Отчёт по 3-му этапу индивидуального проекта

Дисциплина: Информационная безопасность

Выполнил: Танрибергенов Эльдар

Содержание

Список иллюстраций

# 1 Цель работы

Ознакомиться с утилитой Hydra в Kali Linux и испытать.

# 2 Задания

* Ознакомиться с утилитой Hydra в Kali Linux и испытать.

# 3 Ход работы

Для проведения испытания я установил специальную уязвимую ВМ - Metasploitable.

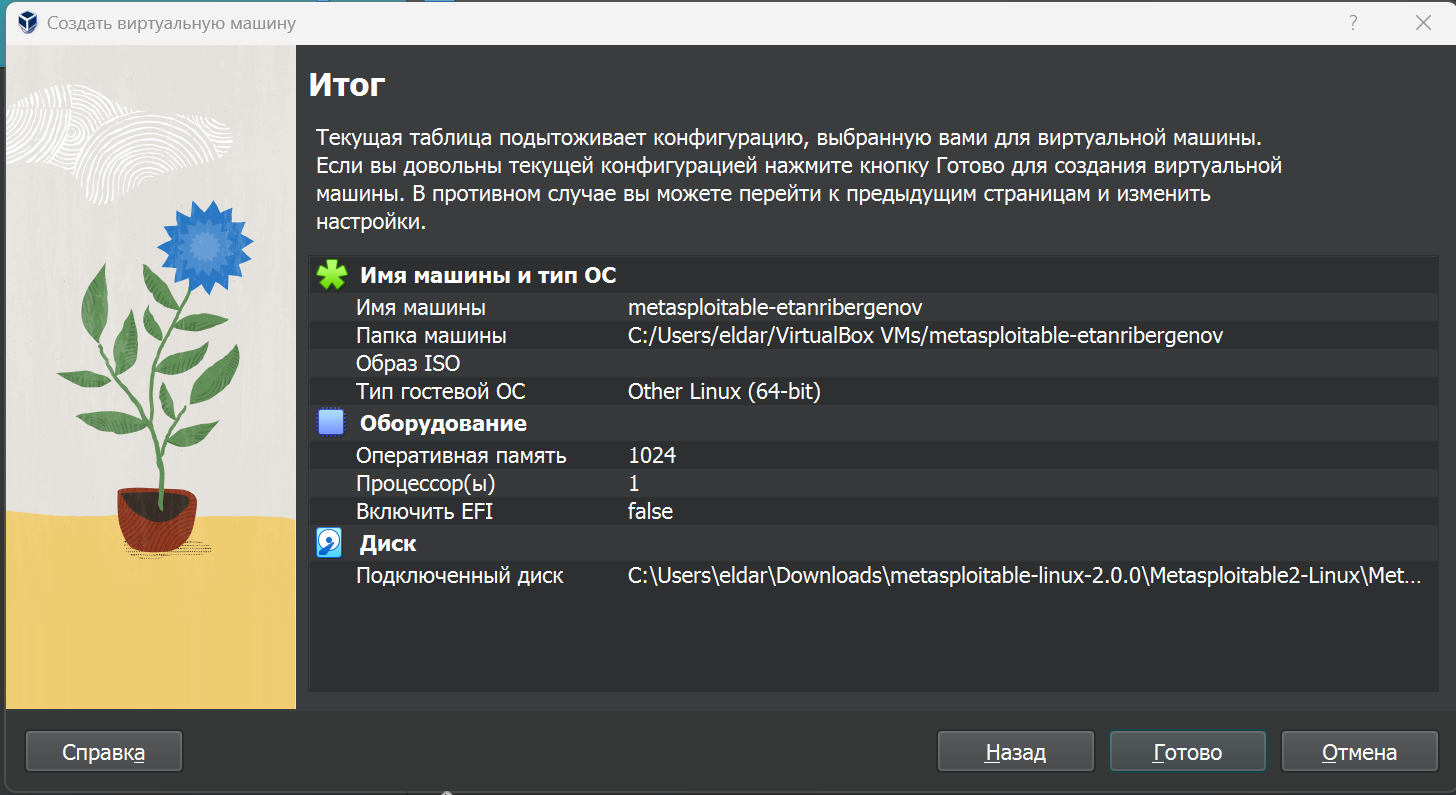


Рис. 1: Создание ВМ metasploitable

Запустил metasploitable и ввёл команду ifconfig, чтобы узнать её ip-адрес.

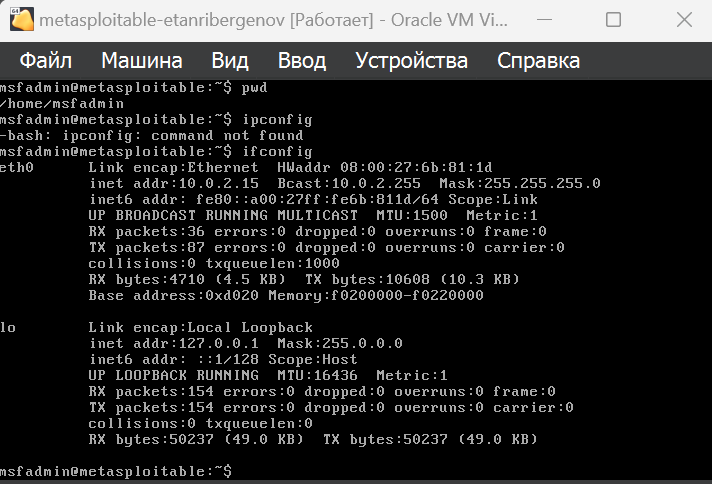


Рис. 2: Выяснение IP-адреса ВМ metasploitable

Произвёл поиск открытых портов “жертвы” при помощи команды nmap в Kali Linux. Открытым оказался - http порт (80).

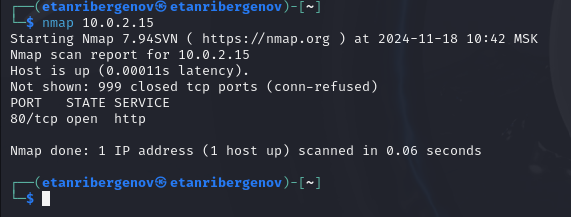


Рис. 3: Поиск открытых портов у хоста с введённым ip-адресом в Kali Linux

Для запуска hydra я воспользовался встроенным списком стандартных паролей - http\_default\_pass.txt.

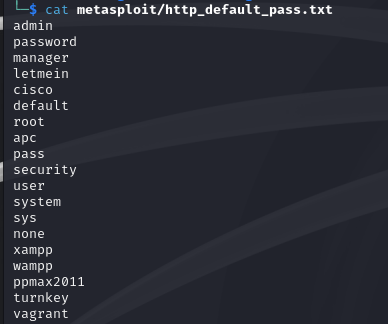


Рис. 4: Содержимое встроенного списка http\_default\_pass.txt

Запустил hydra на поиск пароля по известному логину. Получил пароль - password.

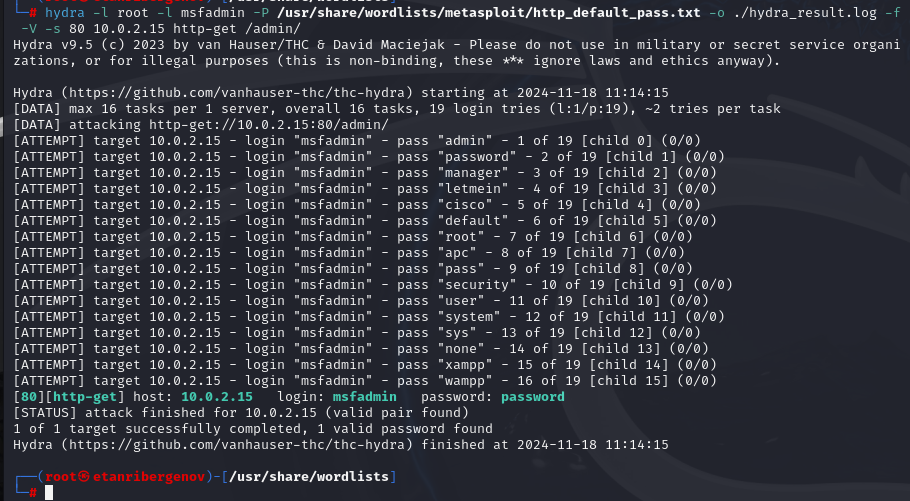


Рис. 5: Результат

# 4 Выводы

В результате выполнения работы я познакомился с утилитой для подбора имён пользователей (логинов) и паролей Hydra.