Использование Hydra

3 этап Индивидуального проекта

Прокопьева М.Е.

Российский университет дружбы народов, Москва, Россия

Информация

Докладчик

- Прокопьева Марина Евгеньевна
- студент
- Российский университет дружбы народов

Вводная часть

Цель работы

Цель работы

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

Теоретическое введение

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.

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^&passwo
```

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

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

##1

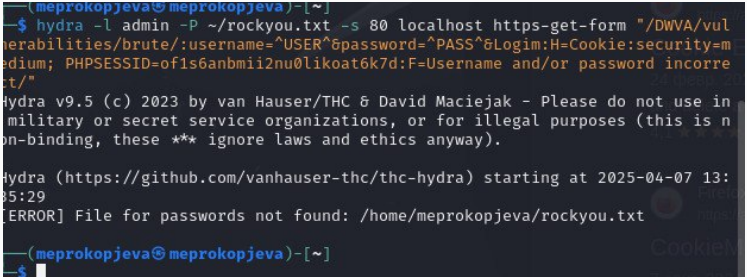
Чтобы получить информацию о параметрах cookie я установила соответствующее расширение для браузера (**cookies?**), теперь могу не только увидеть параметры cookie, но и скопировать их

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

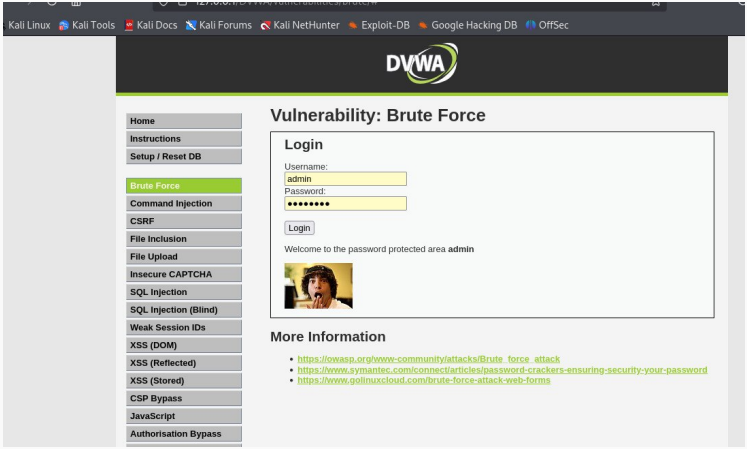
Ввожу в Hydra запрос нужную информацию. Пароль будем подбирать для пользователя admin, используем GET-запрос с двумя параметрами cookie: безопасность и PHPSESSID, найденными в прошлом пункте Спустя некоторое время в результат запроса появится результат с подходящим паролем

##3

Вводим полученные данные на сайт для проверки



Получаем положительный результат проверки пароля. Все сделано верно



Выводы

Выводы

Подобрала логин и пароль пользователя