|  |
| --- |
|  |
| 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

Исаев А.М.

Проверил:

Пимонов Р.В.

Москва, 2023

[1. Настройка DVL 4](#_Toc157172697)

[2. NMAP, OPENVAS 11](#_Toc157172698)

[3. METASPLOIT 18](#_Toc157172699)

[4. Рекомендации 22](#_Toc157172700)

# Настройка DVL

Прежде чем приступить к работе, необходимо установить и настроить Damn Vulnerable Linux.

Устанавливаем Гостевую Операционную систему(рисунки 1-3)

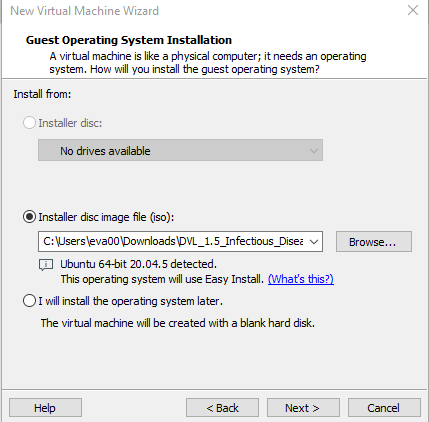


Рисунок 1 – образ DVA

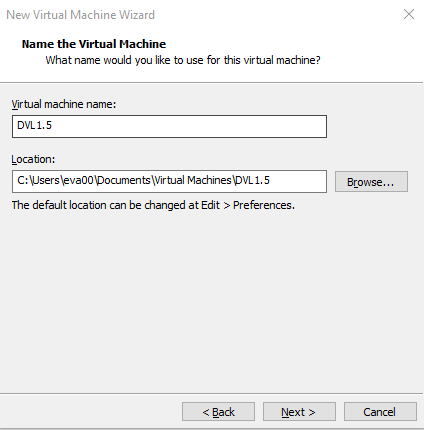


Рисунок 2 – Имя ВМ

Введем логин root, pass toor и создаем разделы диска при помощи fdisk



Рисунок 3 – login pass

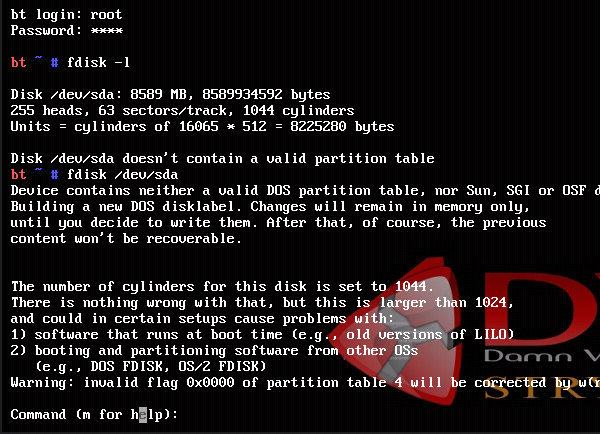


Рисунок 4 – Создаем разделы диска

Добавляем новый раздел: макс. Количество цилиндров 1044

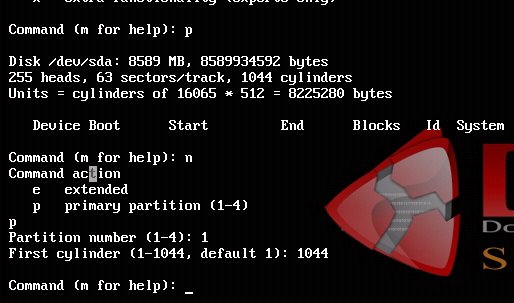


Рисунок 5 – указываем все параметры

Просмотрим созданный раздел и сохраним его

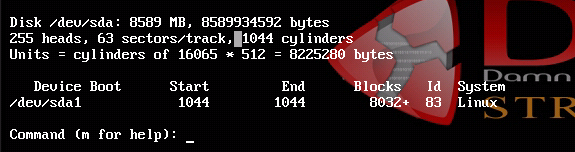


Рисунок 6 – просмотр раздела

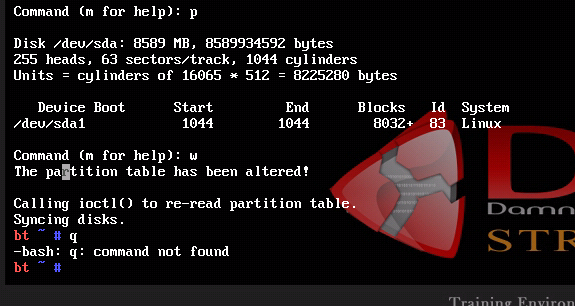


Рисунок 7 – Сохранение раздела

Отформатируем раздел /dev/sda. Далее при помощи последовательности команд необходимо произвести монтирование диска и запуск системы

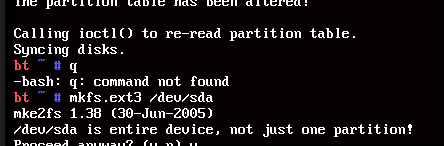


Рисунок 8 – форматирование диска

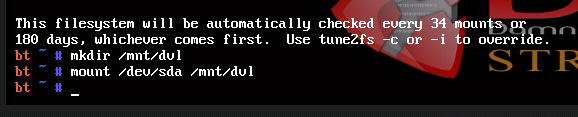


Рисунок 9 – созданием папки и монтирование диска в эту папку

Далее, необходимо скопировать образ DVL на жесткий диск и запустить установщик BackTrackInstaller.

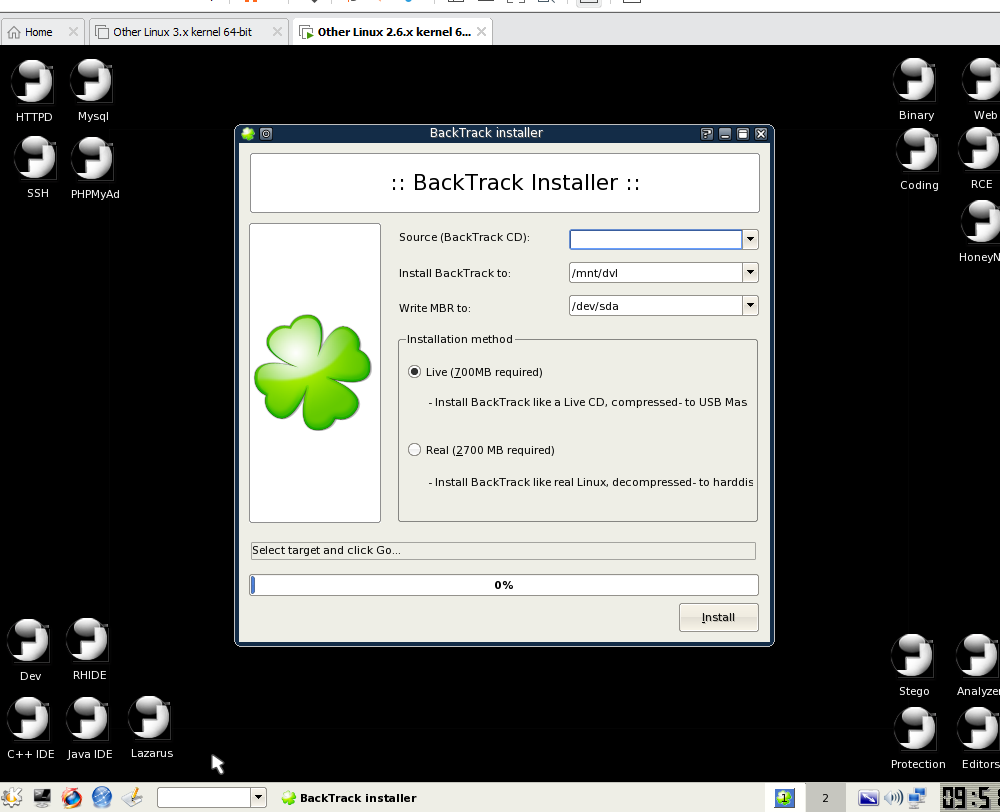


Рисунок 10 - установщик

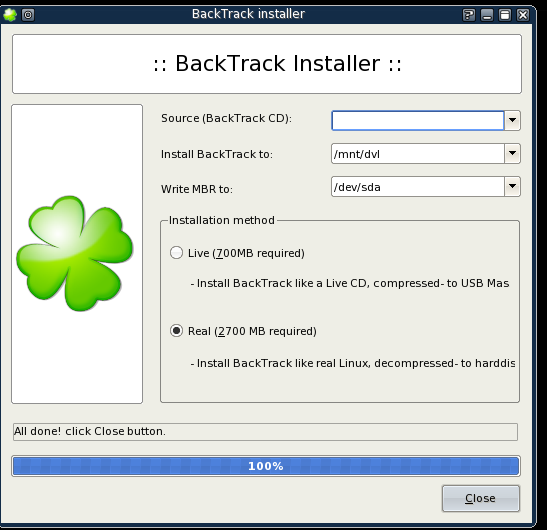


Рисунок 11 – успешное выполнение

Посмотрим сетевой адрес узла и пропингуем с Kali его для просмотра доступности узла

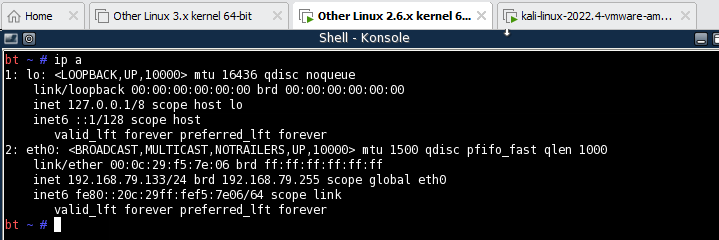


Рисунок 11 – IP адрес

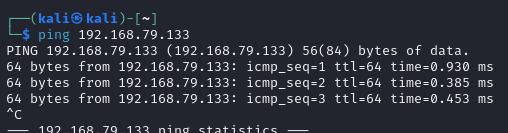


Рисунок 12 – сетевой обмен доступен

# NMAP, OPENVAS

В качестве задачи необходимо просканировать DVL на наличие открытых портов, используем nmap – v сетевой узел

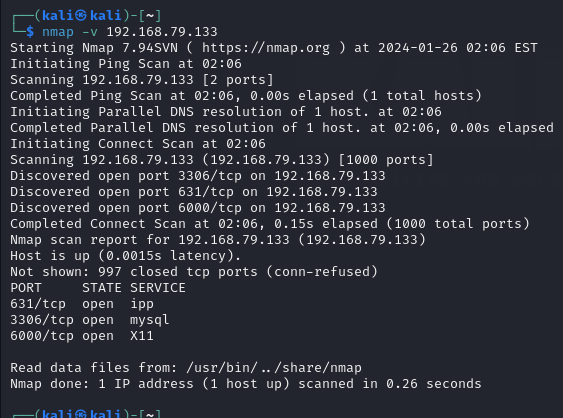
z

Рисунок 14 – Результат выполнения nmap

Список открытых портов:

631/tcp – IPP (протокол для передачи документов на печать)

3306 - MySQL

6000 – x11 (протокол для связи клиент-сервер)

Используем флаг vulners на наличие уязвимостей в DVL

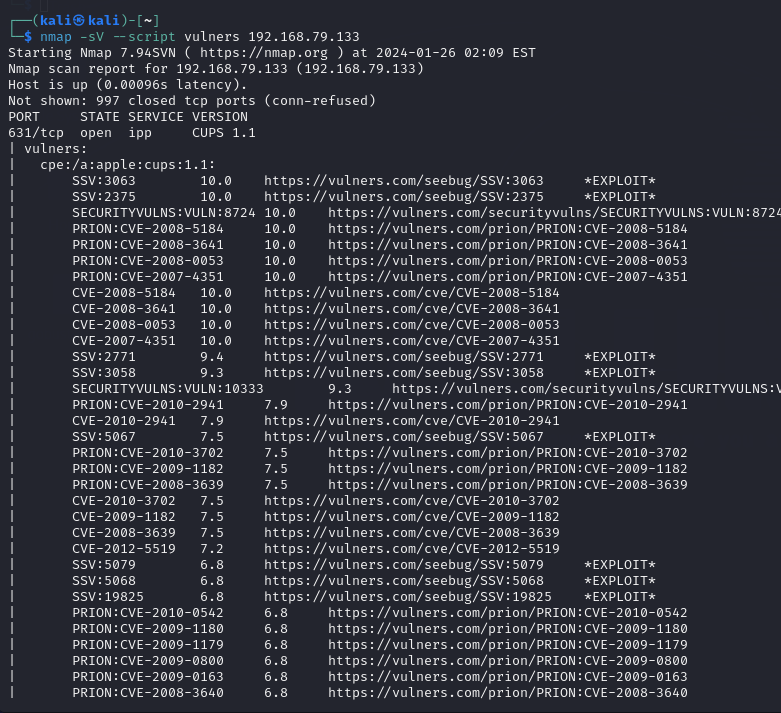


Рисунок 15 – Результат сканирования

Далее, необходимо настроить OPENVAS. Выполним check-setup для проверки целостности установки компонентов

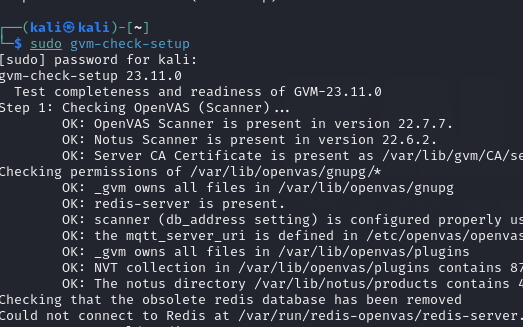


Рисунок 16 – Первые steps

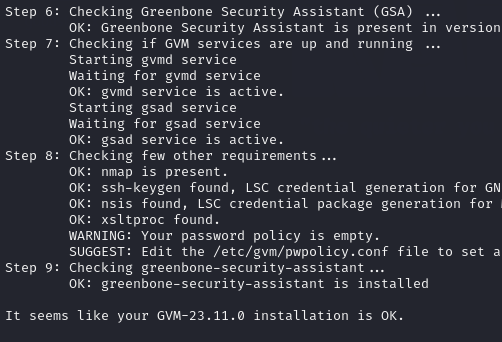


Рисунок 17 – все компоненты успешно прошло проверку

Для доступа к веб-интерефейсу на 127.0.0.1/9332 необходимо ввести пароль и логин admin

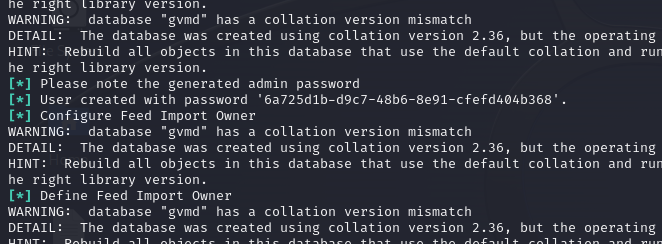


Рисунок 18 – Креды

В процессе установки возникли проблемы с PSQL, все проблемы были устранены

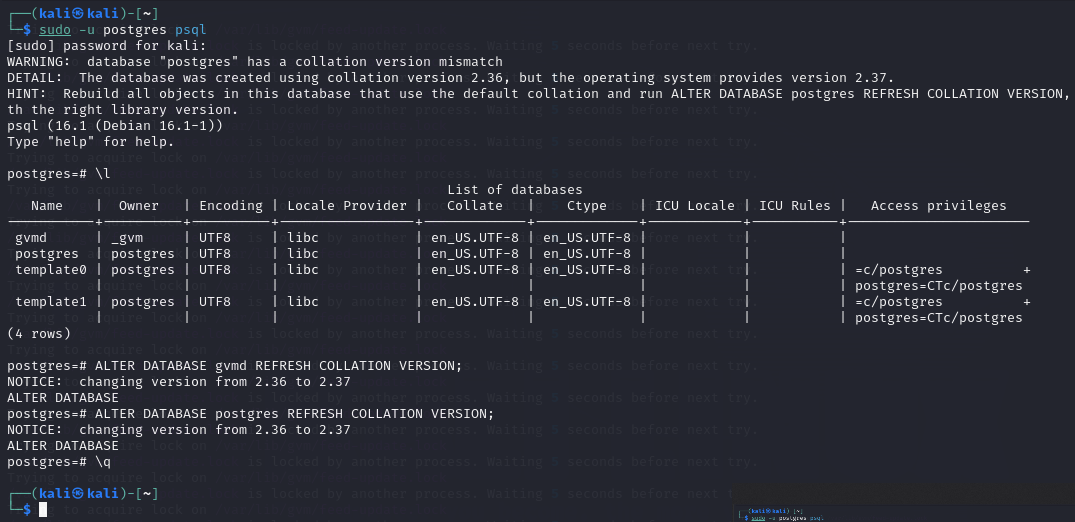


Рисунок 19 – Неполадки с SQL

Для сканирование DVL указываем IP адрес и ждем окончания сканирования.

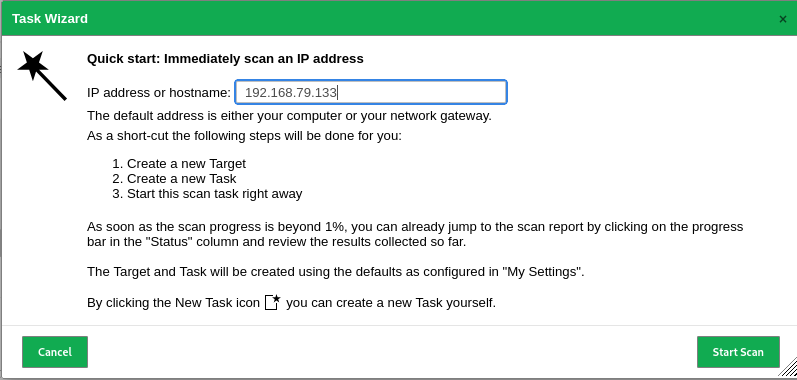


Рисунок 20 – Указываем адрес

Ожидаем окончания сканирования узла и получаем и анализируем информацию.

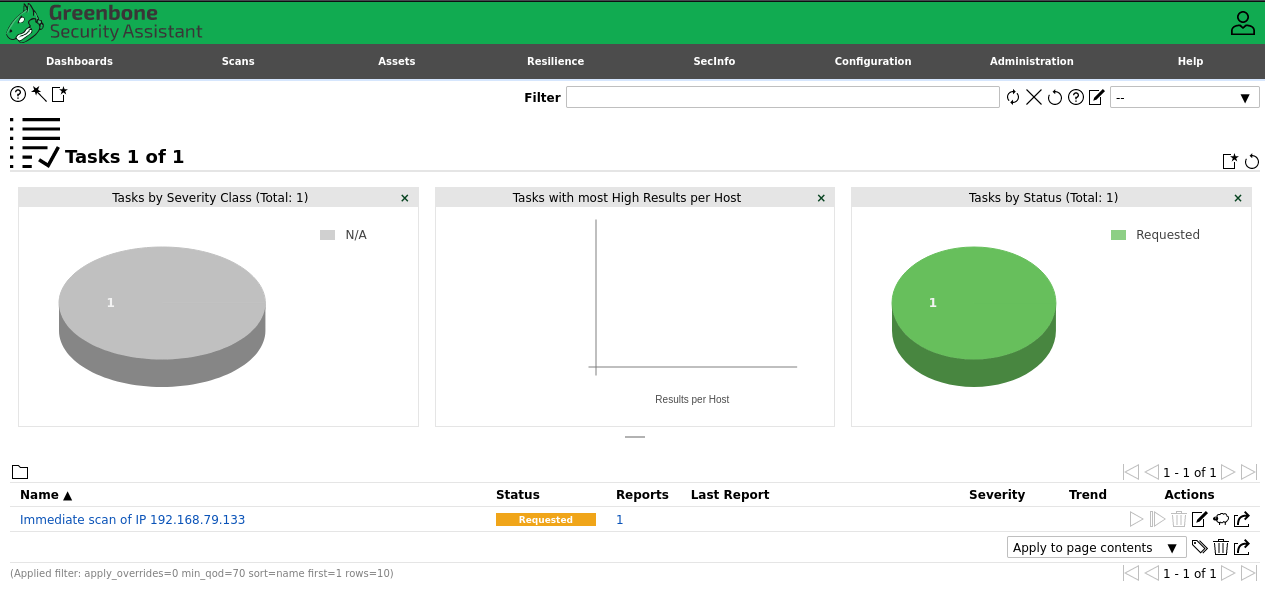


Рисунок 21 – дашборд Greenbone

Видим сводку результатов

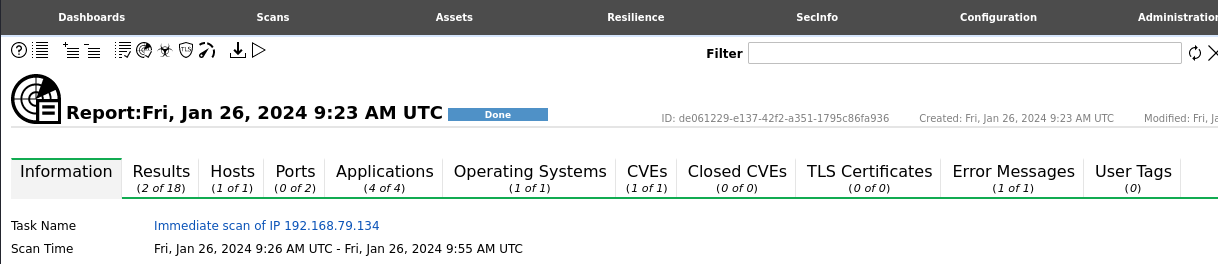
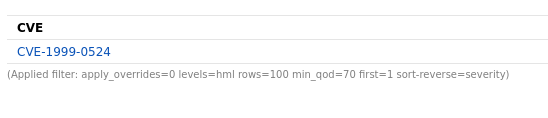


Рисунок 22 – Найденная уязвимость

Была найдена крайне старая уязвимость CVE-1999-0524 – ее CVSS 3.1 – 2.1

****

Убедимся что сетевой узел правильный

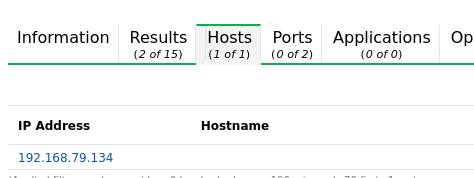
****

Рисунок 23 – Правильность узла

Проведем анализ выявленной уязвимости

****

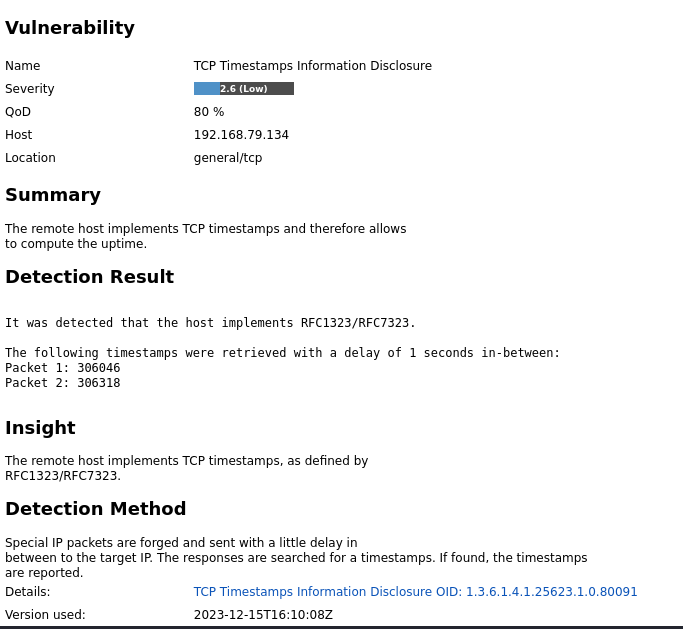
****

Рисунок 24 – описание уязвимости

# METASPLOIT

Metasploit Framework — это мощнейший инструмент, который могут использовать как киберпреступники, так и «белые хакеры» и специалисты по проникновению для исследования уязвимостей в сетях и на серверах. Поскольку это фреймворк с открытым исходным кодом, его можно легко настроить и использовать на большинстве операционных систем.

Выполним запуск утилиты, предварительно обновив ее.

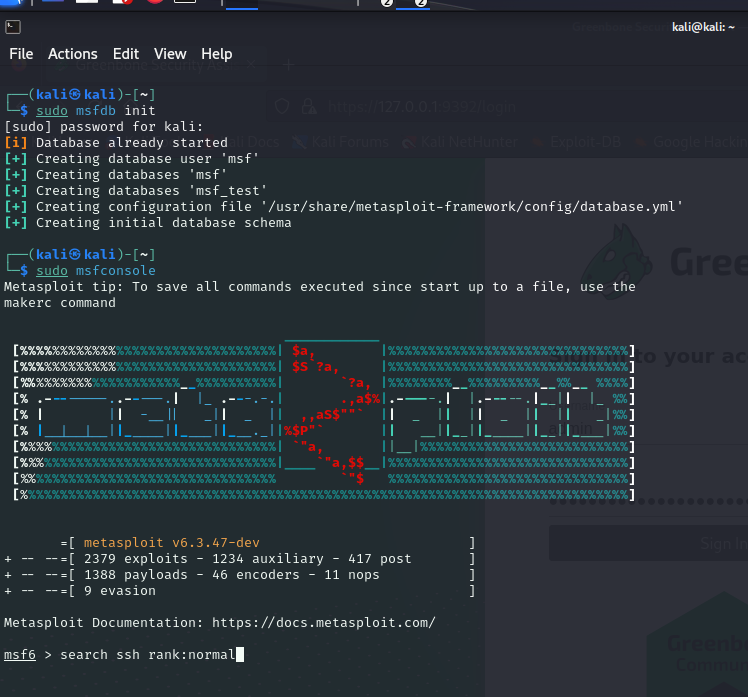
****

Рисунок 25 – запуск утилиты

Проверим совпадение по поиску ssh rank:normal и убедимся в наличии эксплойтов.

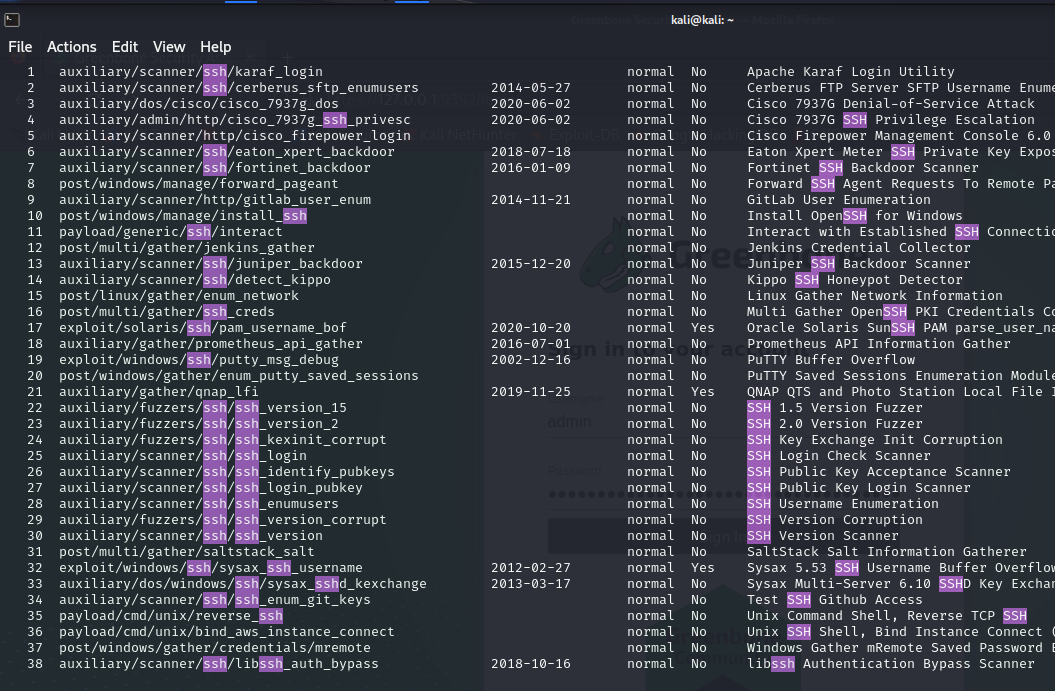
****

Рисунок 26 – Видимый список эксплойтов

Воспользуемся 25 файлом – ssh\_login. Для этого используем словарь общедоступных логинов

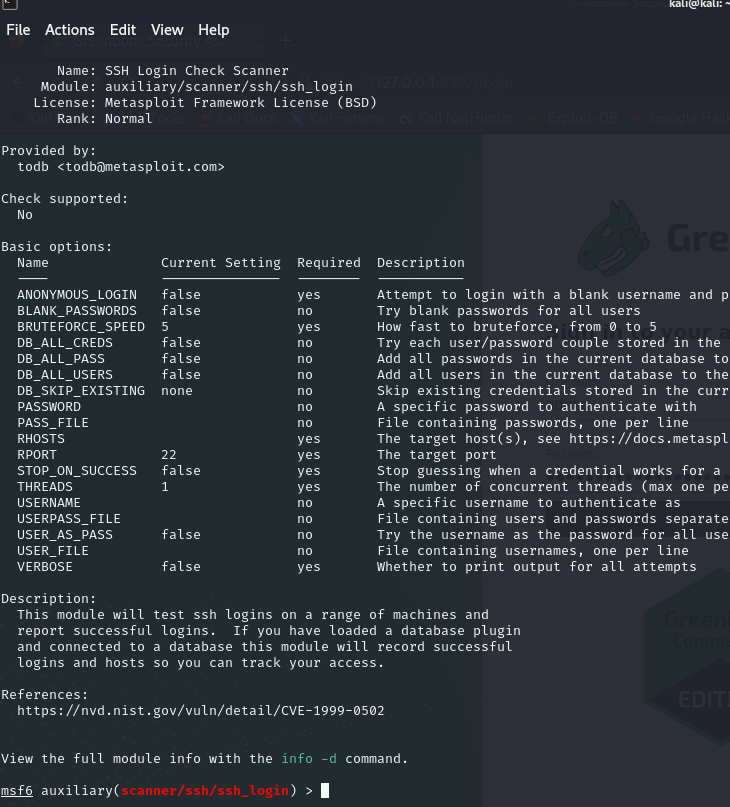
****

Рисунок 26 – Опции и описание

Убедимся в наличии требуемого словаря – root\_userpass.txt

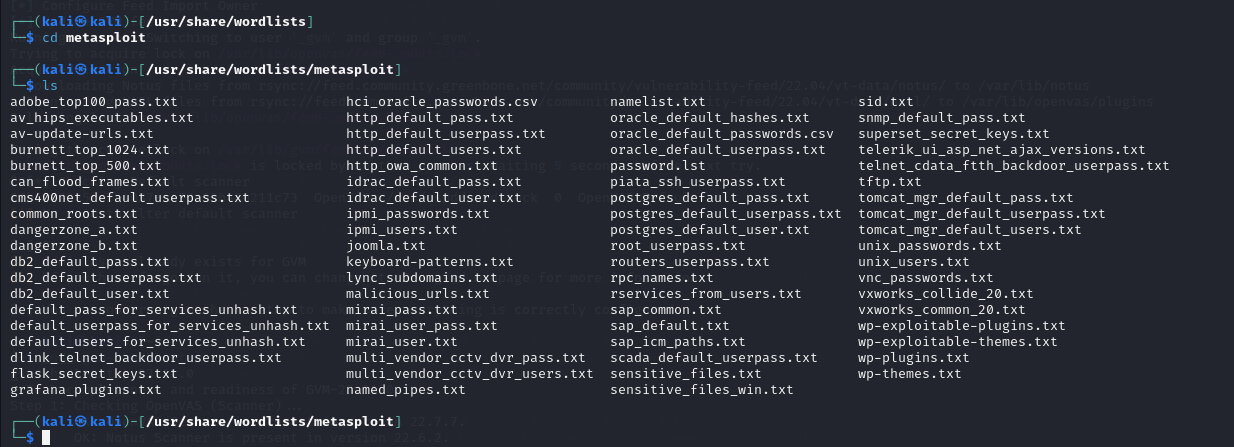
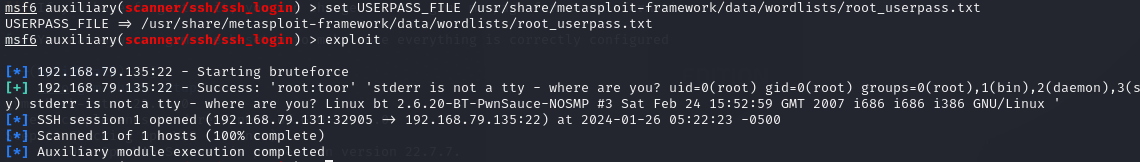
****

Рисунок 27 – Наличие словаря

И проведем попытку подключения по ssh к DVL: обнаружены совпадение с учетными данными в словаре, пароль, видимо по умолчанию пустой.

****

# Рекомендации

1. Усложнить пароль, использовать специальные символы
2. Включение 2FA для усиления защиты доступа к SSH
3. Внедрить системы предотвращения вторжений и брандмауры для активной защиты от потенциальных атак