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

Институт кибербезопасности и цифровых технологий

Практическая работа № 3.2

по дисциплине

«Управление информационной безопасностью»

**Выполнил:**

ББМО–01–22

Чадов В. Т.

**Проверил:**

Пимонов Р. В.

«Зачтено» «\_\_»\_\_\_\_\_\_\_\_\_2023 г. \_\_\_\_\_\_\_\_\_\_\_\_\_\_

Москва 2023

Содержание

Установка и настройка виртуальных машин 3

Использование инструментов анализа защищенности 14

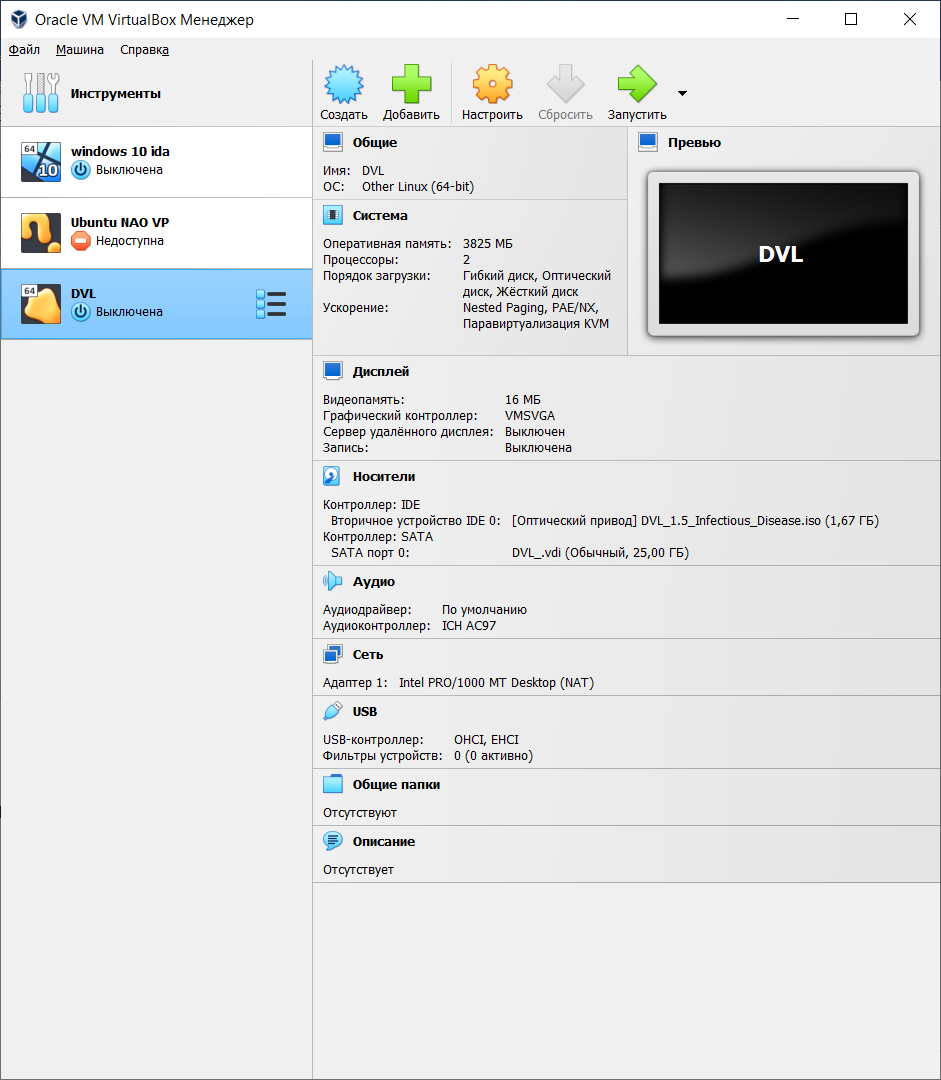
Анализ полученных результатов 21

**Установка и настройка виртуальных машин**

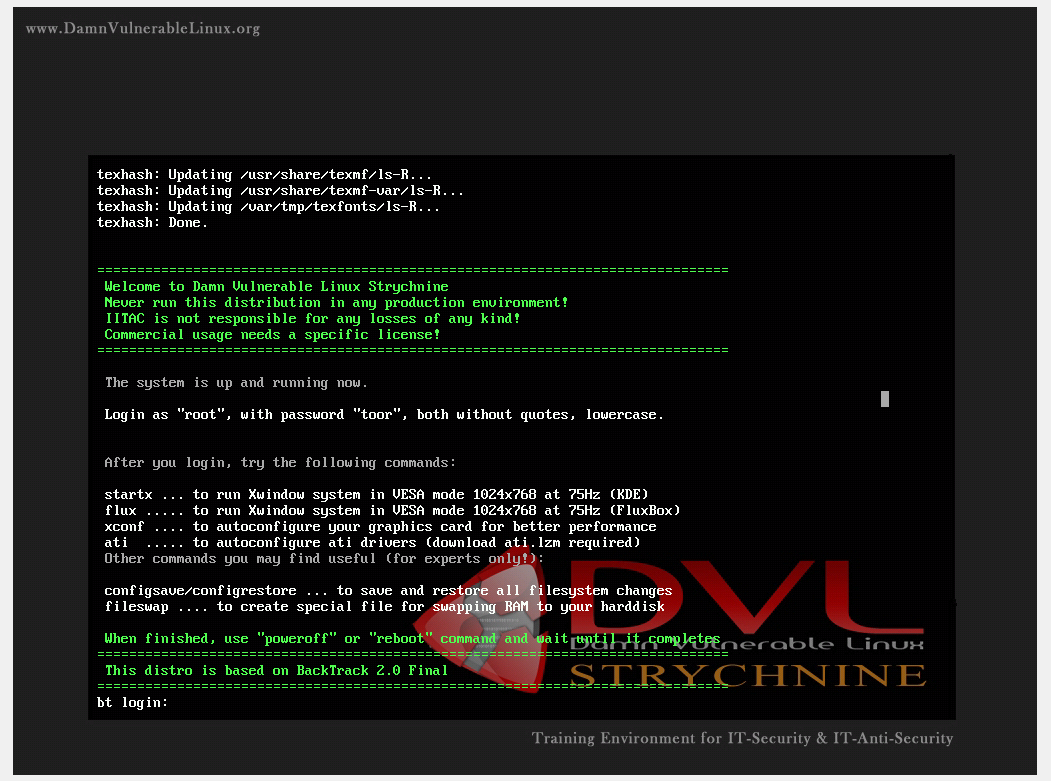
Добавим и запустим Kali linux

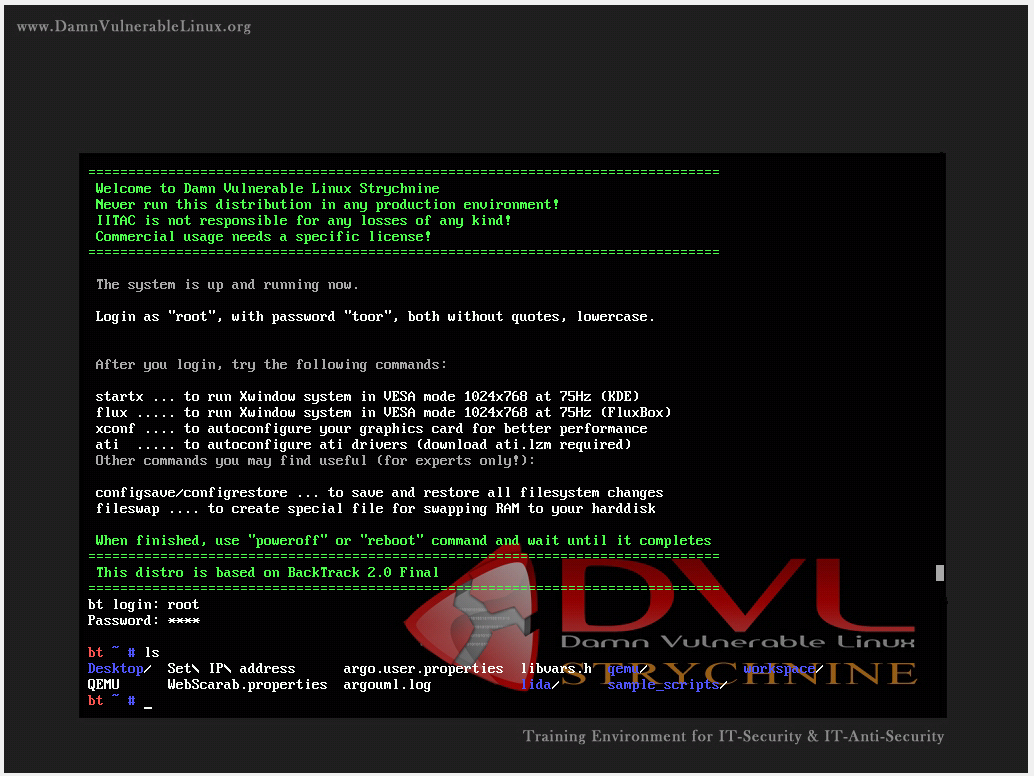


Создадим вм с DamnVulnerableLinux

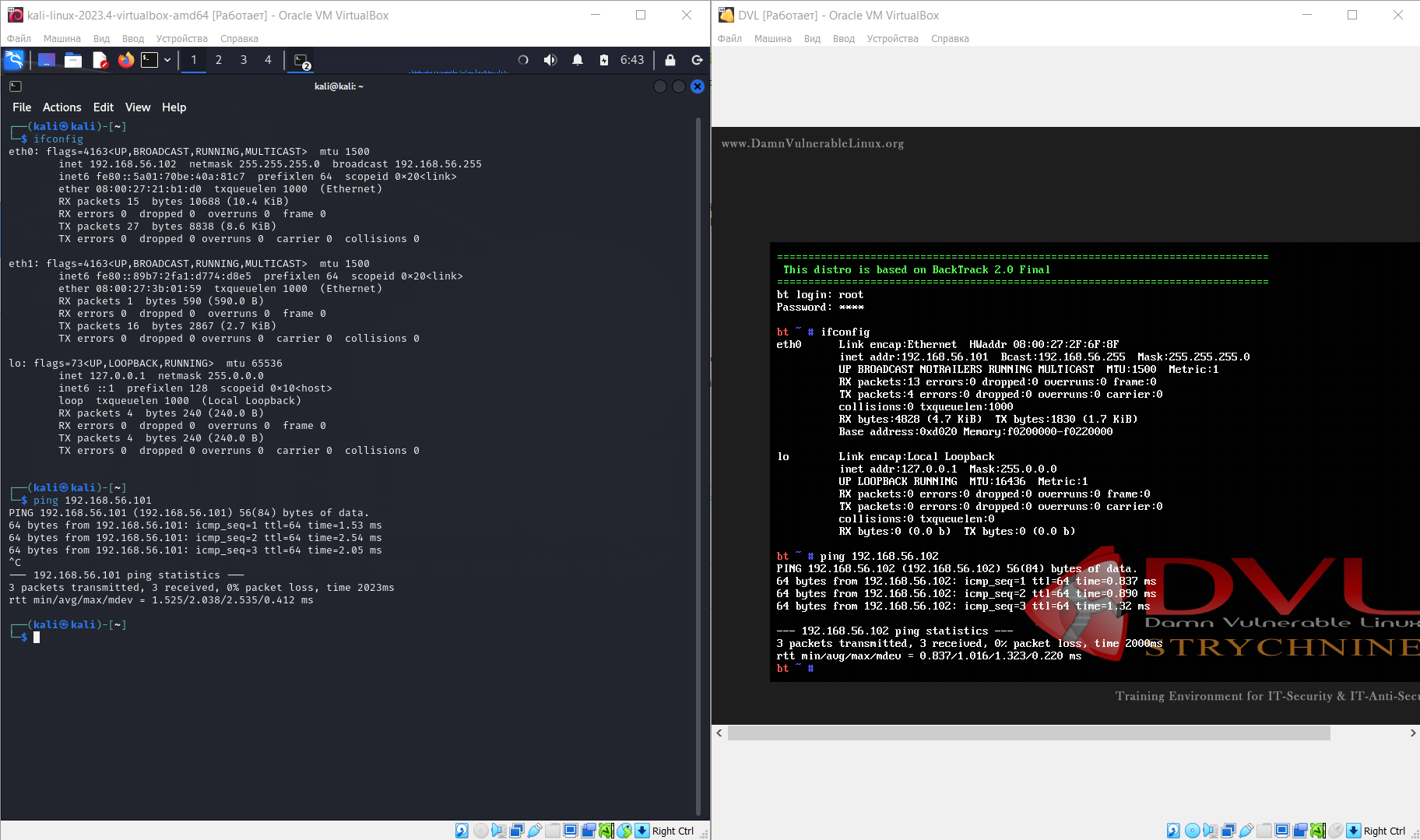


Установим все необходимое для dvl. Используя туториал для настройки <https://www.computersecuritystudent.com/SECURITY_TOOLS/DVL/lesson1/>. Требуется авторизация root/toor

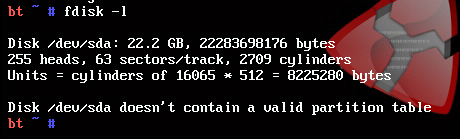


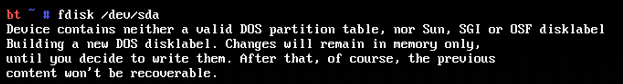


Проверим что у вм есть доступ к сети и друг другу



Настроим DVL, выведем fdisk -l и видим отсутствие таблицы разделов, создадим новую

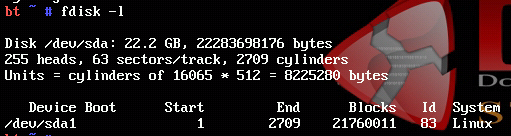




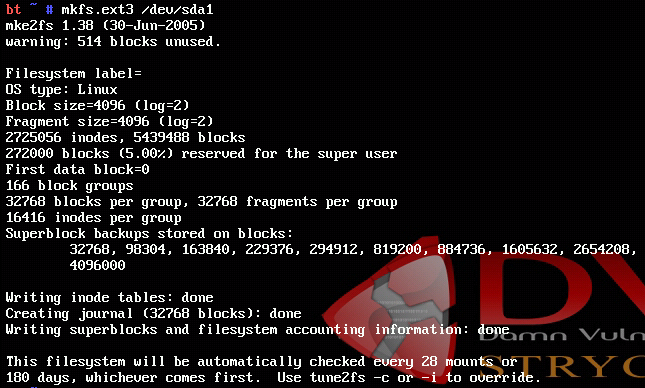




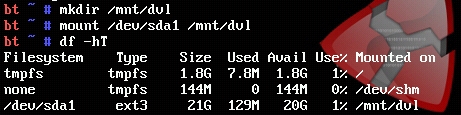
Видим новую таблицу разделов



Отформатируем диск



Создадим директорию /mnt/dvl и примонтируем туда созданный раздел /dev/sda1



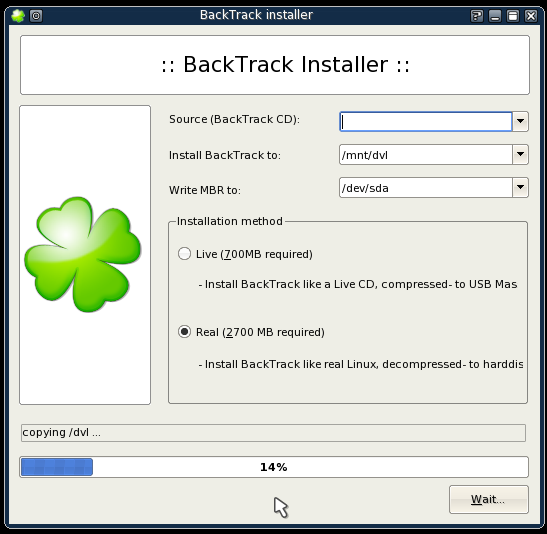
Запустим графическую оболочку



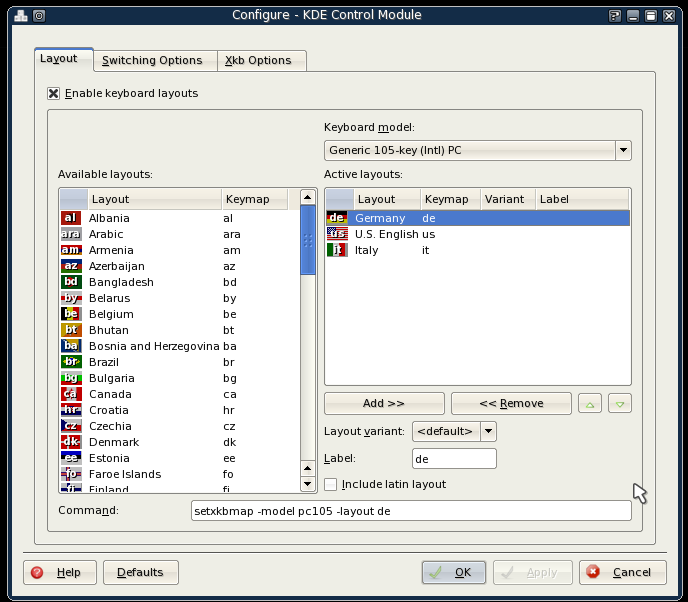
Запустим BackTrack Installer



Установим с параметрами как на картинке



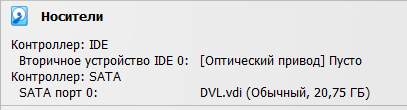
Также подправим сломавшуюся раскладку клавиатуры только на US



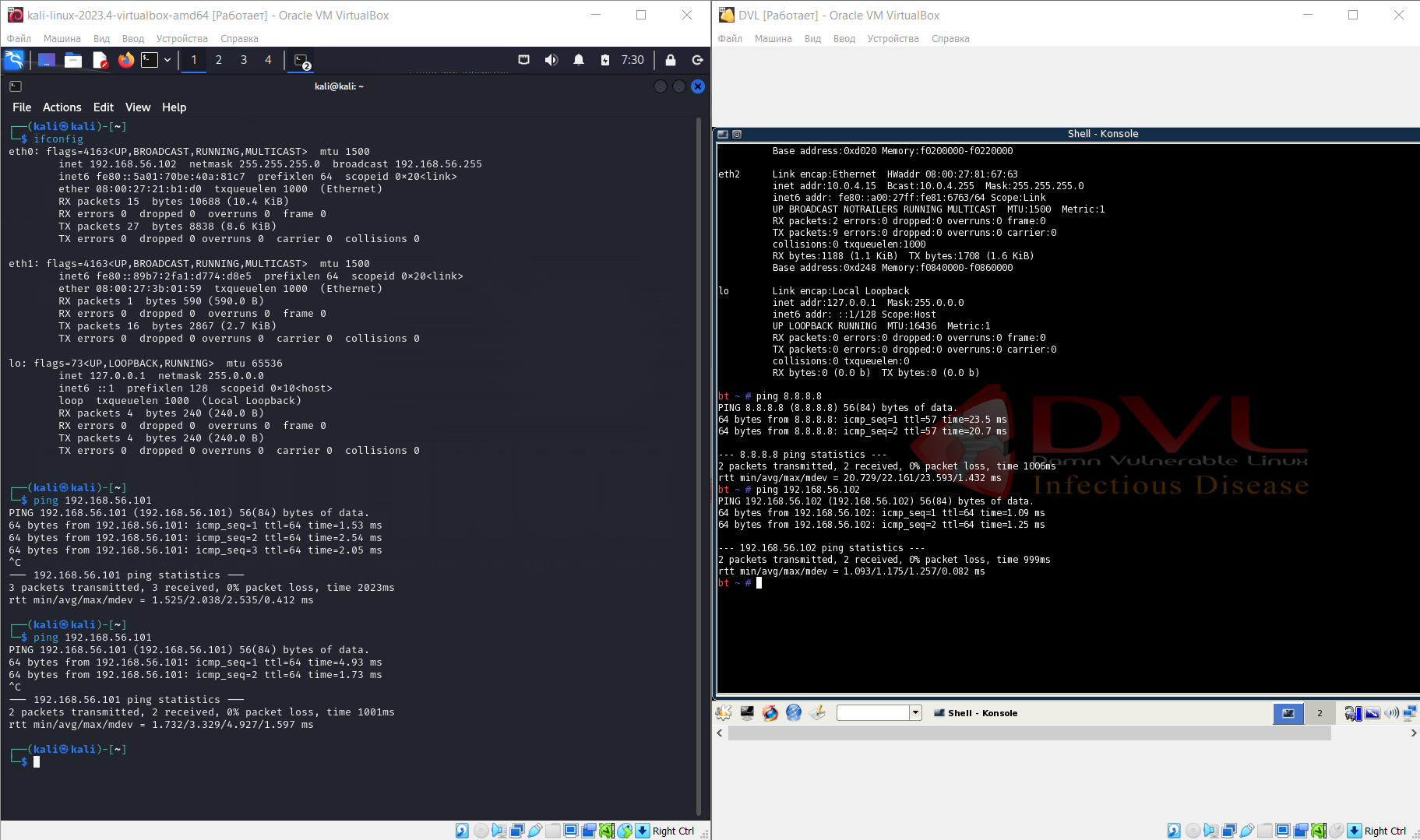
Установим boot loader при помощи lilo



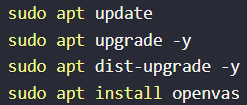
Перезапустим вм и отключим iso файл

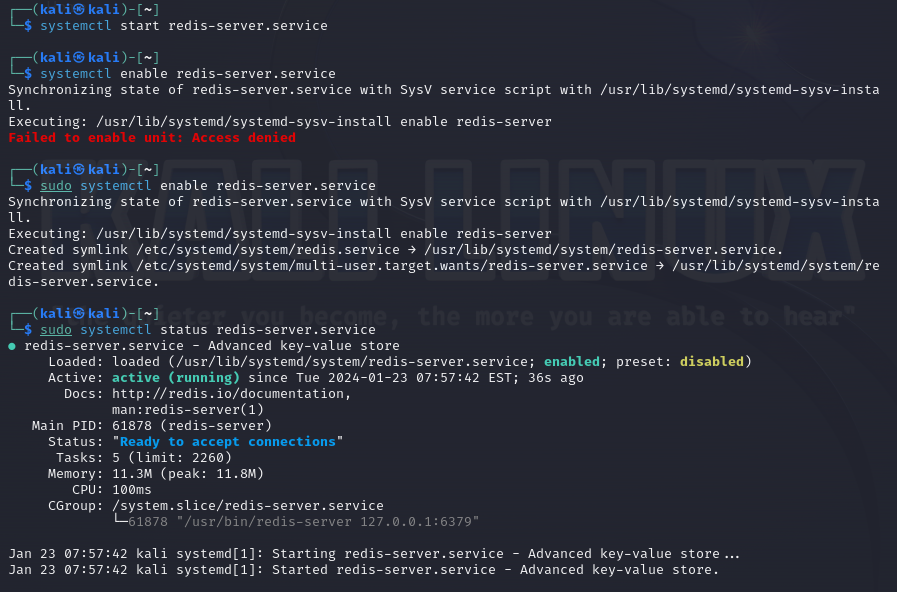


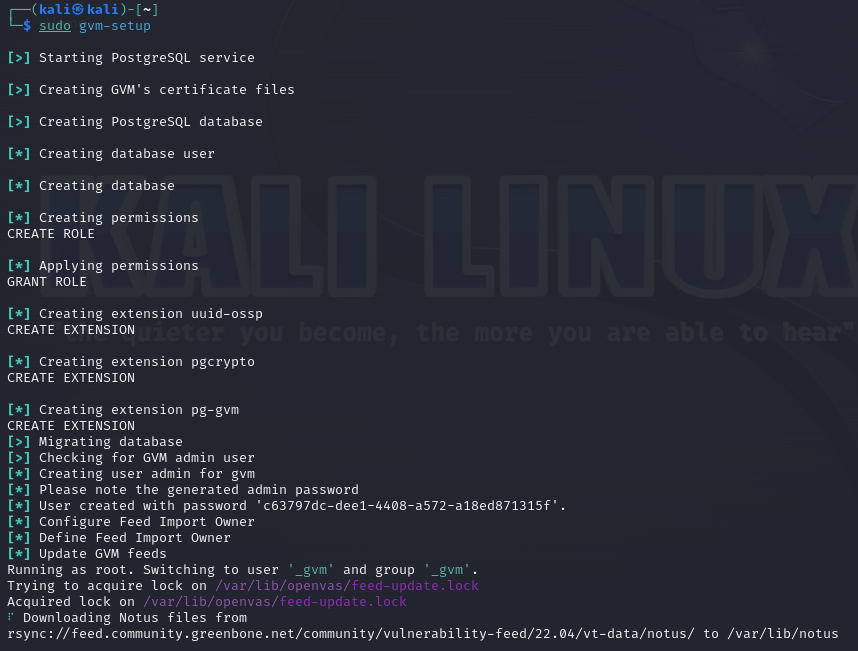
Повторно проверим соединение и подключение к интернету

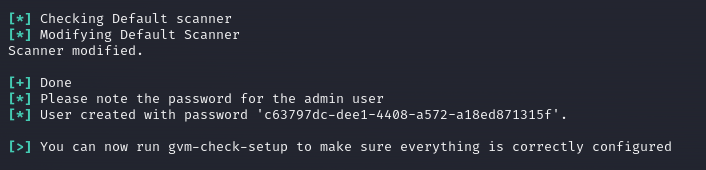


Установим openvas для kali linux



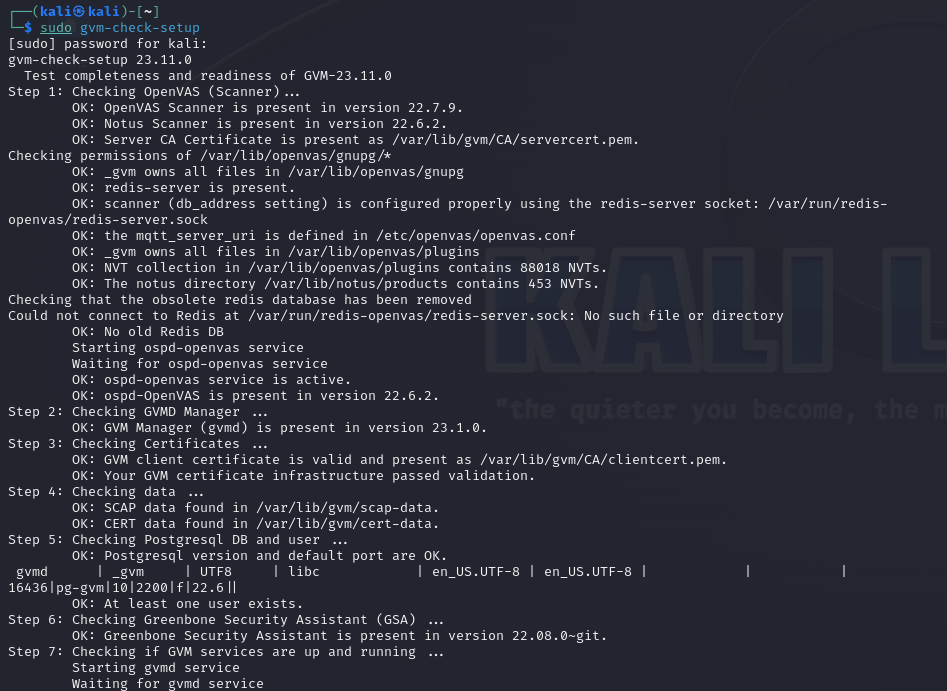




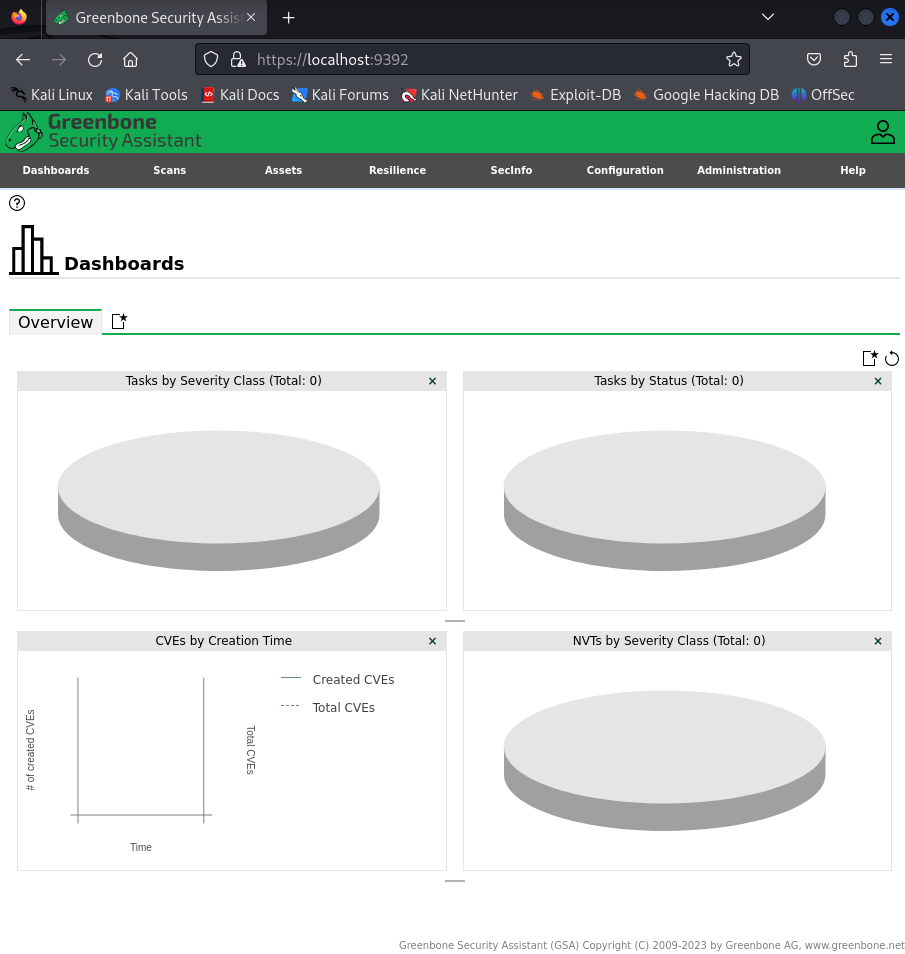


c63797dc-dee1-4408-a572-a18ed871315f

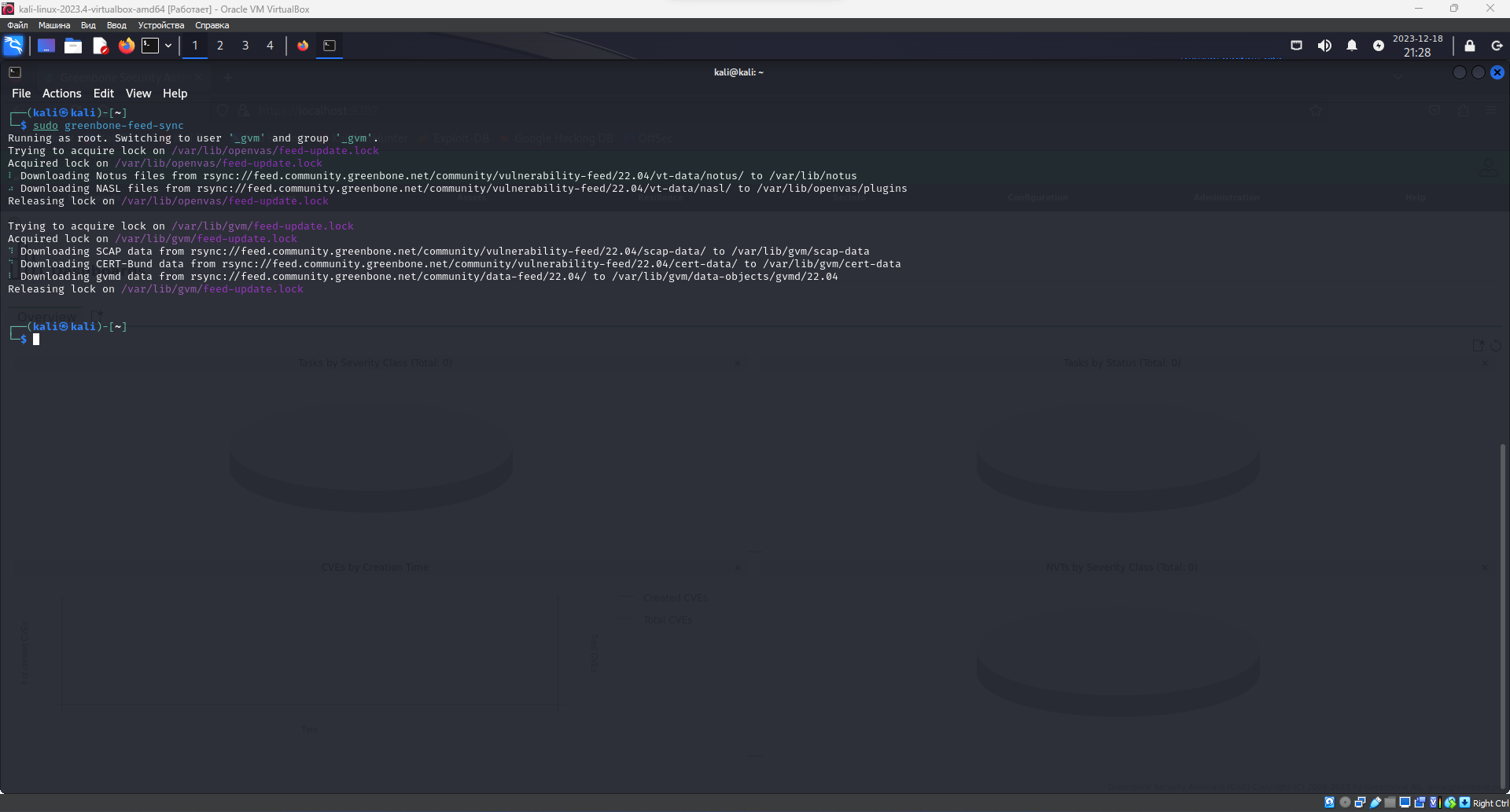
Проверим корректность установки

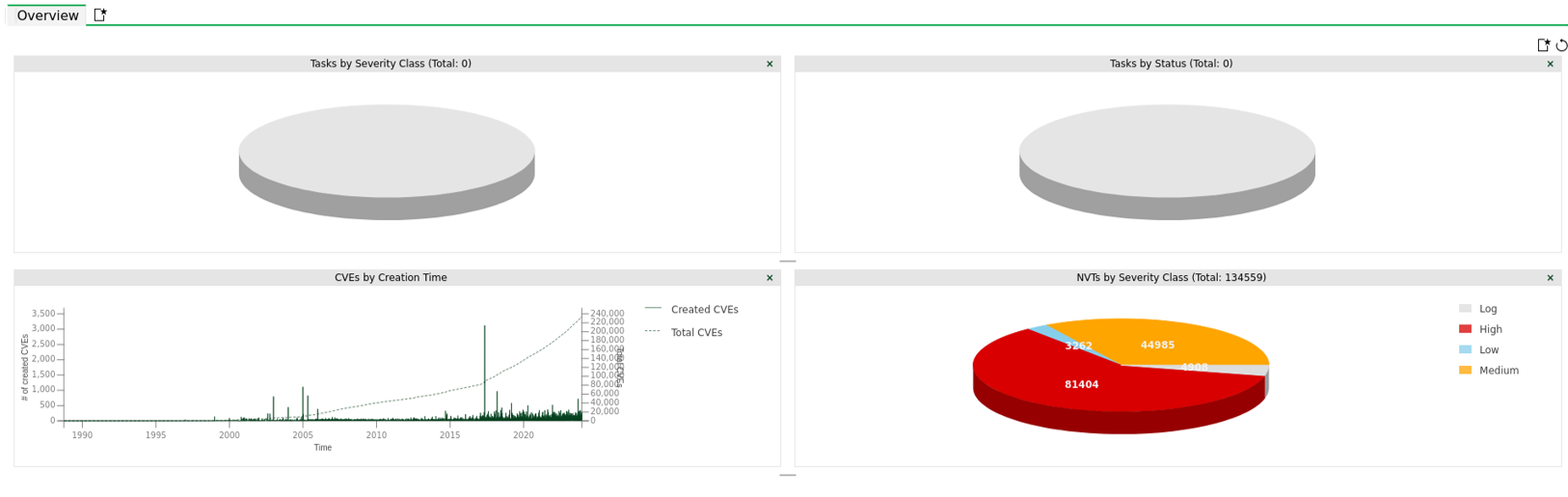


Войдем в интерфейс приложения



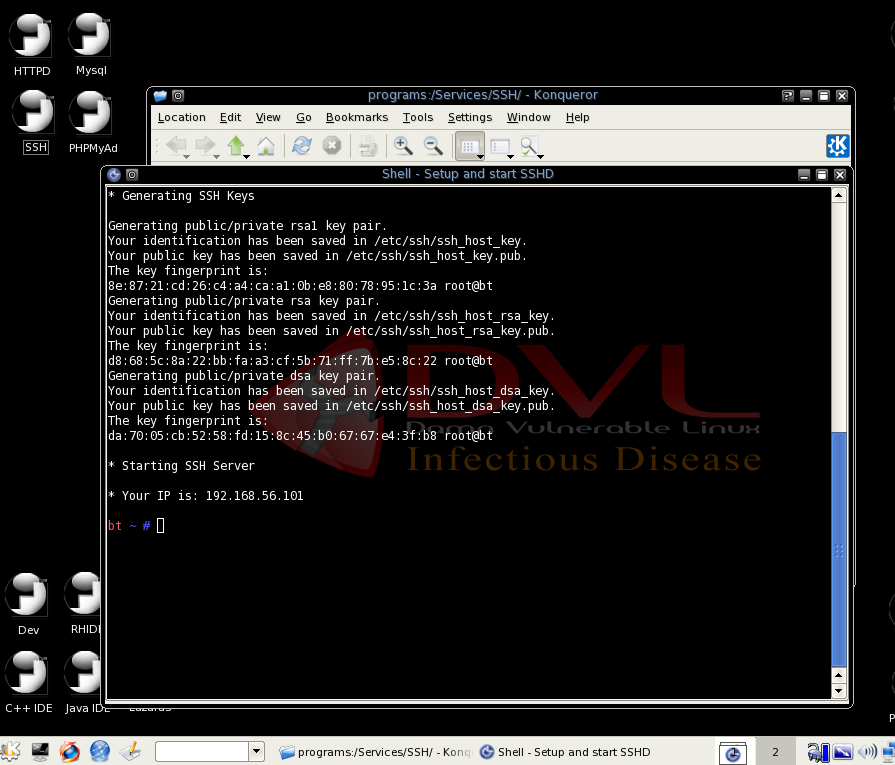
Обновим базы данных openvas



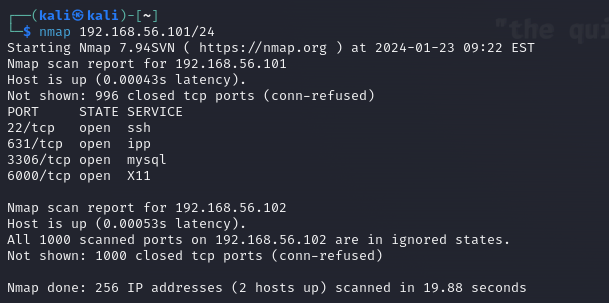


**Использование инструментов анализа защищенности**

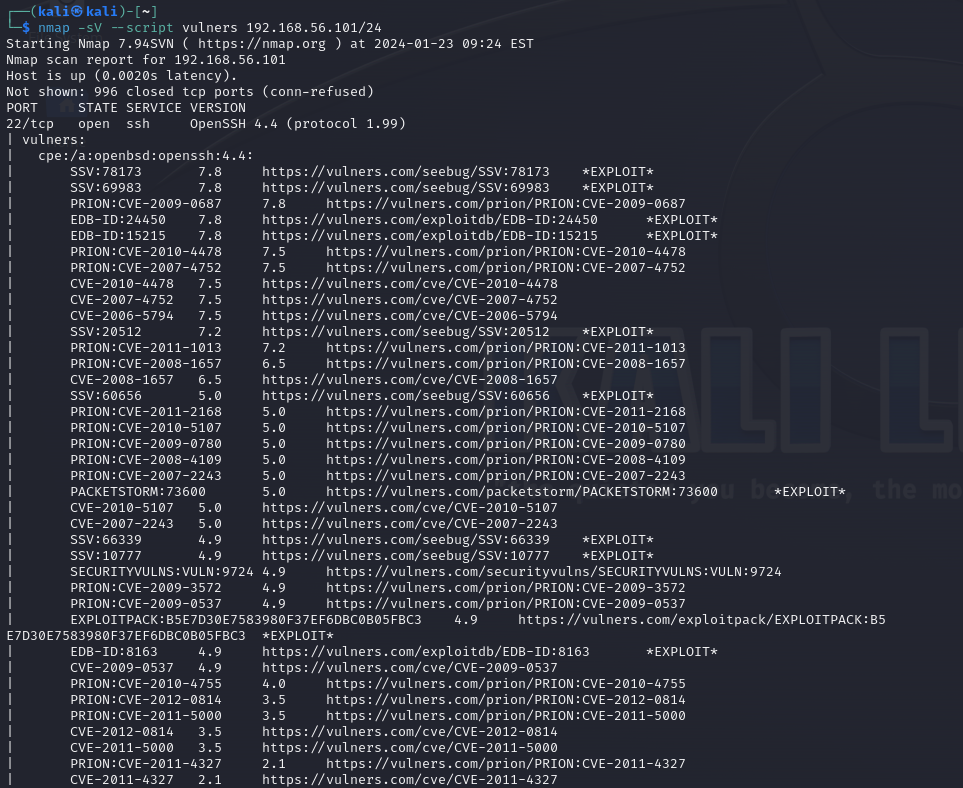
Запустим ssh server на dvl

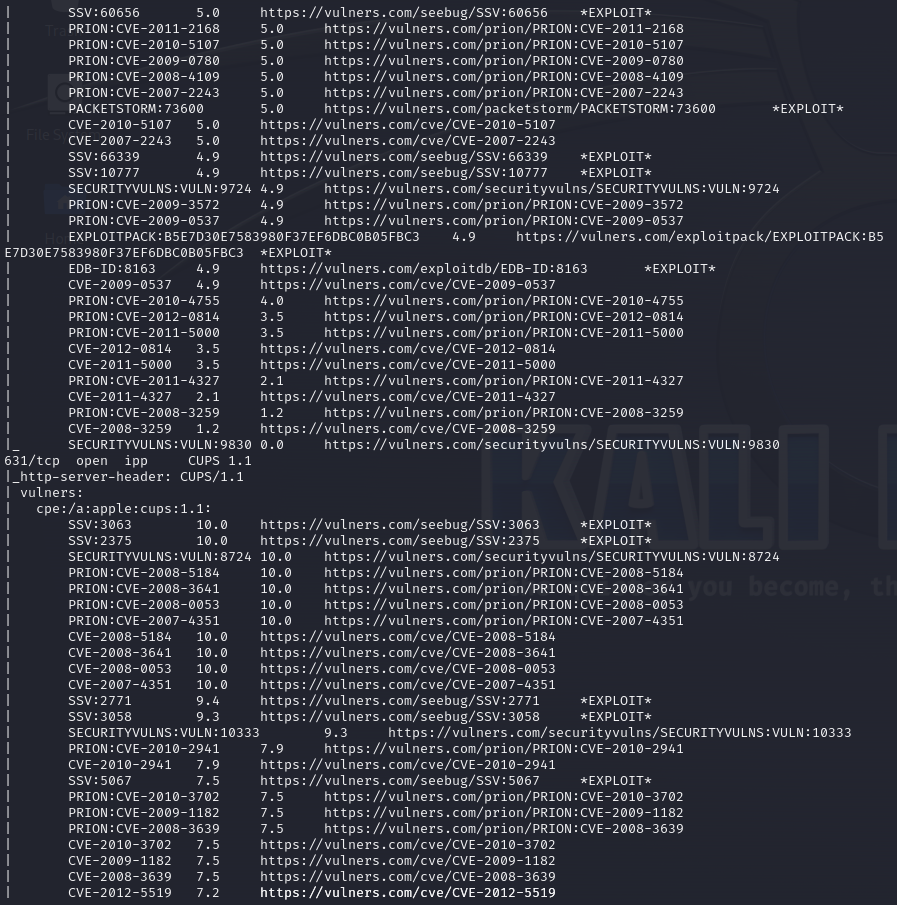


Просканируем dvl через nmap, видим открытые порты



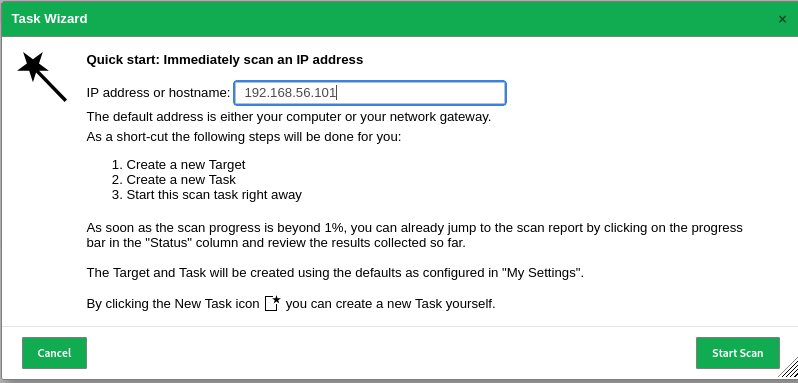
Просканируем при помощи скрипта vulners, уязвимости найденные nmap



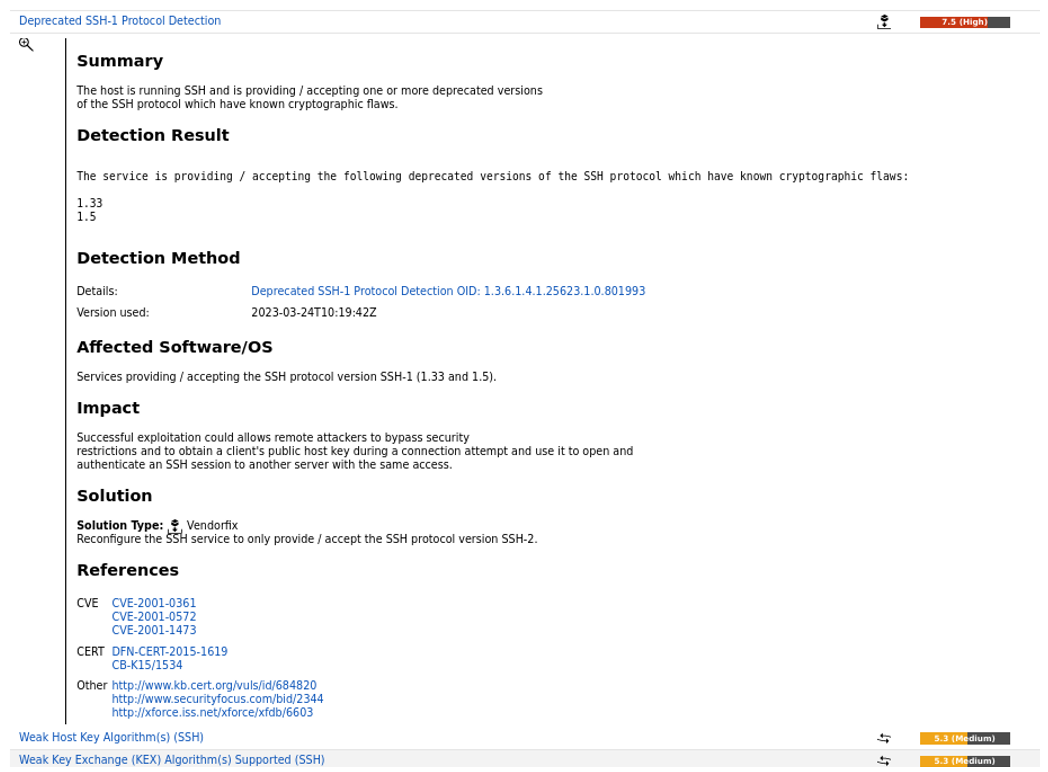




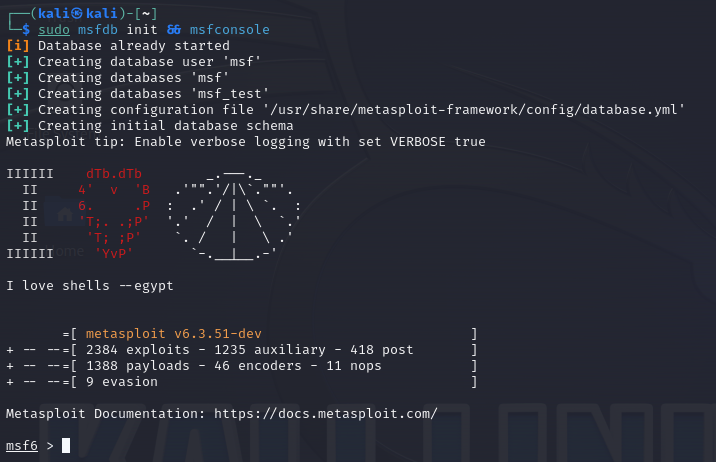
Просканируем через openvas



Видим критическую уязвимость ssh



Запустим Metasploit

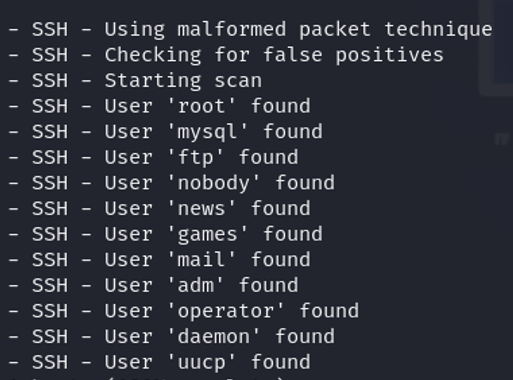


Отобразим информацию по выбранной уязвимости и выполним настройку





Результат выполнения эксплойта – список пользователей ssh dvl. Рекомендация по исправлению – обновить OpenSSH до последней версии.



**Анализ полученных результатов**

OpenVAS и Nmap - это инструменты для обнаружения уязвимостей в сети, но они имеют разные подходы и функциональность.

OpenVAS - это полноценная система управления уязвимостями, которая включает в себя OpenVAS-manager, OpenVAS-scanner и Greenbone-security-assistant. OpenVAS предлагает широкий спектр функций, таких как:

* Поиск уязвимостей на основе базы данных CVE
* Поиск уязвимостей с использованием скриптов NSE (Nmap Scripting Engine)
* Создание детальных отчетов о сети
* Поддержка различных политик сканирования

В то же время, OpenVAS является более сложным и глубоким инструментом, который может быть более уязвим к ошибкам и проблемам в сравнении с Nmap.

Nmap - это инструмент для обнаружения уязвимостей, который предоставляет более ограниченный набор функций, но может быть использоваться в сочетании с другими инструментами, такими как Vulners. Nmap может использоваться для обнаружения уязвимостей с помощью скриптов NSE, но его основная сила заключается в сканировании сети и обнаружении открытых портов и уязвимостей.

В нашем конкретном случае Nmap нашла значительно больше уязвимостей, однако основная причина в OpenvVAS включен скудный набор параметров сканирования по умолчанию.

Как OpenVAS, так и Nmap являются инструментами с открытым исходным кодом, что позволяет пользователям свободно использовать их для обнаружения уязвимостей.

В целом, OpenVAS предлагает более полную функциональность для управления уязвимостями, включая создание детальных отчетов и поддержку различных политик сканирования. В то же время, Nmap может быть использоваться для обнаружения уязвимостей с помощью скриптов NSE, но его функциональность ограничена сканированием сети и обнаружением открытых портов. Также Nmap значительно более быстра, что дает ей преимущество при поиске уязвимостей в большой сети.

В итоге, оба инструмента лучше использовать вместе для более полного обнаружения уязвимостей. Например, результаты, полученные с помощью Nmap, могут быть использованы в OpenVAS для более глубокого анализа уязвимостей.

Metasploit — это мощный фреймворк для исследования уязвимостей в сетях и приложениях, который может быть использован как киберпреступниками, так и специалистами по информационной безопасности. Он предоставляет широкий спектр инструментов для сканирования, обнаружения уязвимостей, эксплуатации и управления безопасностью. Metasploit Framework является открытым исходным кодом и может быть легко настроен и использован на большинстве операционных систем. Он также предлагает готовые модули и возможность создания собственных надстроек. Metasploit широко используется специалистами по безопасности для проверки уровня защиты сетей и приложений.