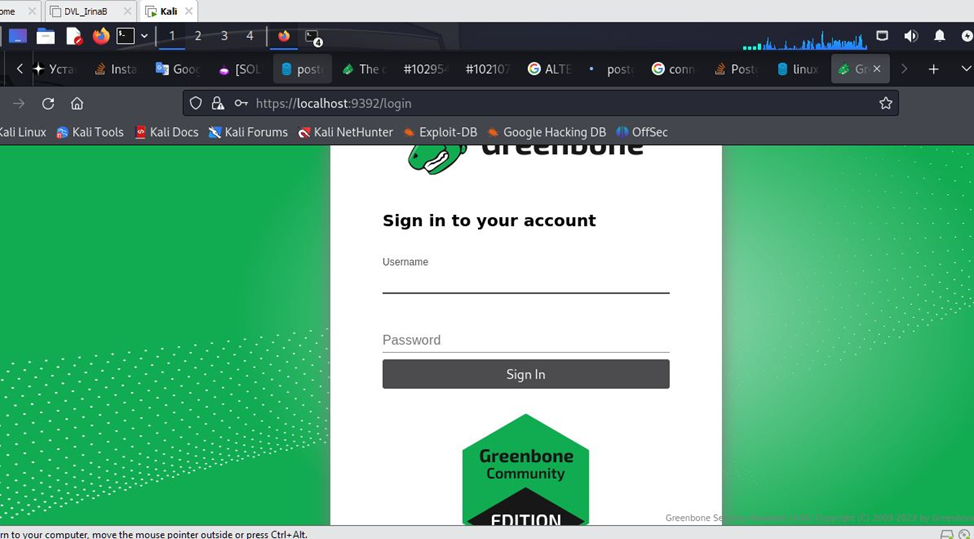


Рисунок 33 – Ввод учётной записи OpenVAS

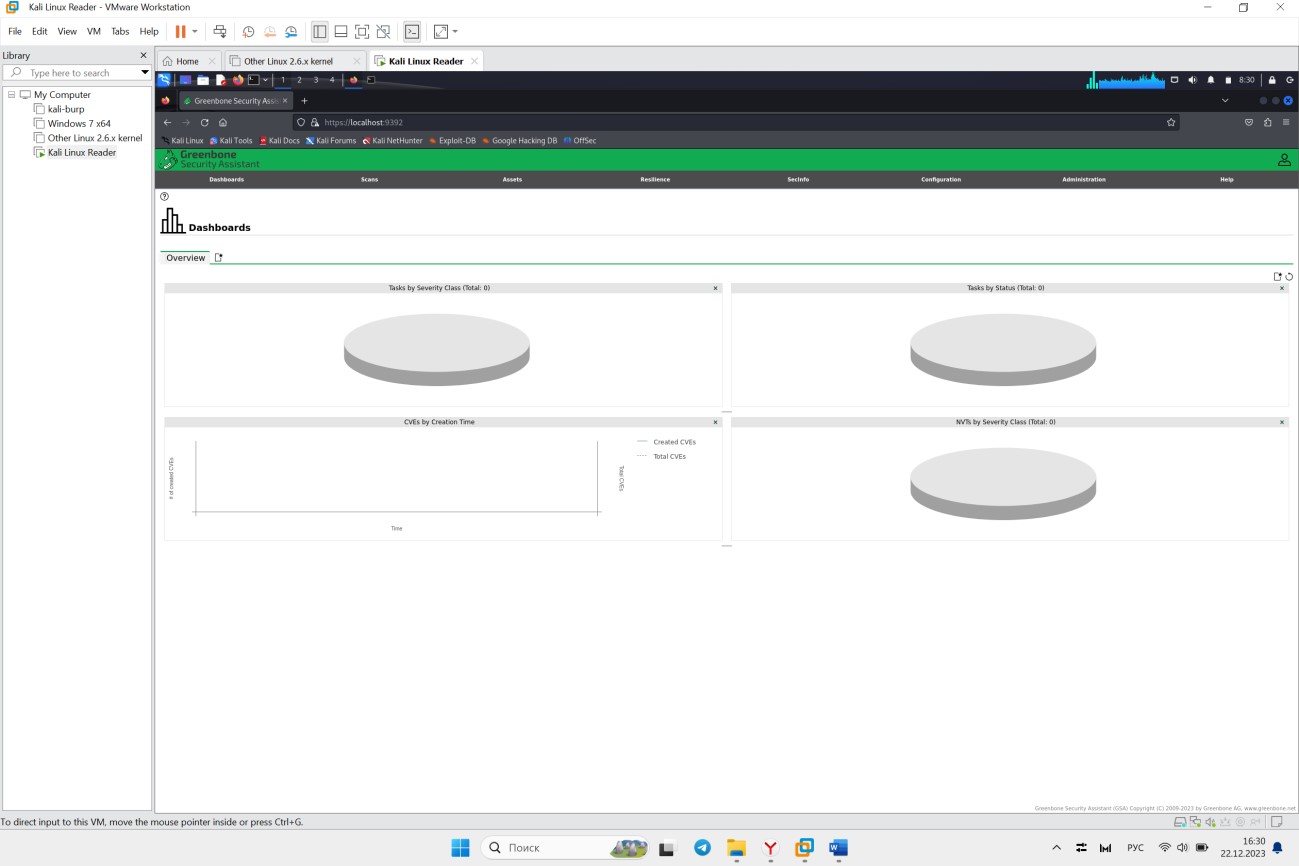


Рисунок 34 – Главная страница веб-интерфейса OpenVAS

**Сканирование сети с помощью OpenVAS.**

Проведем операции по сканированию сети. Создадим задачу на сканирование нашего целевого узла (рисунок 35).

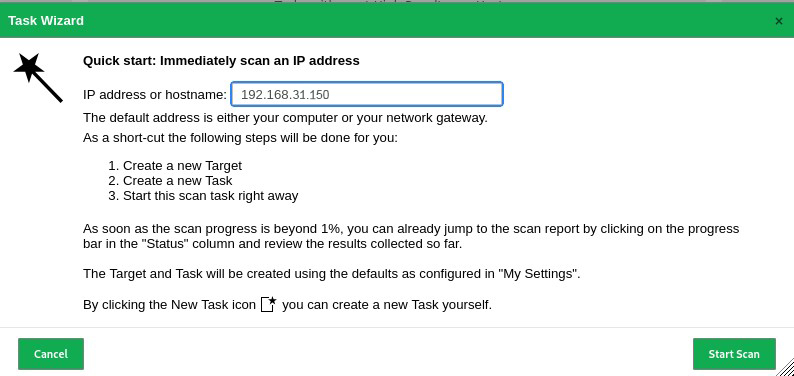


Рисунок 35 – Создание задачи

Теперь посмотрим, что находится в отчете по итогам сканирования узла (рисунки 36-37).

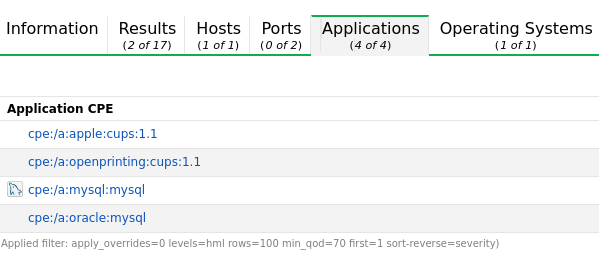


Рисунок 36 – Обнаруженные приложения на узле

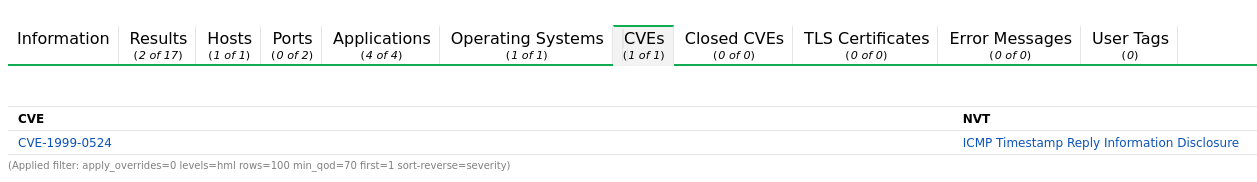


Рисунок 37 – Обнаруженные CVE на узле

Если нажать на уязвимость, то будет отображено её подробное описание.

Запущен сервис ssh на DVL (рис. 38):

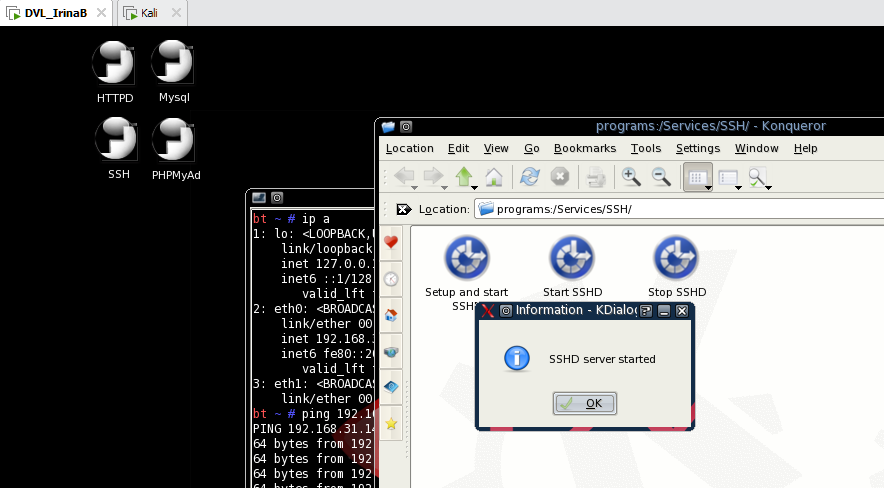


Рисунок 38 – ssh на DVL

# Шаг 4. Инструмент Nmap

Проведем операции по сканированию сети. Выполним поиск узлов в подсети (рис. 39).

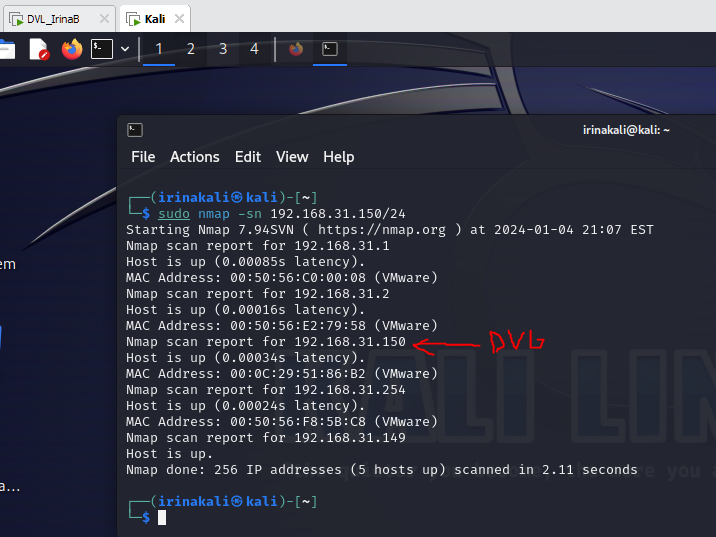


Рисунок 39 – Поиск узлов

Затем просканируем конкретный узел с целью выявления рабочих сервисов и портов, по которым они выходят наружу (рис. 40).

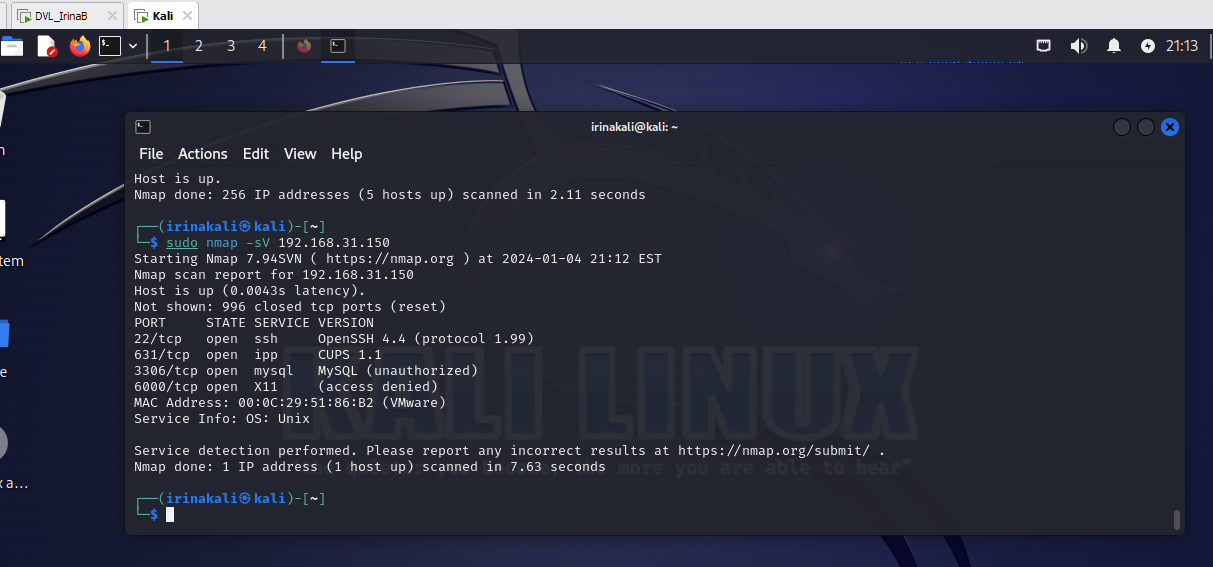
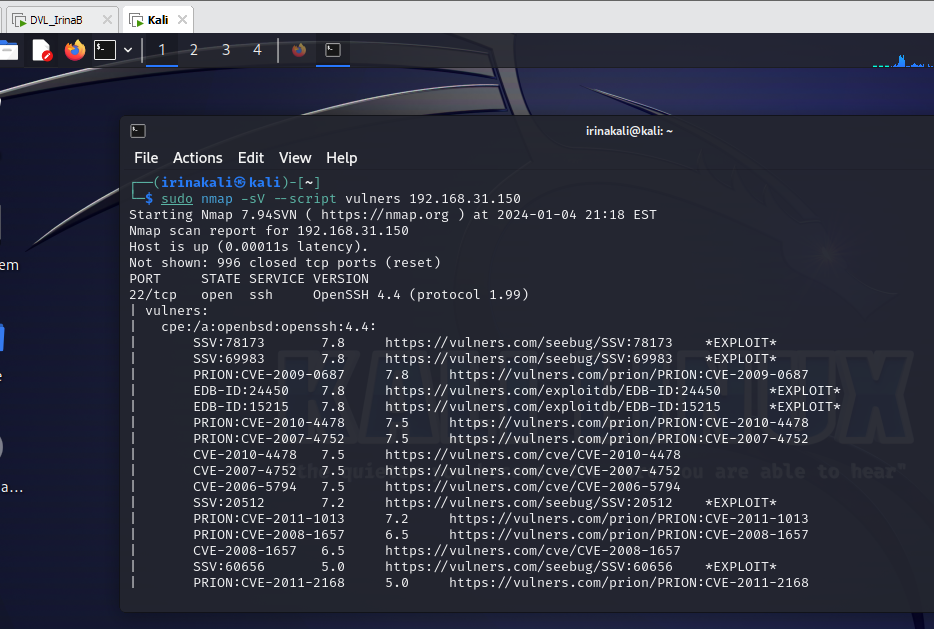
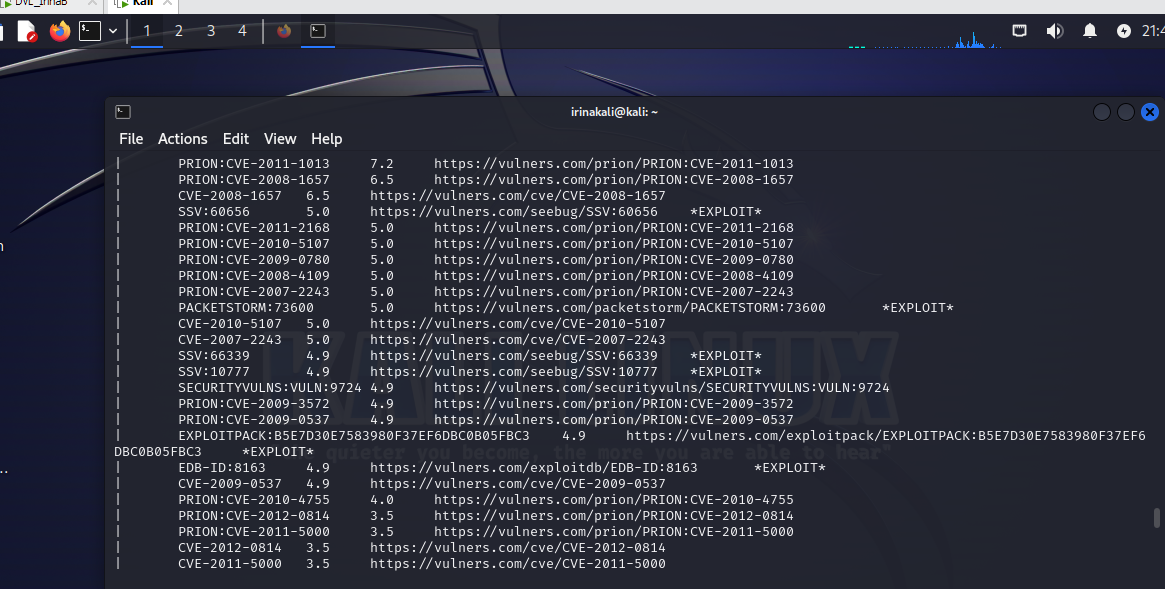
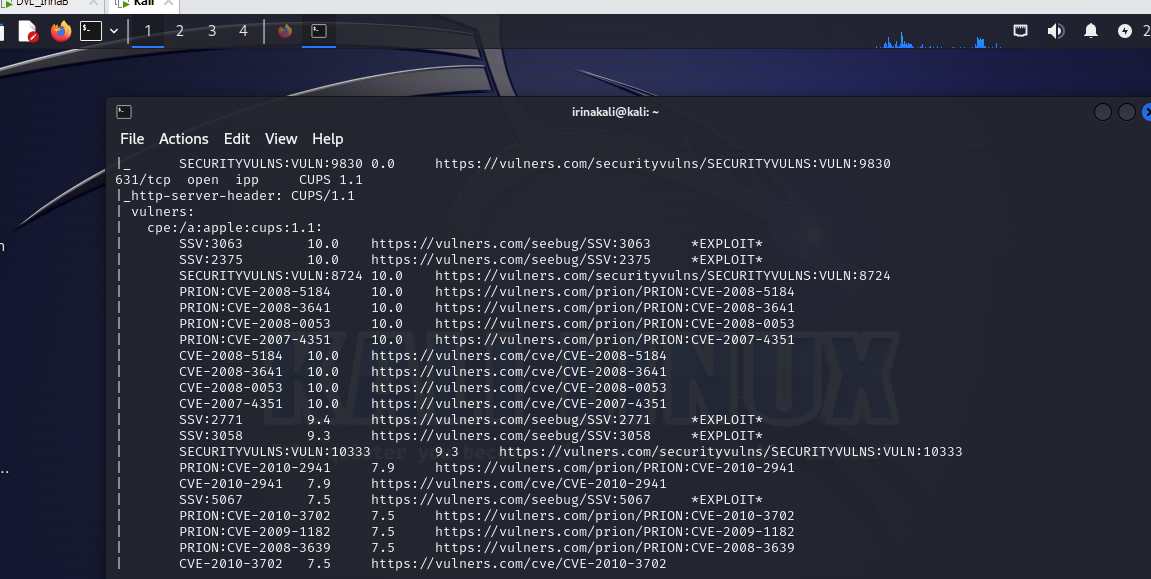


Рисунок 40 – Запрос по сервисам

После чего попробуем просканировать узел на наличие потенциальных угроз безопасности (рис. 41).







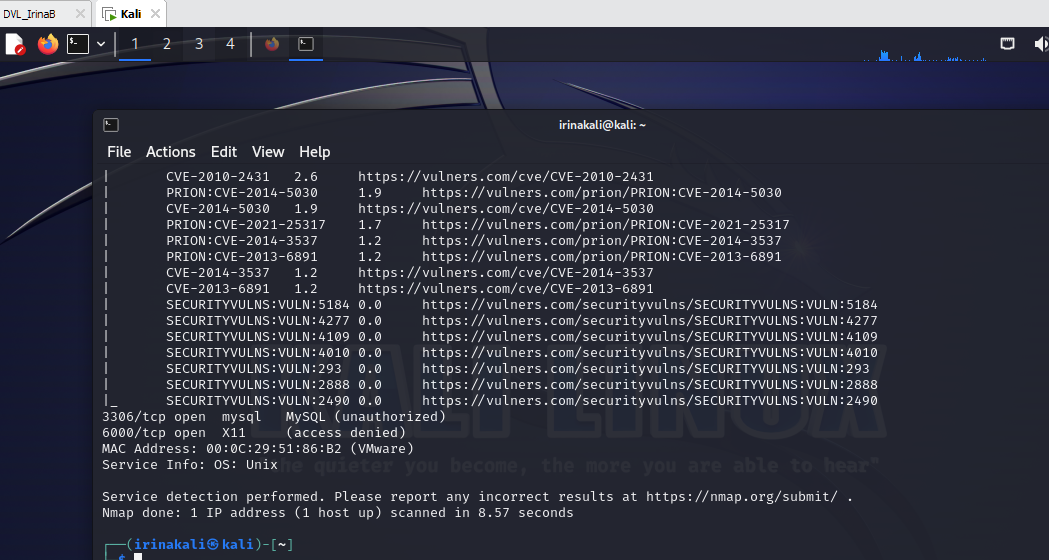


Рисунок 41 – Поиск уязвимостей

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 будет являться функционал по визуализации и настройки расписания сканирований, что будет полезным при постоянном мониторинге узлов в сети на предмет возможных уязвимостей.

# 3 Анализ безопасности системы

# 3.1 Инструмент Metasploit

Установка Metasploit, обновление и запуск (рис. 42-44).

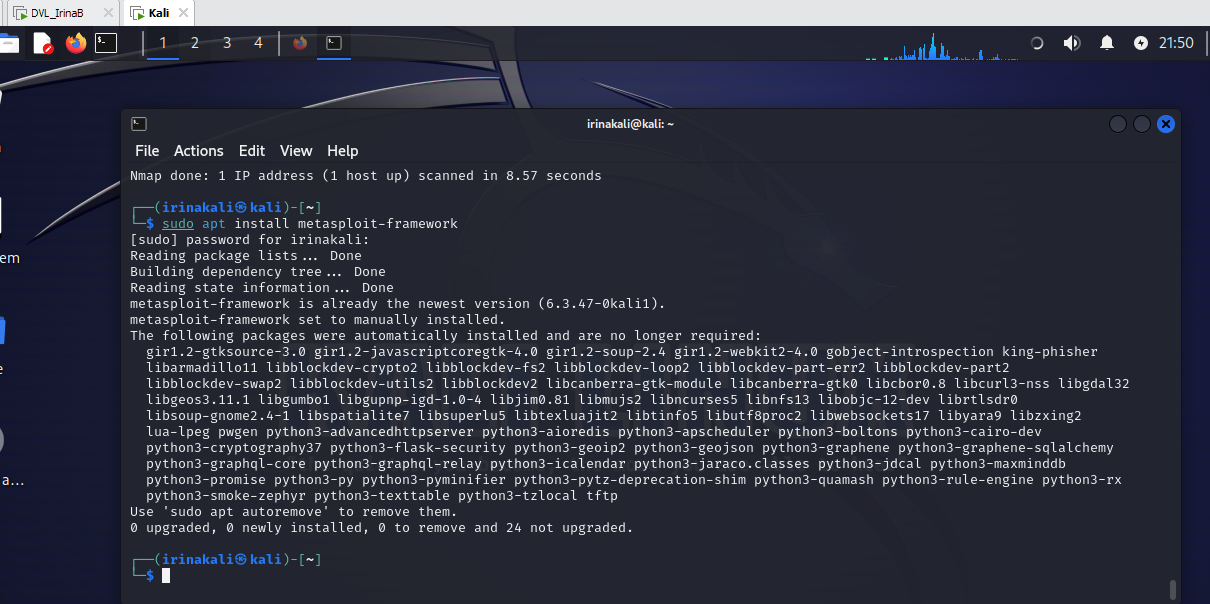


Рисунок 42 – Установка Metasploit

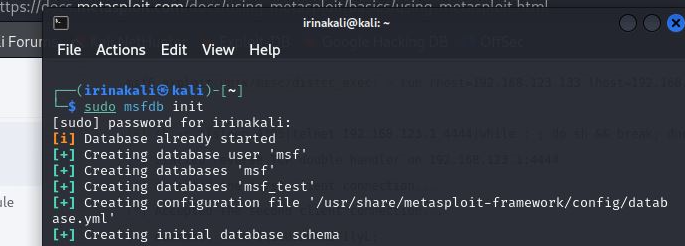


Рисунок 43 – Обновление и запуск

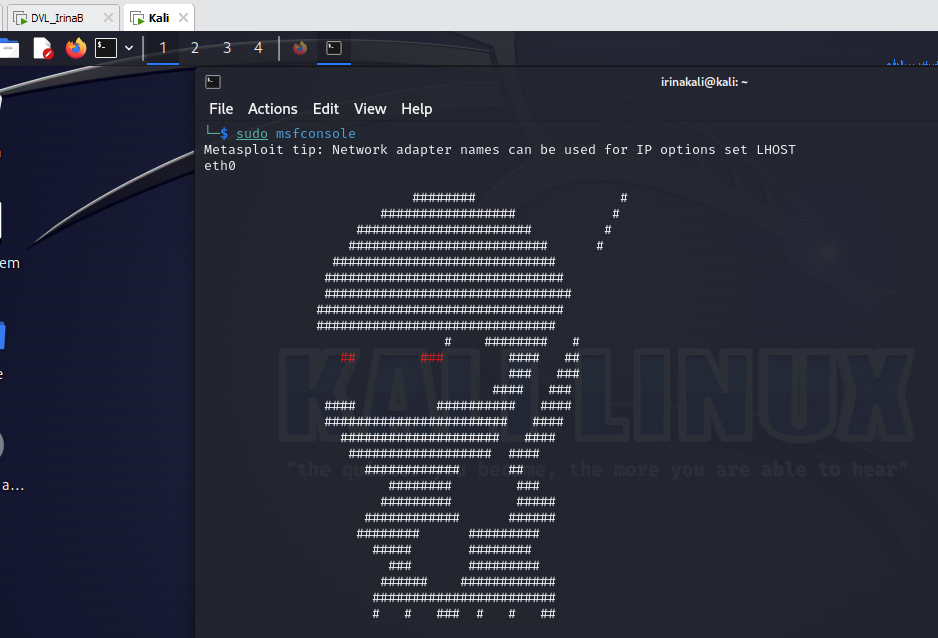
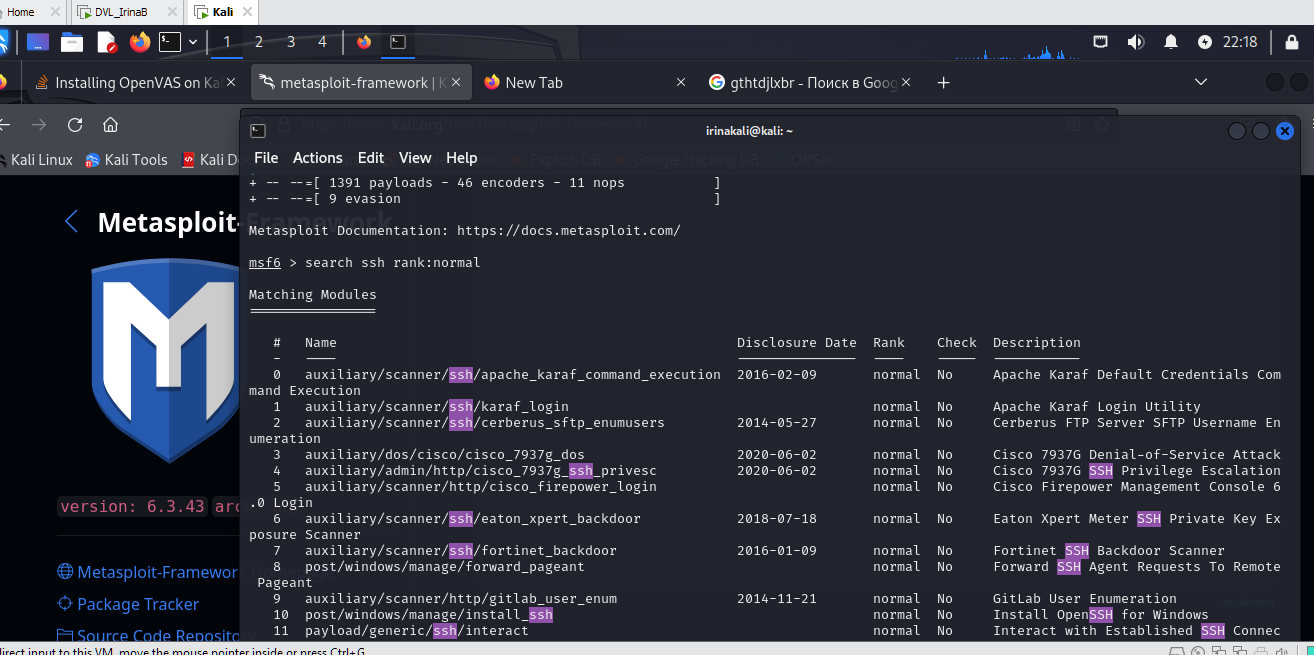




Рисунок 44 – Запуск

Посмотрим какие функциональные возможности нам предлагает утилита в отношении SSH (рис. 45).



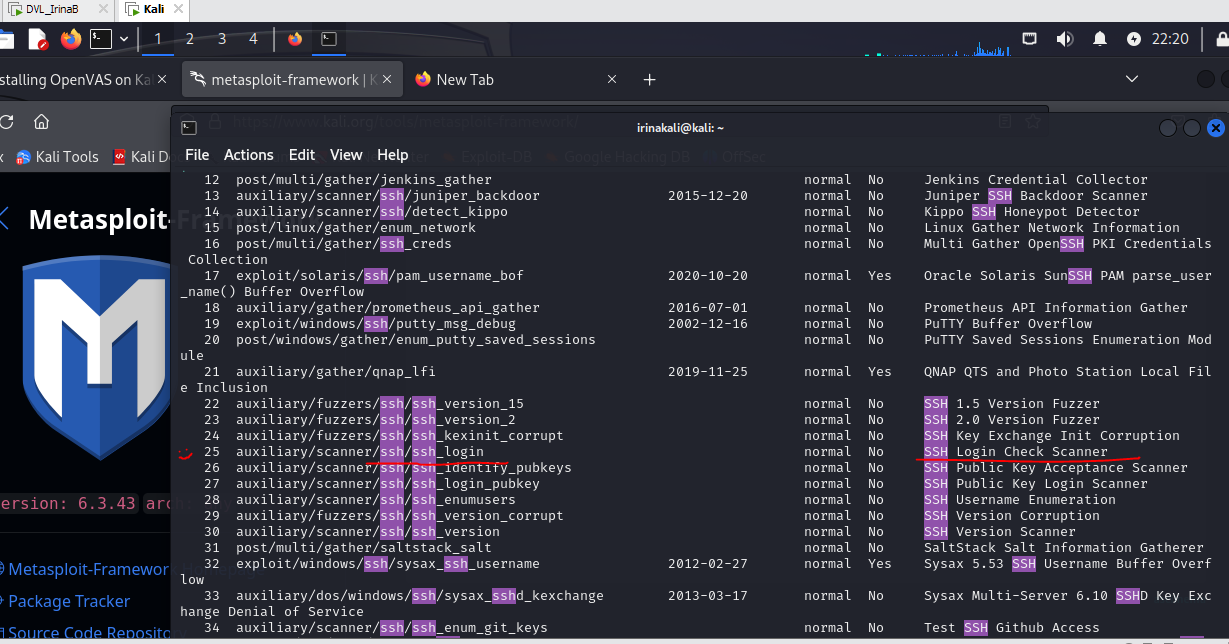


Рисунок 45 – Поиск вектора

Выберем вариант – сканер логина под номером «25», пропишем «use 25». Из представляемых функцией опций нам потребуется только указание целевого узла и подключение словаря в формате «логин пароль». Укажем необходимые опции и запустим (рис. 46).

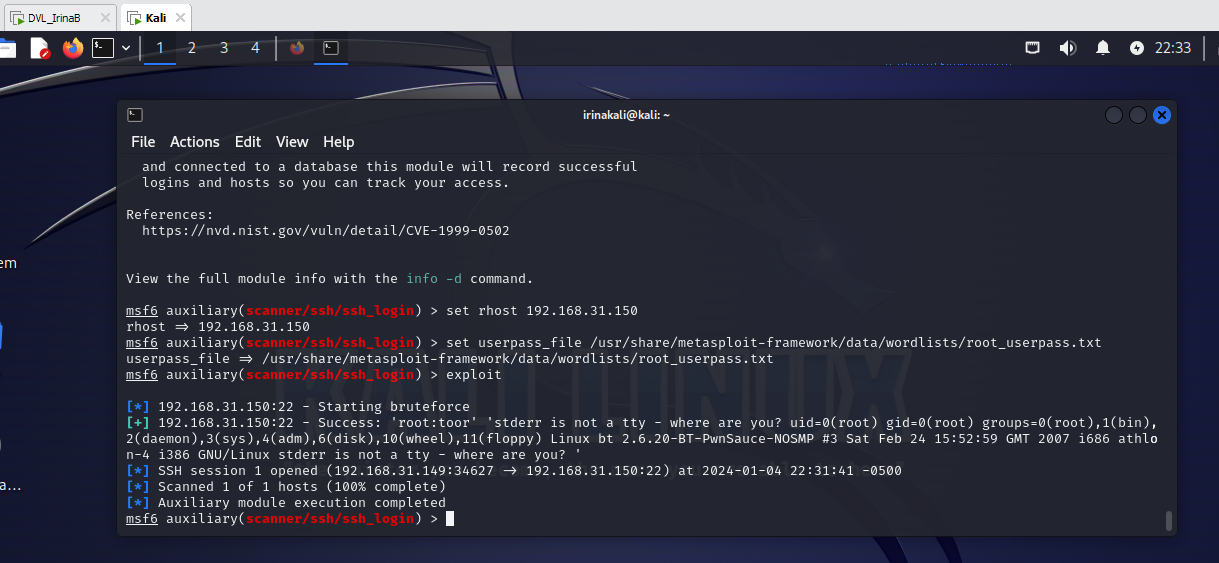


Рисунок 46 – Подготовка и запуск

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 данной уязвимости:**

1. Следует отключить учетную запись root или задать ей сложный пароль.

2. Использовать авторизацию по приватному ключу.

3. Использовать двухфакторную аутентификацию для SSH.

4. Убедиться, что на сервере и клиентских машинах установлены последние обновления безопасности для операционной системы и приложений.

5. Обновить программное обеспечение, использующее уязвимые функции, до последних версий, в которых уязвимость была исправлена.

6. Если это невозможно, отключить 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. Ограничить доступ к уязвимым функциям или службам, которые их используют, только для доверенных источников и пользователей.

8. Использовать системы предотвращения вторжений и брандмауэры для защиты от возможных атак, использующих уязвимость.

9. Постоянно следить за обновлениями безопасности и новыми угрозами, связанными с этой уязвимостью, и своевременно применять необходимые исправления.

**Заключение**

В ходе выполнения данной практической работы цель работы была достигнута и были выполнены следующие задачи:

- Сканирование сети с помощью Nmap;

- Сканирование сети с помощью OpenVAS;

- Анализ безопасности системы с помощью Metasploit.