|  |
| --- |
| https://lh4.googleusercontent.com/tS5cTTevL4ZZD-Y6EQWokctOq3SQO-C0kzxGBmhAvcwDsnVe_mD6kMaIbo1W2N-HCZRZDIBs8XXcMbgzyjXUr_vv9zc_X3YJ6yEbhuzmVoDtDBmbCAuitSejeymhPd2H8OfWhLB2 |
| МИНОБРНАУКИ РОССИИ |
| Федеральное государственное бюджетное образовательное учреждение  высшего образования  **«МИРЭА – Российский технологический университет»**  **РТУ МИРЭА** |

ИКБ «Киберразведка и противодействие угрозам с применением технологий искусственного интеллекта» 10.04.01

Кафедра КБ-4 «Интеллектуальные системы информационной безопасности»

# Практическая работа №3.2

по дисциплине

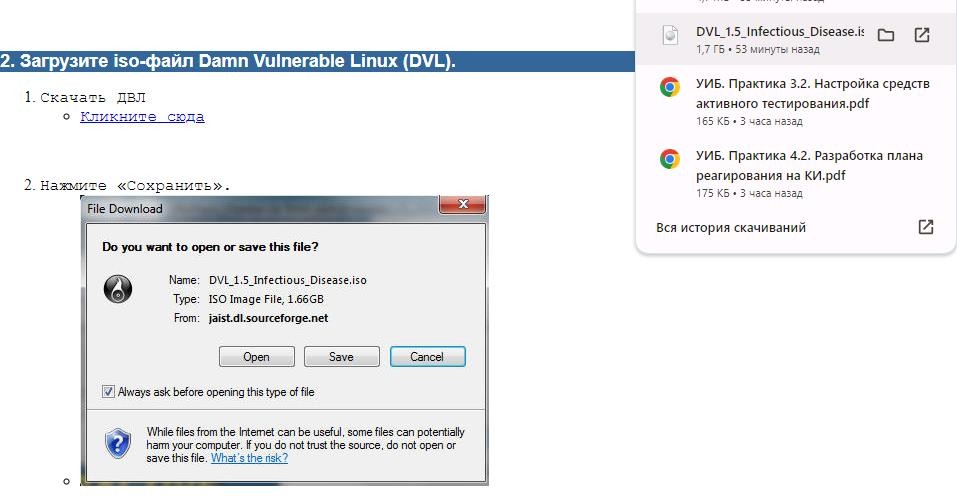
«Управление информационной безопасностью»

Группа: ББМО-02-22 Выполнил: Давыдов И.Д

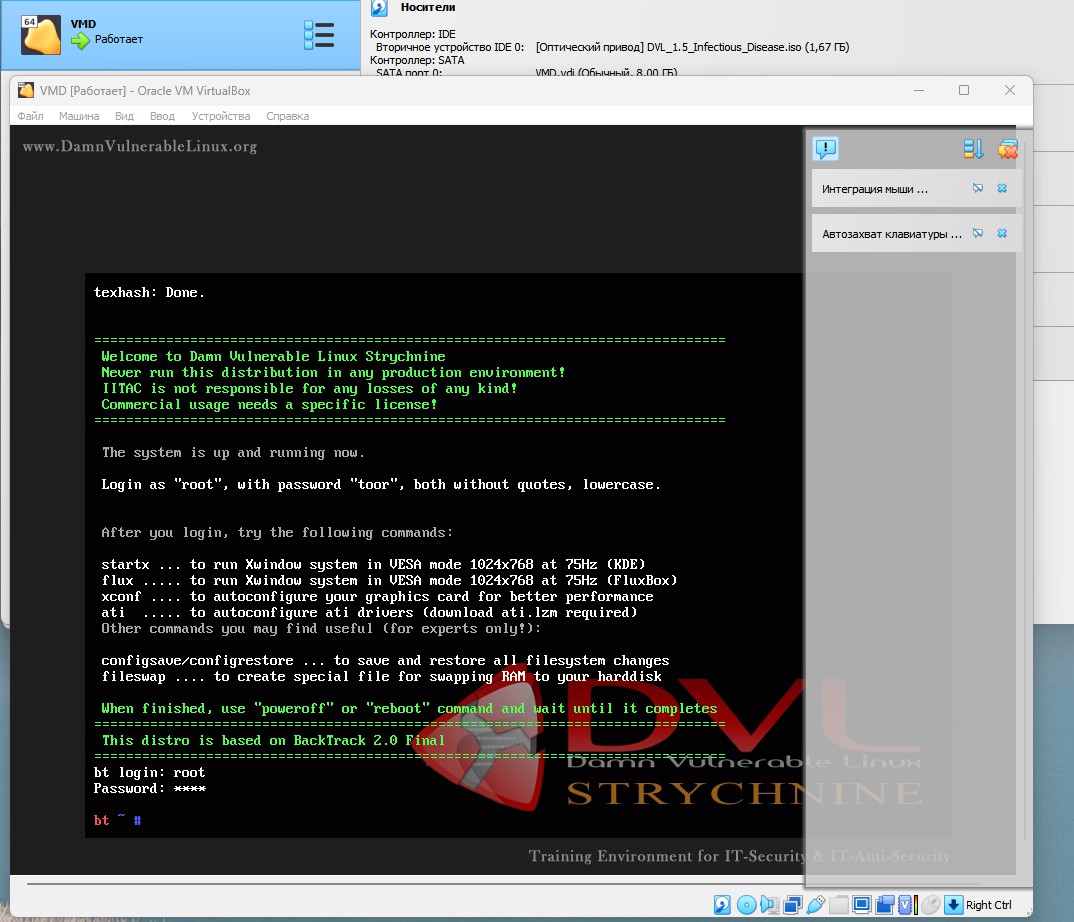
Проверил: Пимонов Р.В.

# Москва 2024

**Ход работы**

Установка ВМ (виртуальной машины) Damn Vulnerable Linux (DVL):

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



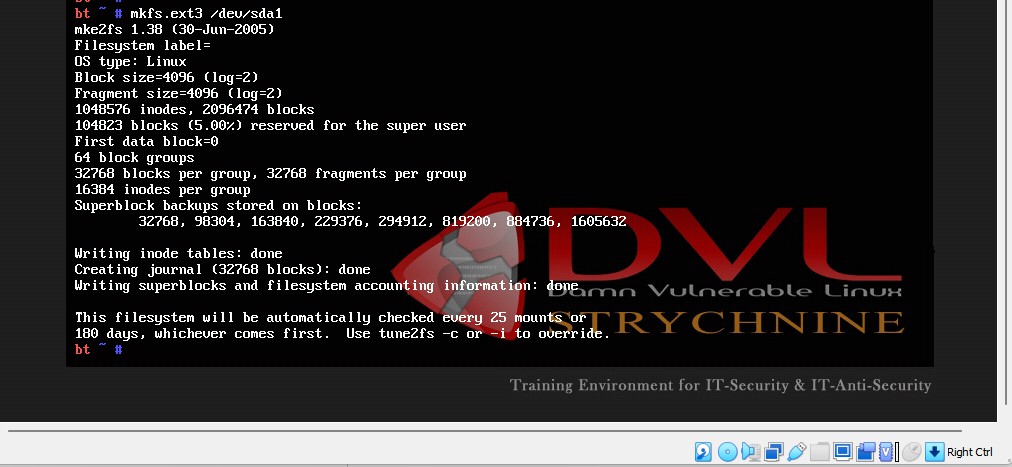
Root; Toor

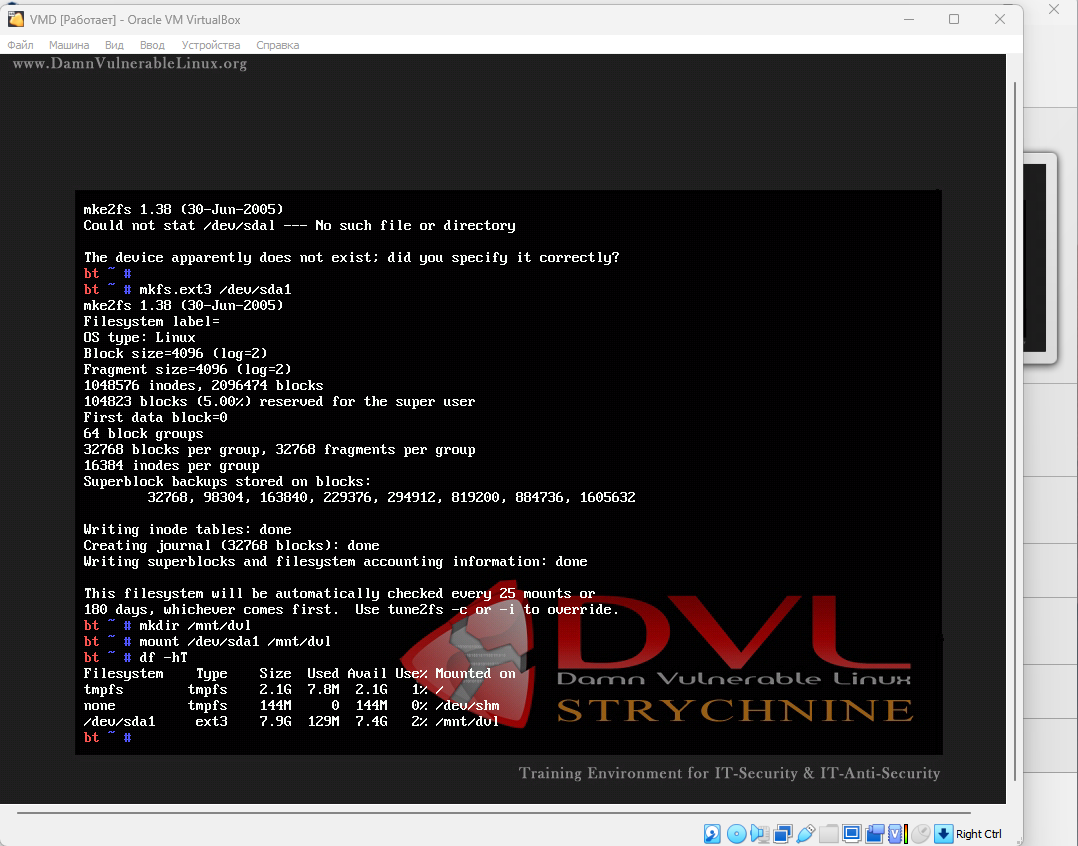
Выведем все разделы на выбранном устройстве. Увидим запись о том, что диск

/dev/sda не содержит допустимую таблицу разделов:

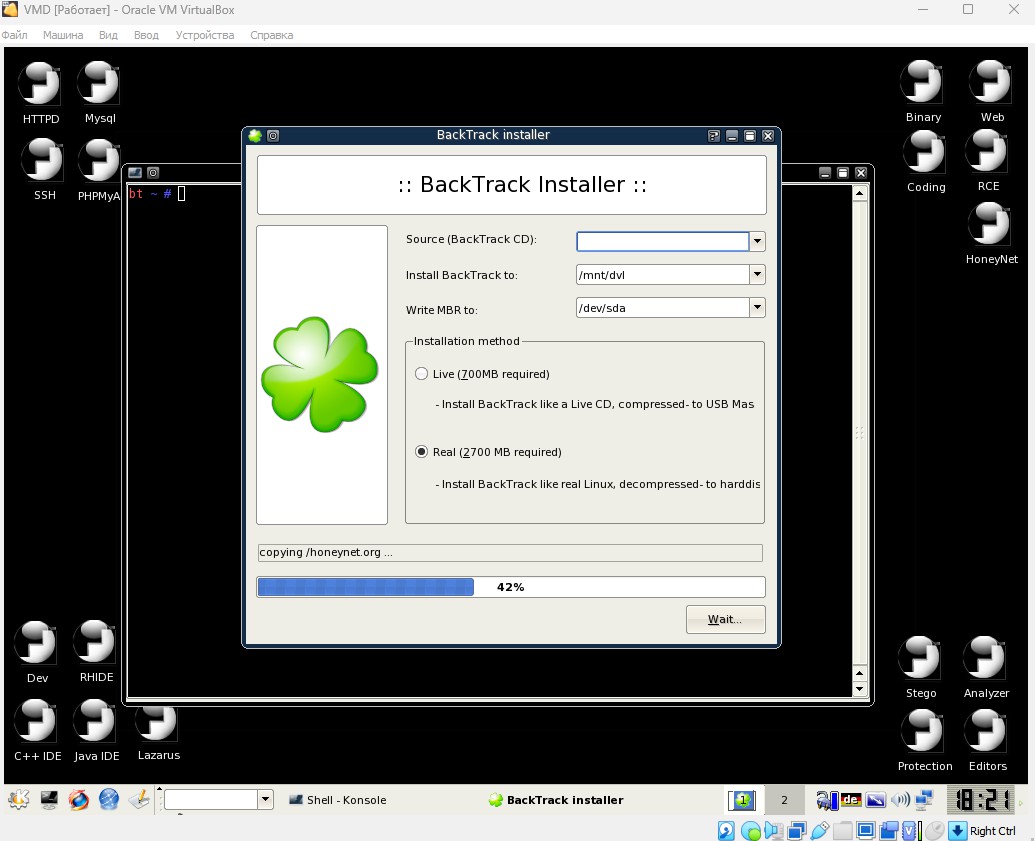


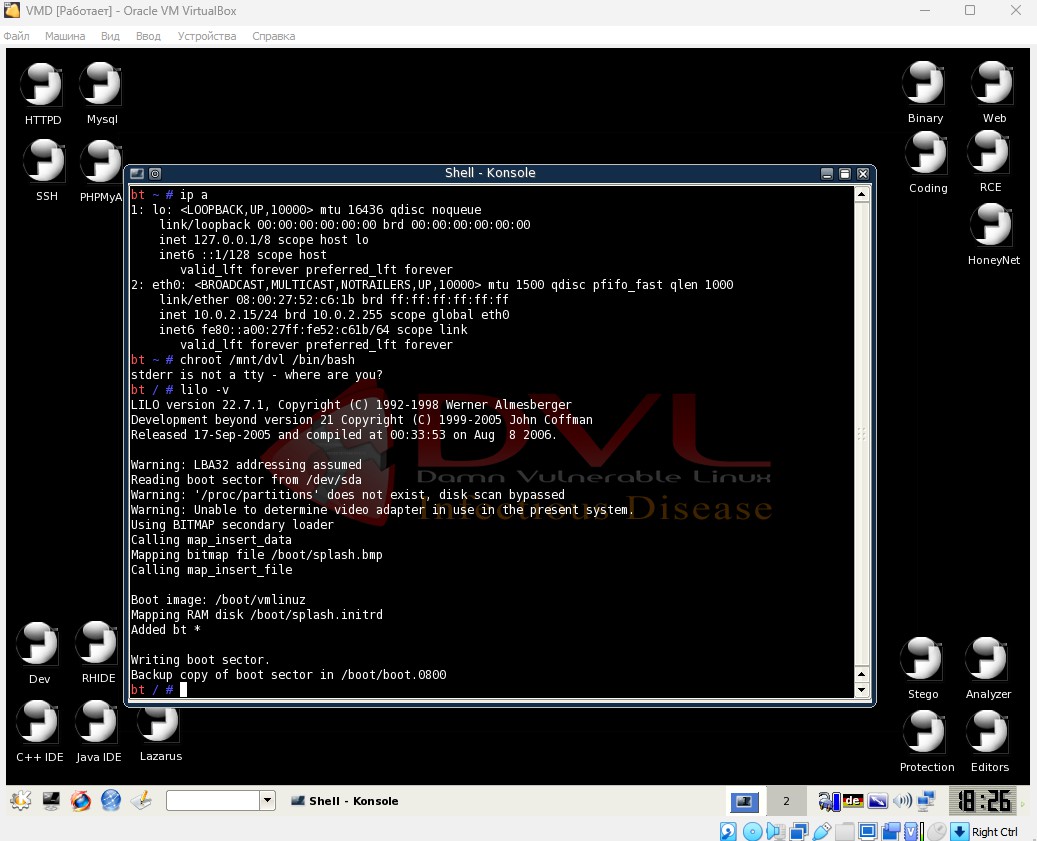
Форматируем диск



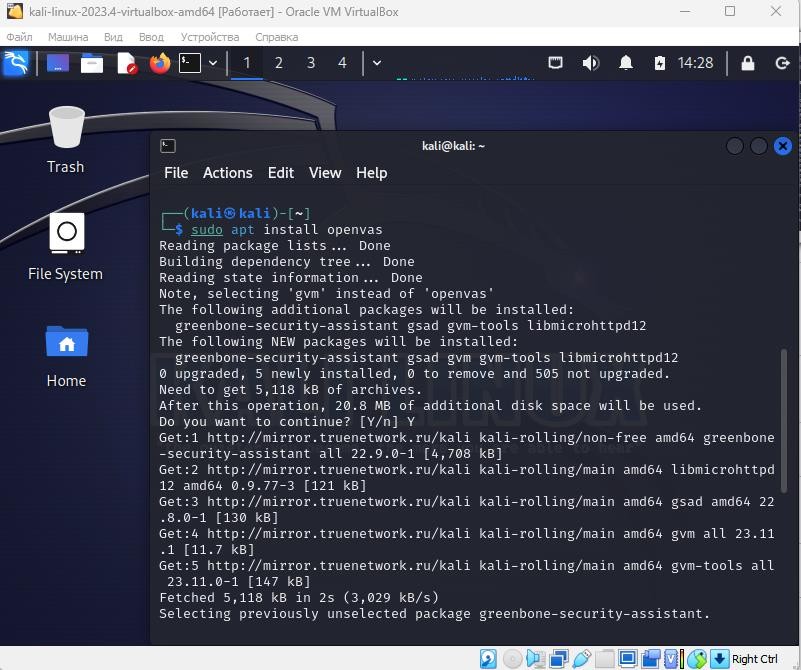
Создадим директорию /mnt/dvl и монтируем туда созданный раздел /dev/sda1:

Запустим оконную систему

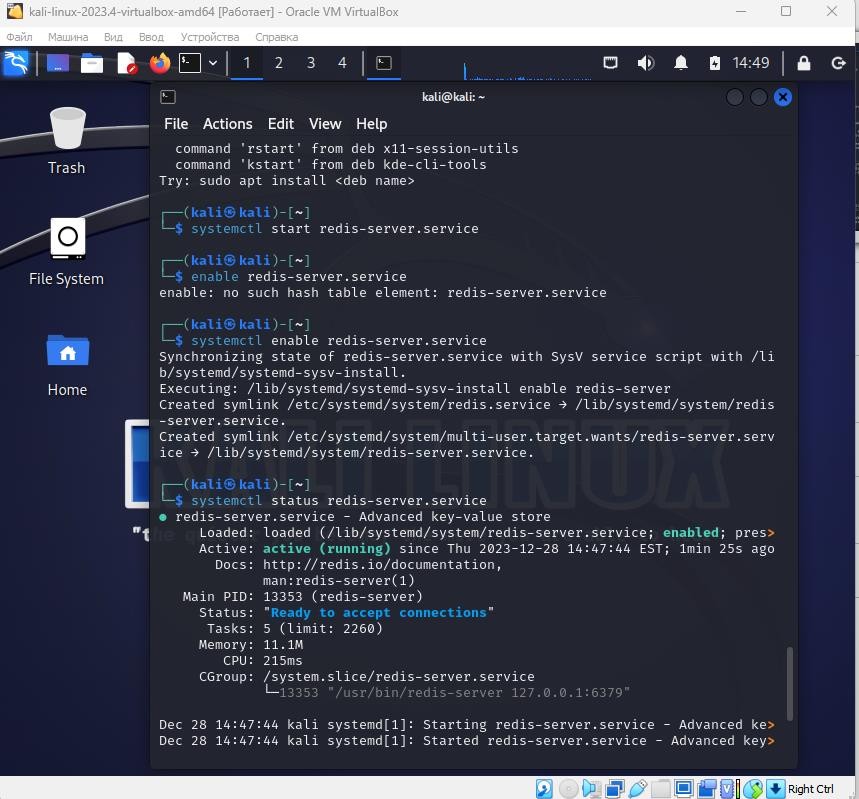


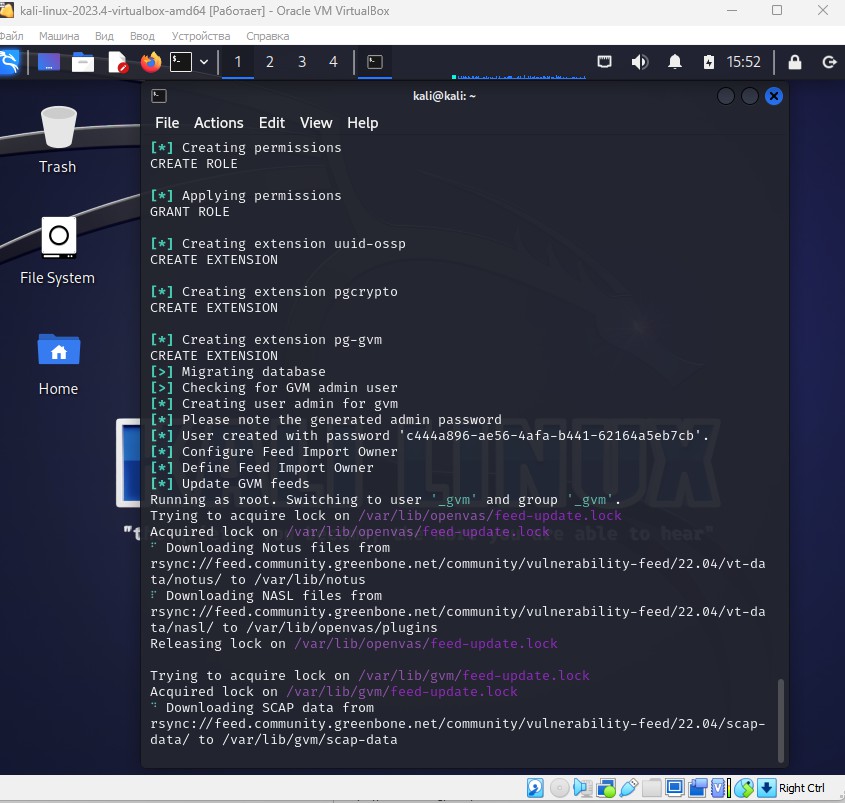
Создадим chroot среду и установим загрузчик операционной системы (ОС) с помощью lilo:

Выйдем из chroot среды и выключим ВМ Установим сканер OpenVAS на Kali Linux

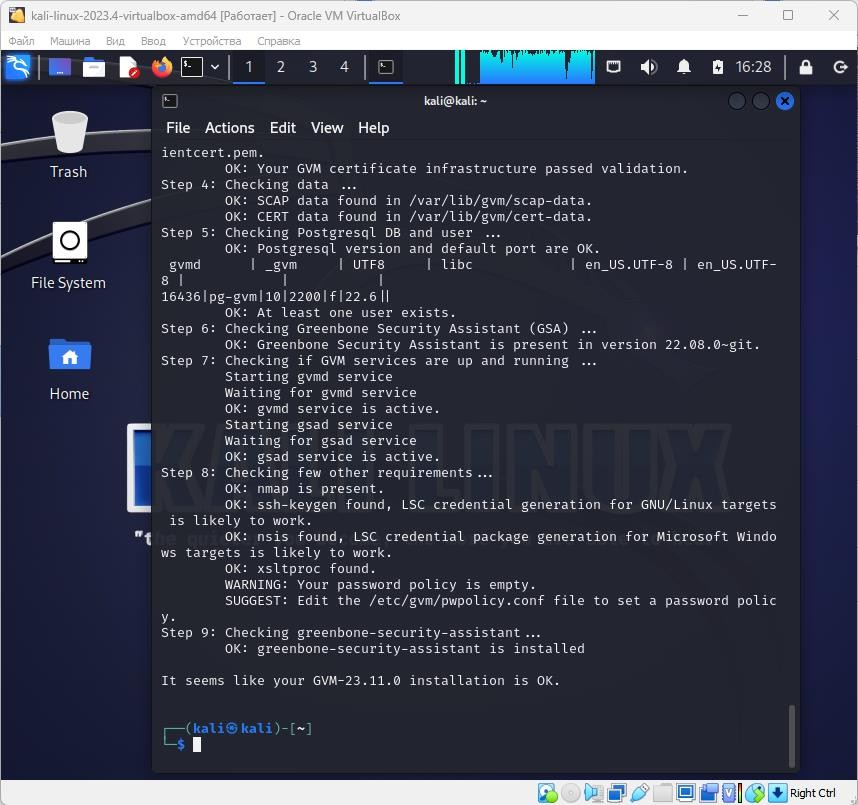


Запустим базу данных redis и включим её запуск после старта ОС

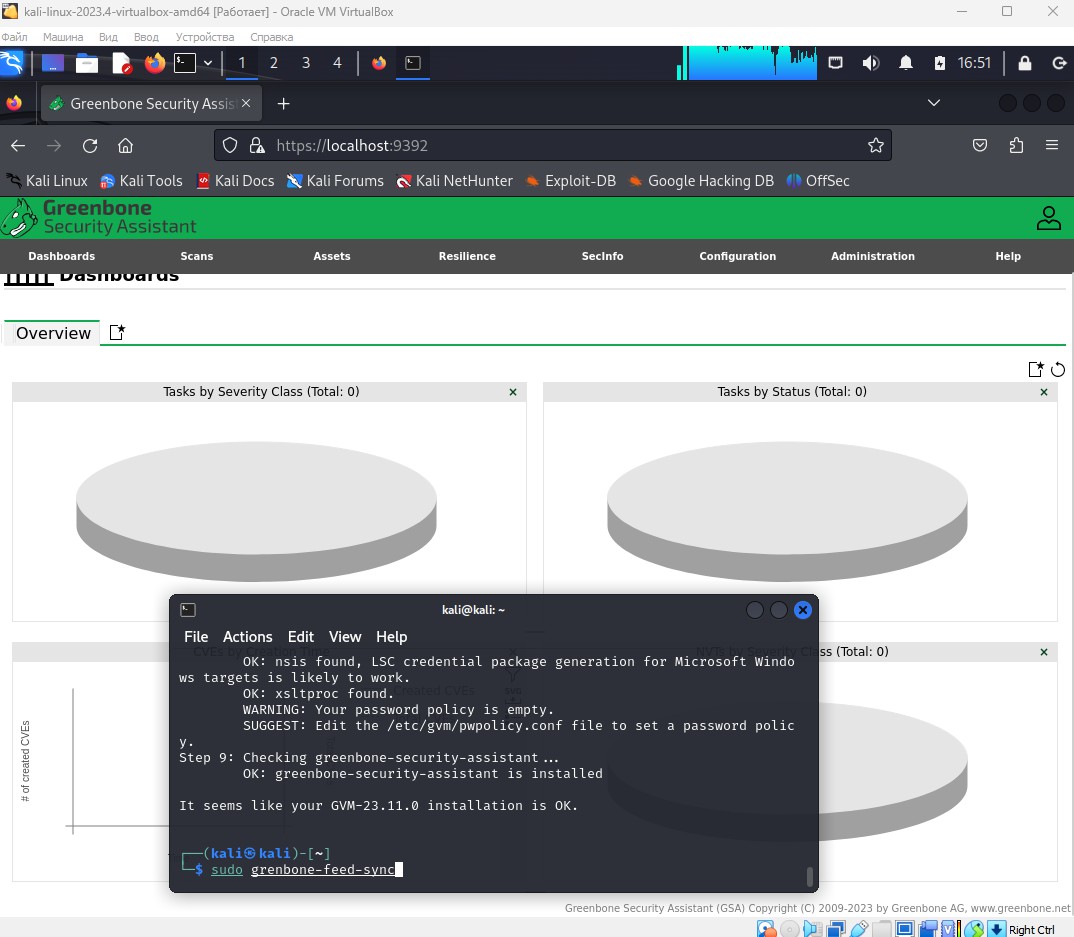


sudo gvm-setup

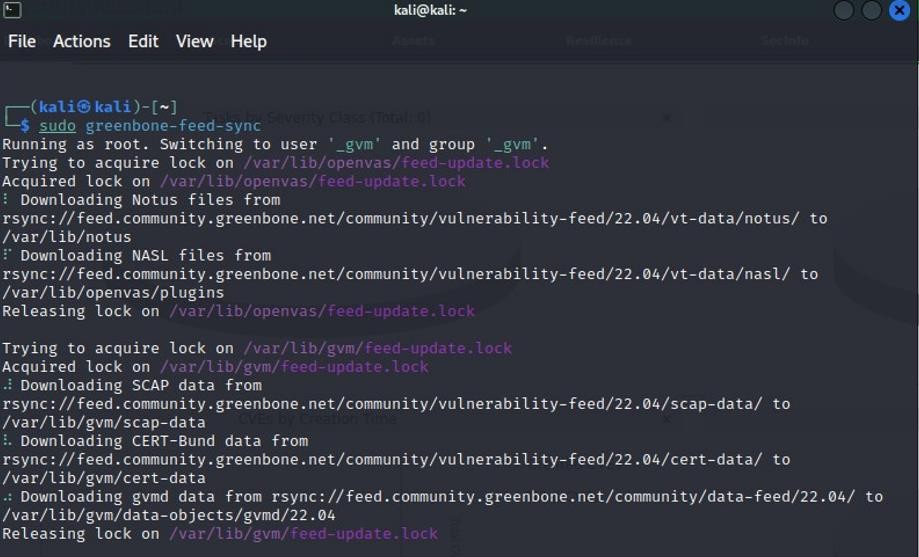
Проверим, что все компоненты были верно установлены и функционируют sudo gvm-check-setup



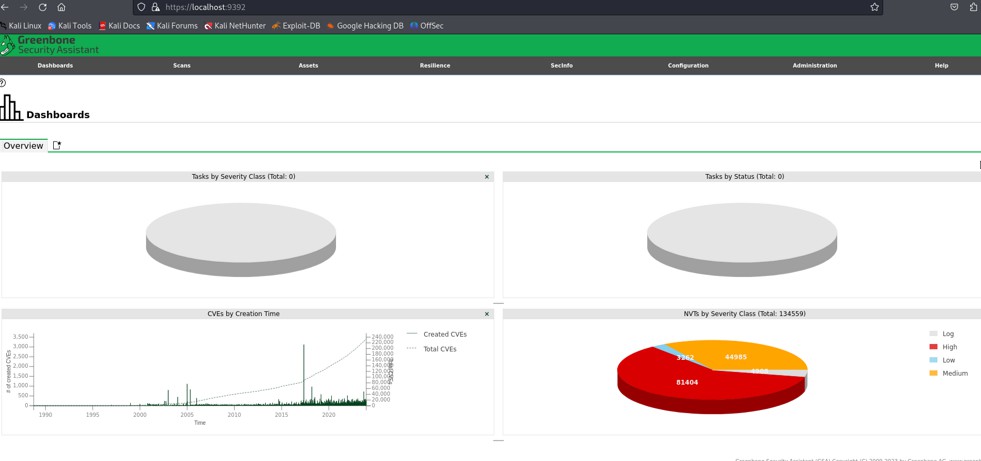
Выполним вход в приложение по адресу “https://localhost:9392”:



Обновим базы уязвимостей OpenVAS



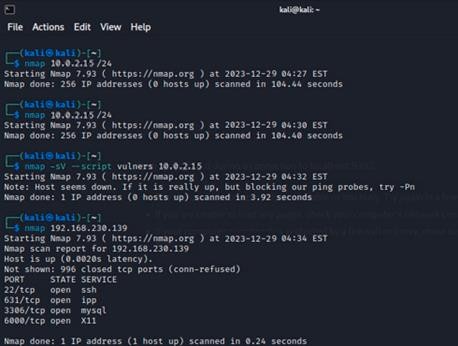
Смотрим на информацию, которая отображается в веб-интерфейсе



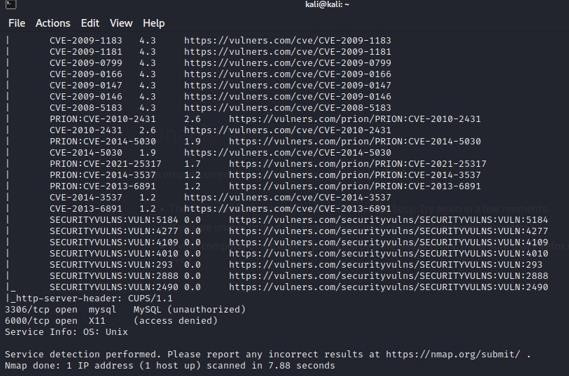
Запустим сервис ssh на DVL



Выполним сканирование сети с помощью утилиты nmap. Найдём ВМ DVL и Kali Linux



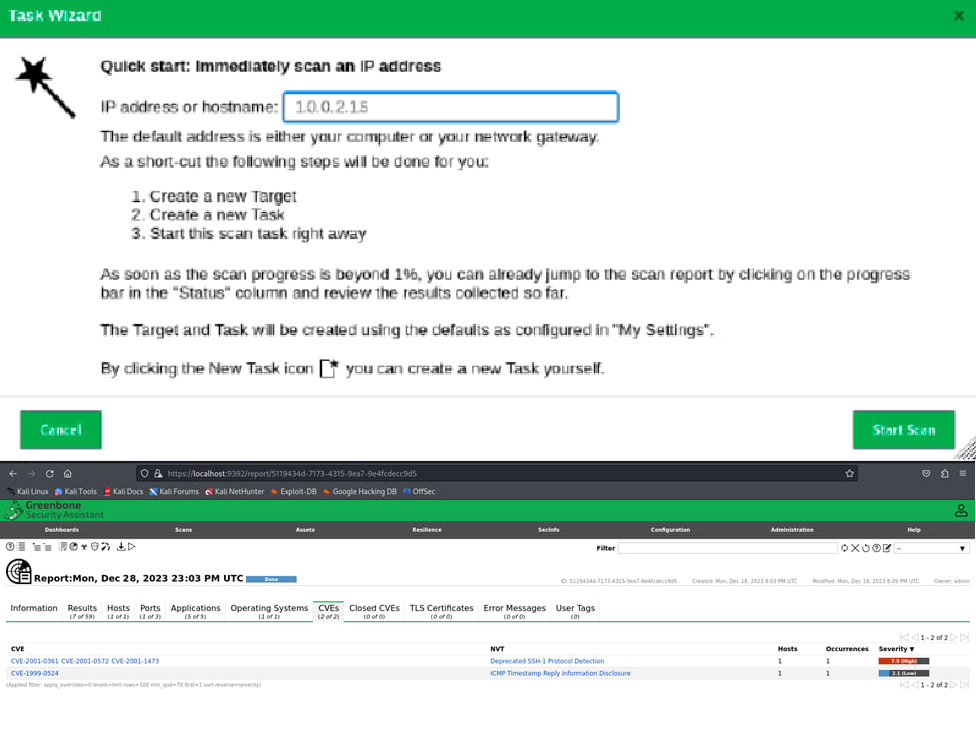
Используем скрипт vulners в утилите nmap, чтобы найти уязвимости на DVL

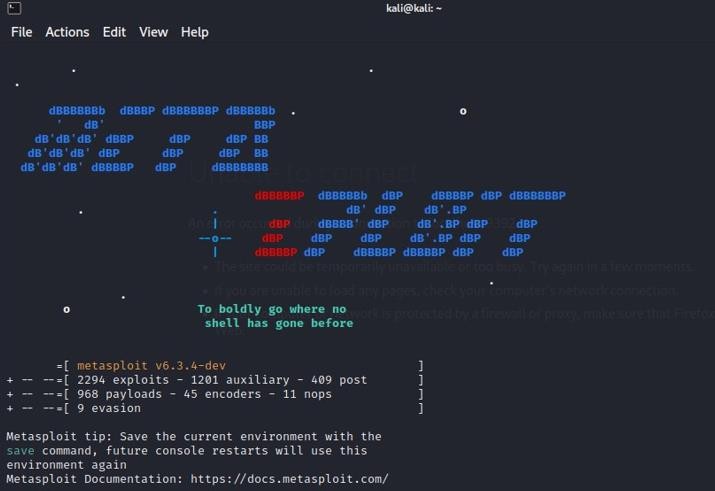


Выполним сканировение DVL с помощью OpenVAS, заметим, что nmap

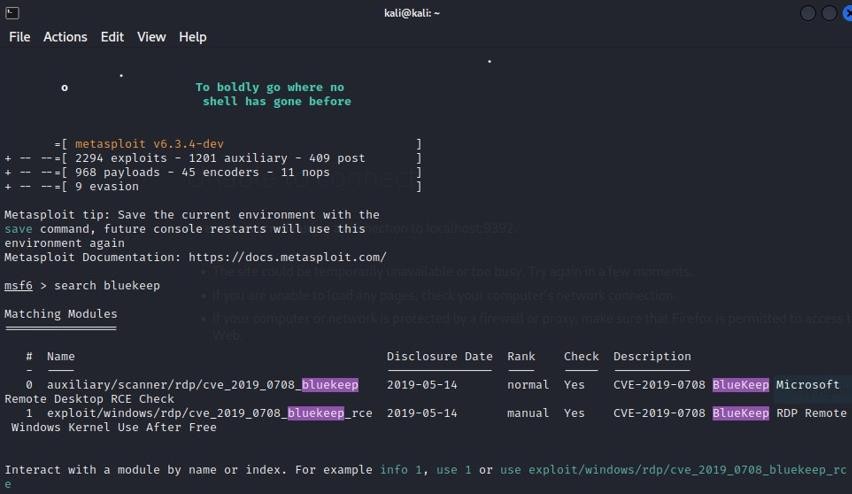
справился гораздо лучше (это связано с тем, что по умолчанию в OpenVAS включен небольшой набор параметров сканирования)

Вернёмся в веб интерфейс во вкладку Scans – Tasks и укажем localhiost

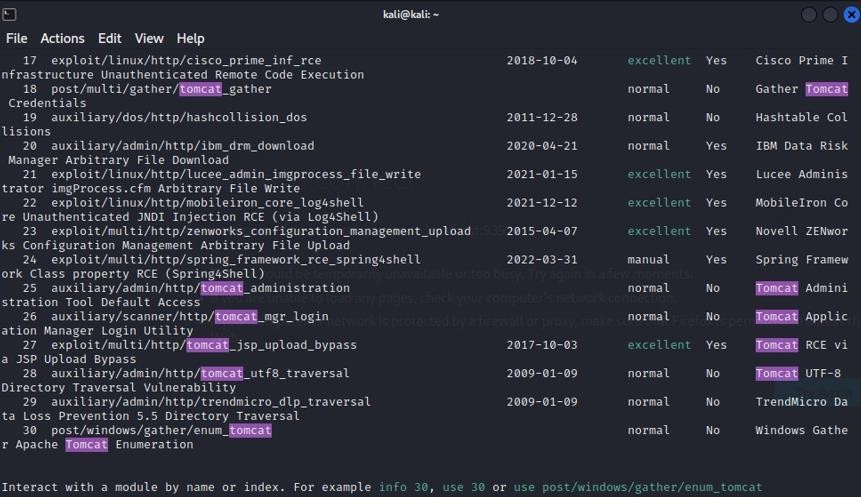


Выполним загрузку Metasploit

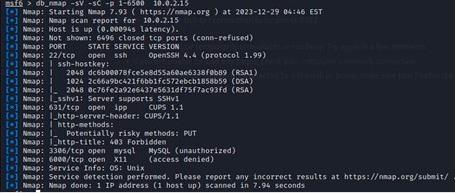
Выполним поиск и настройку BlueKeep



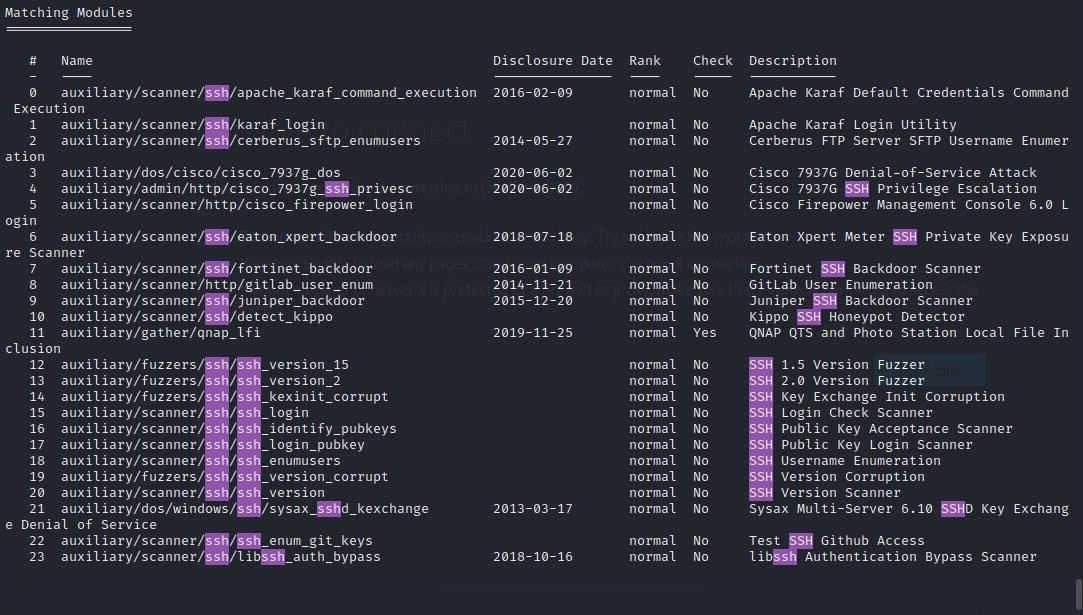
Выполним поиск по tomcat



Далее поиск эксплойдов виртуальной машины



Выполним эксплуатацию по ssh



# Сравнительный анализ

**OpenVAS** — это открытая система оценки уязвимости, которая

используется для сканирования сетей и поиска уязвимостей в системах и

приложениях. Она предоставляет средства для выявления потенциальных угроз и уязвимостей в компьютерных системах и сетях.

Основные характеристики OpenVAS:

* Сканирование уязвимостей: OpenVAS проводит автоматическое сканирование сетей, портов и служб на наличие известных уязвимостей.
* База данных уязвимостей: Она использует обновляемую базу данных уязвимостей, чтобы определить, насколько системы уязвимы к известным атакам.
* Отчеты и анализ: OpenVAS генерирует отчеты о найденных уязвимостях и предоставляет анализ безопасности сети.

**Nmap** — это мощное средство сканирования сети, которое

используется для анализа и исследования сетей, определения активных хостов, портов и служб, а также выявления уязвимостей.

Основные характеристики Nmap:

* Сканирование сети: Nmap позволяет сканировать сети для поиска активных хостов, открытых портов и служб, работающих на этих портах.
* Определение уязвимостей: с помощью дополнительных сценариев и

плагинов Nmap может выявлять уязвимости и выполнять сканирование на наличие известных уязвимостей.

* Скрипты и пользовательские сценарии: Nmap поддерживает создание

собственных скриптов и сценариев для выполнения специфических задач.

Сходства:

* 1. Сканирование сети: как OpenVAS, так и Nmap предназначены для сканирования сети и выявления уязвимостей.
  2. Базы данных уязвимостей: Обе системы могут использовать базы данных уязвимостей для определения уровня уязвимости систем.
  3. Отчеты: как OpenVAS, так и Nmap способны генерировать отчеты о результатах сканирования.

Различия:

* + 1. Цель использования:

OpenVAS прежде всего ориентирован на сканирование уязвимостей и проведение анализа безопасности.

Nmap, хотя также может выполнять сканирование уязвимостей, в первую очередь используется для сбора информации о сетях и хоста.

* + 1. Функциональность:

OpenVAS более специализирован для оценки уязвимостей и имеет расширенные инструменты для этой цели.

Nmap имеет более широкий набор функций, включая определение активных хостов, сбор информации о службах и портах.

* + 1. Интерфейс пользователя:

OpenVAS: OpenVAS обычно имеет веб-интерфейс, который удобен для

настройки и управления задачами сканирования. Он также предоставляет отчеты в удобном виде для анализа результатов.

Nmap: Nmap в основном используется через командную строку, но также имеет графические оболочки для удобства пользователей. Он обычно

предоставляет текстовые результаты сканирования.

* + 1. Сценарии и расширения:

OpenVAS: OpenVAS предоставляет сценарии и плагины, которые позволяют пользователю выполнять дополнительные проверки безопасности и

анализировать уязвимости на более глубоком уровне.

Nmap: Nmap также позволяет пользователю создавать пользовательские сценарии и расширения, но его основной фокус — это сбор базовой

информации о сети.

* + 1. Подход к безопасности:

OpenVAS: OpenVAS более ориентирован на более высокий уровень безопасности и предназначен для выявления и решения уязвимостей в системах.

Nmap: Nmap, хотя и может выполнять сканирование уязвимостей, более фокусируется на сборе информации о сети и не обязательно на выявлении уязвимостей.

Заключение

OpenVAS: OpenVAS подходит для оценки безопасности информационных систем, сетей и приложений. Его можно использовать в корпоративных

средах и организациях, чтобы регулярно проверять и обнаруживать уязвимости в сетях и серверах.

Nmap: Nmap может быть полезным инструментом для администраторов сетей и безопасности, когда требуется получить информацию о сетевой инфраструктуре, определить активные хосты, контролировать открытые

порты и проводить исследование сетей. Он также может использоваться для сканирования уязвимостей, но его главное предназначение — это сбор

информации о сети.