Отчёта по индивидуальной проекте этап 3

Основной информационной системе

Нджову Нелиа

Содержание

Список иллюстраций

Список таблиц

1 Цель работы

Приобретение практических навыков по использованию инструмента Hydra для брутфорса паролей.

2 Задание

1. Реаловать эксплуатацию нязвимости с помощью брутфорса паролей.

3 Теоретическое введение

3.0.1 Переписано и кратко изложено:

Hydra — это инструмент для подбора или взлома логинов и паролей. Он поддерживает множество протоколов и сервисов.

3.0.1.1 Пример использования:

- **IP сервера**: `178.72.90.181`
- **Сервис**: HTTP на порту `80`
- **Авторизация**: через HTML-форму, отправляющую POST-запрос на `http://178.72.90.181/cgi-bin/luci`
- **Формат запроса**: `username=root&password=test_password`
- **Ответ при ошибке входа**: `Invalid username and/or password! Please try again.`

3.0.1.2 Команда Hydra:

```
hydra -l root -P ~/pass_lists/dedik_passes.txt -o ./hydra_result.log -f -V -s 80
```

3.0.1.3 Пояснения:

- Используется модуль `http-post-form`, так как авторизация осуществляется через POST-запрос.
- После модуля указывается:

1. Путь к скрипту: `/cgi-bin/luci`
2. Формат POST-запроса с подстановками `^USER^` и `^PASS^`
3. Сообщение об ошибке при неверных данных: `Invalid username`

Hydra определяет успешную авторизацию по отсутствию этой строки в ответе.

4 Выполнение лабораторной работы

Чтобы ввести пробрутфорсить пароль, вам сначала нужно найти большой список часто используемых паролей. Стандартный список rockyou.txt уже был в моем kali linux, поэтому я скопировала его в каталог загрузок и извлек.(рис.1).

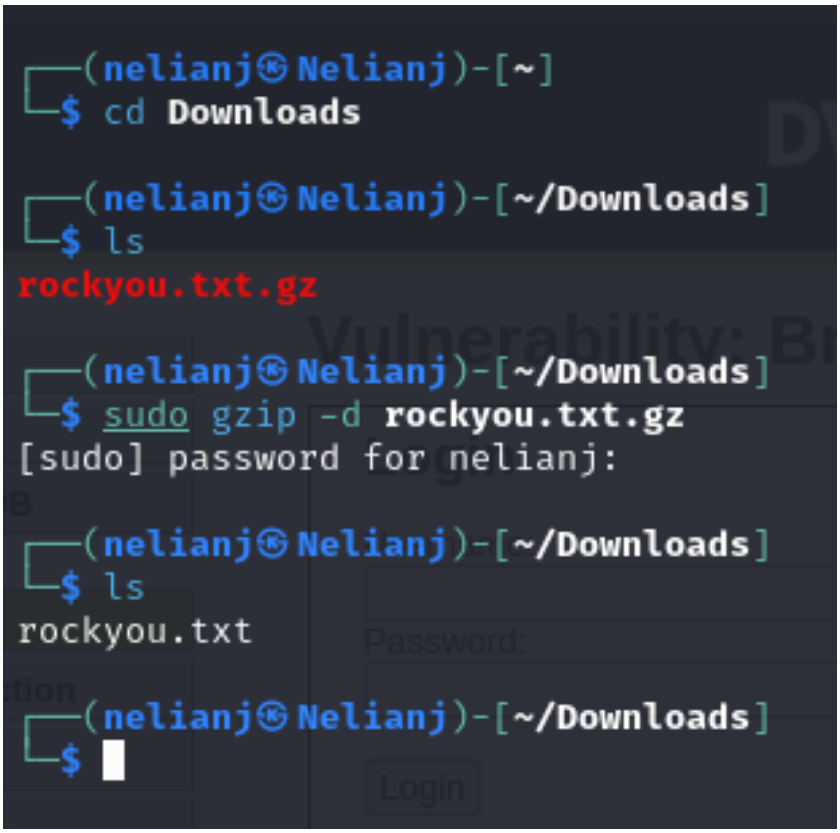

Рис. 4.1: Распаковка архив со списком паролей

Я захожу на сайт DVWA, полученный в ходе предыдущего этапа проекта. Для запроса hydra мне понадобятся параметры cookie с этого сайта(рис.2)

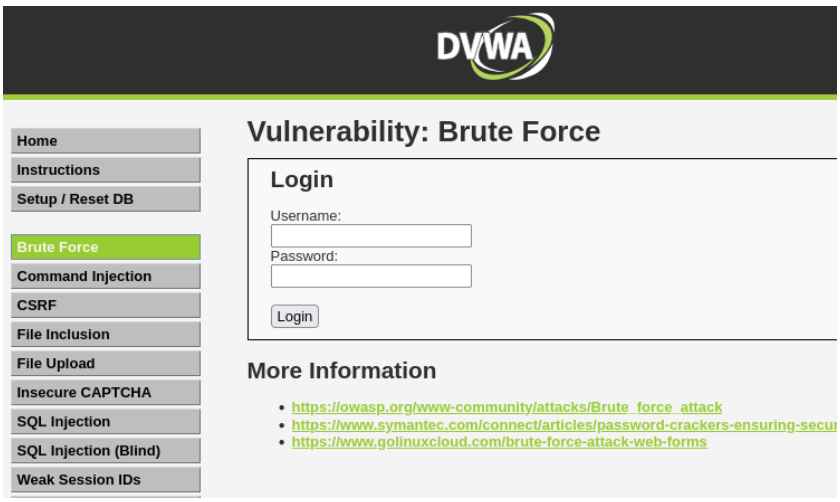

Рис. 4.2: Сайт, с которого получаем информацию о параметрах cookie

Чтобы получить информацию о параметрах cookie, необходимо расширение для браузера(cookie editor). Итак, я установила его и скопировала параметры cookie с его помощью(рис.3)

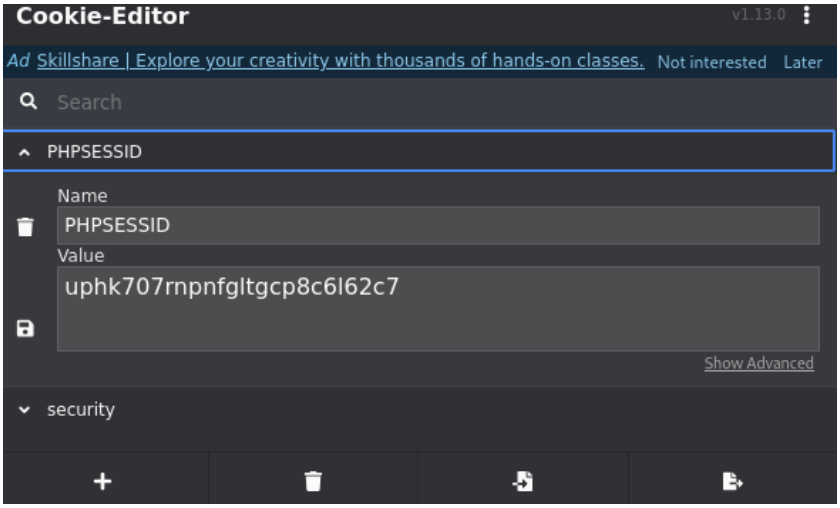

Рис. 4.3: информация о параметрах cookie

Я ввожу необходимую информацию в запрос Hydra. Мы подберем пароль для пользователя admin, используя запрос GET с двумя параметрами cookie: security и PHPSESSID, которые указаны в последнем абзаце(рис.4)

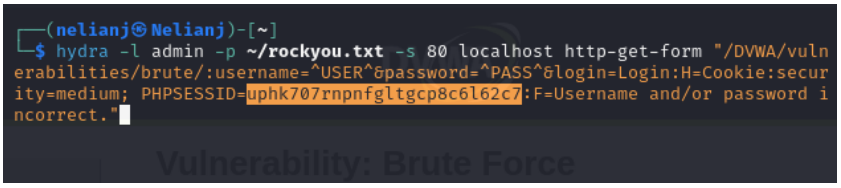

Рис. 4.4: Запрос Hydra

Через некоторое время я получил список подходящих паролей(рис.5)

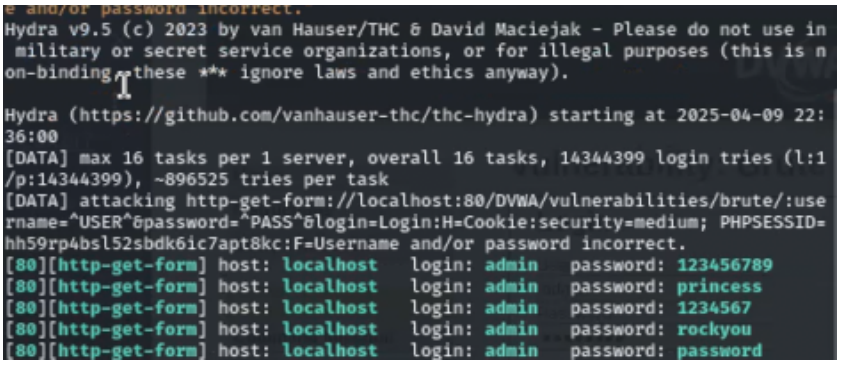

Рис. 4.5: Результат запроса

Я ввожу полученные данные на сайте для проверки и получаю положительный результат проверки пароля.

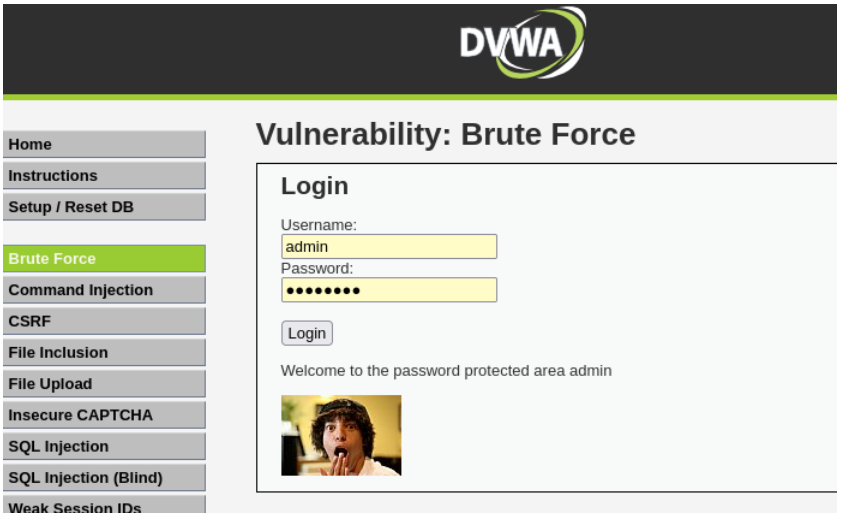

Рис. 4.6: Результат

5 Выводы

Выполнив эту работу, я приобрела практические навыки по использованию инструмента Hydra для брутфорса паролей.

Список литературы

https://addons.mozilla.org/en-US/firefox/addon/cookie-editor/?utm_campaign=external-cookie-editor.com

https://github.com/vanhauser-thc/thc-hydra/issues/612