# Индивидуальный проект. Этап 3

**Основы информационной безопасности**

Тойчубекова Асель Нурлановна

# Содержание

# Список иллюстраций

# Список таблиц

# 1 Цель работы

Целью данного этапа индивидуального проекта является получение навыков работы с инструментом Hydra.

# 2 Задание

- Реализовать эксплуатацию уязвимости с помощью брутфорса паролей.

# 3 Теоретическое введение

Hydra (или THC-Hydra) — это мощный инструмент для проведения атак методом подбора паролей (brute-force) и словарных атак на различные протоколы и сервисы, такие как HTTP, FTP, SSH, RDP, MySQL и многие другие. Он был разработан группой THC (The Hacker's Choice) и широко используется как в тестировании на проникновение (penetration testing), так и для обучения по вопросам информационной безопасности. Hydra может эффективно использоваться для взлома аутентификационных механизмов на сервисах, которые не применяют защиты от атак на основе подбора паролей (например, отсутствие ограничений по числу попыток входа или слабыми паролями).

Hydra использует метод перебора возможных комбинаций логинов и паролей, которые предоставляются в виде списка (например, с помощью словаря). Во время атаки она тестирует каждую пару "пользователь-пароль" с использованием различных протоколов и сервисов.

Основные характеристики Hydra:

- Многопоточность: Hydra позволяет запускать несколько потоков одновременно, что значительно увеличивает скорость подбора паролей.
- Поддержка множества протоколов: Можно атаковать как стандартные сервисы (SSH, FTP), так и веб-формы.
- Гибкость конфигурации: Hydra предоставляет множество опций для настройки атаки, таких как количество потоков, использование прокси-серверов, настройка параметров аутентификации и т. д.

Для использования Hydra необходимо установить ее на свою машину. Hydra поддерживает операционные системы Linux, Windows и macOS. После установки, инструмент запускается через командную строку и требует указания параметров для атаки.

Пример:

hydra -l admin -P /path/to/rockyou.txt -s 80 localhost http-get-form "/path/to/login:username=^USER^&

- -l admin — логин, который будет использоваться в атаке (в данном случае "admin").
- -P /path/to/rockyou.txt — путь к файлу словаря паролей (например, популярный словарь rockyou.txt).
- -s 80 — порт, на котором работает целевой сервис (в данном случае HTTP — порт 80).
- localhost — целевой хост (в данном случае — локальный сервер).
- http-get-form — указание, что атака будет на веб-форму через метод GET.
- Путь к форме аутентификации и другие параметры конфигурации (например, типы полей формы) указываются в конце команды.

# 4 Выполнение лабораторной работы

Для начала нам нужен словарь для брута. Мы будем использовать словарь rockyou, который является сборником наиболее популярных и потенциальных паролей. В Kali Linux словарь находится в каталоге /usr/share/wordlists/ нам нужно его только разархивировать и переместить в домашнюю директорию. (рис. 4.1).

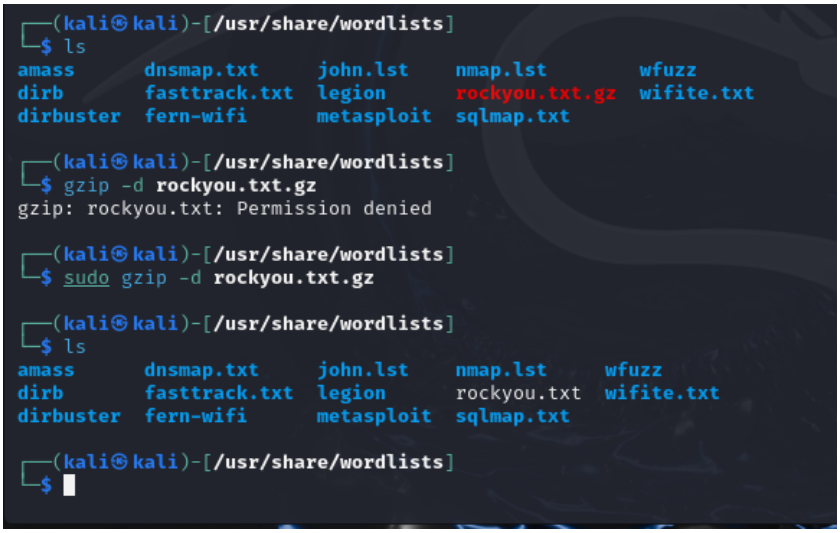


Рис. 4.1: Установка словаря с потенциальными паролями

Захожу на сайт DVWA, полученный в ходе выполнения предыдущего этапа проекта.Нам нужны будут данные о cookie для запроса hydra, из за этого включаем функцию cookie-editor. (рис. 4.2).

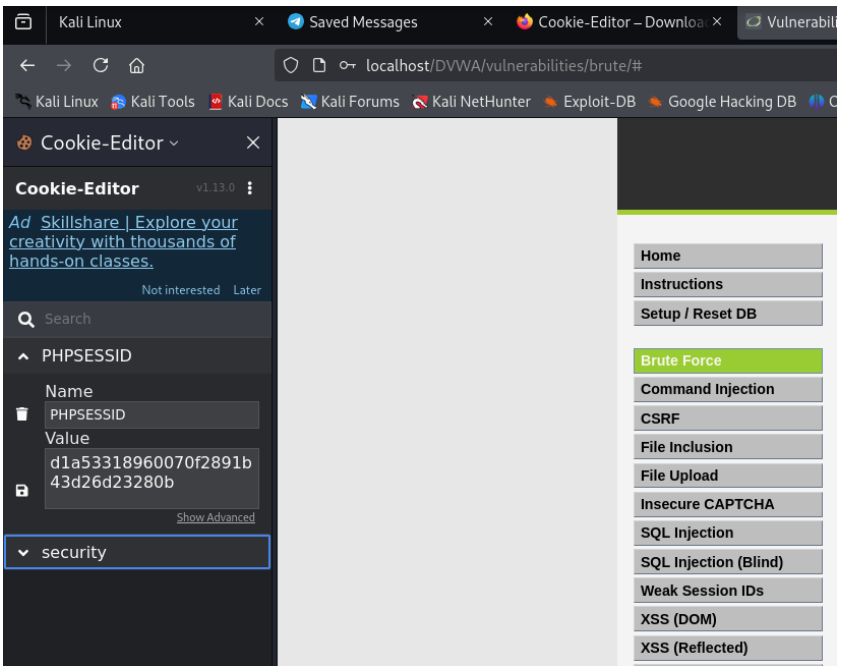


Рис. 4.2: Добавление функции cookie-editor

Теперь можем отправить запрос hydra, указывая имя пользователя, словарь с паролями, домашний host, данные о DVWA, параметры cookie, строка, которая присутствует на странице при неудачной аутентификации. В результате мы видим, что нам вывелся подходящий пароль. (рис. 4.3).

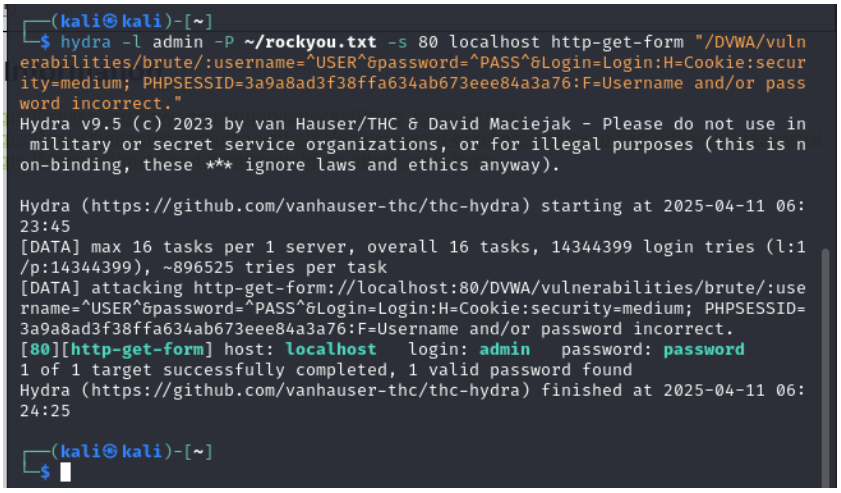


Рис. 4.3: Hydra-запрос

Далее перейдем в DVWA и введем логин и соответствующий пароль, который

выдал нам Hydra. Мы видим, что пароль был успешно подобран. (рис. 4.4).

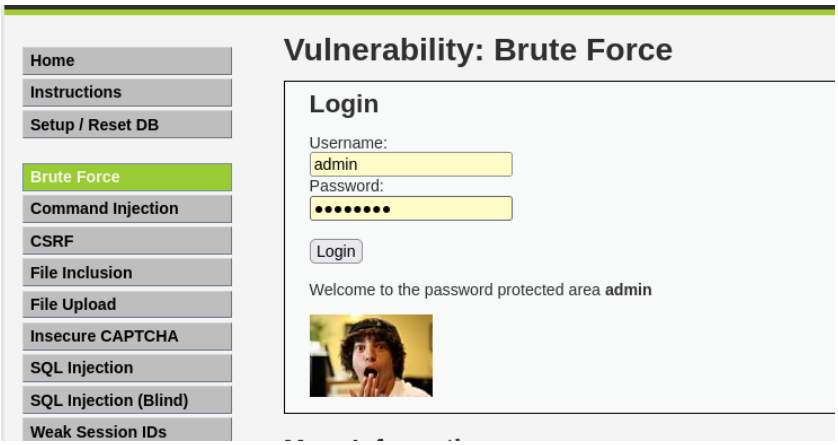


Рис. 4.4: Результат

# 5 Выводы

В ходе выполнения третьего этапа индивидуального проекта я познакомилась с инструментом Hydra и получила практические навыки с ним.