Индивидуальный проект - Этап 3

Основы информационной безопасности

Чистов Даниил Максимович

Содержание

# 1 Цель работы

Получение навыков пользование утилитой Hydra

# 2 Выполнение лабораторной работы

Мне потребуется список часто используемых паролей, в Kali Linux уже есть такой список в виде файла, его лишь нужно разархивировать (рис. 1).

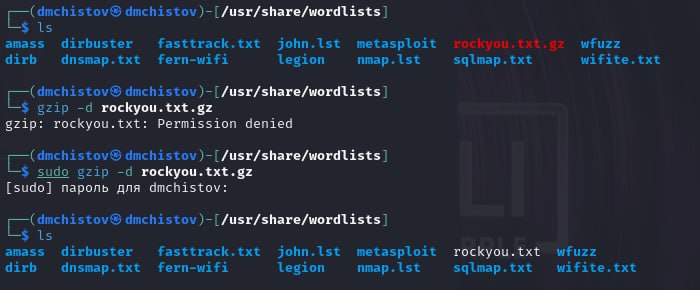


Рис. 1: Список паролей в Kali Linux

Захожу на страничку DVWA про Brute Force (рис. 2).

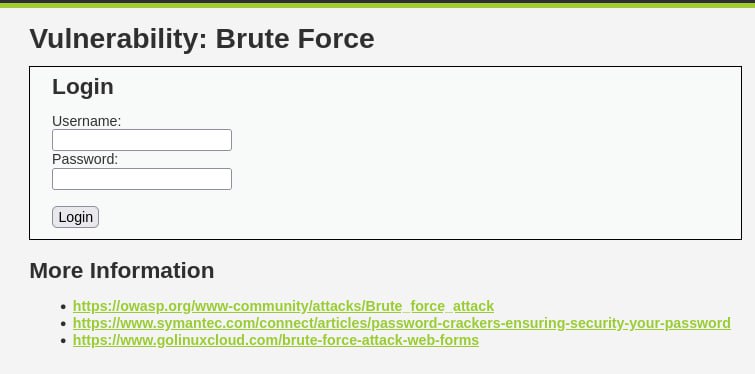


Рис. 2: Brute Force в DVWA

Важно отметить, что в DVWA есть несколько уровней защиты, которые можно самостоятельно менять. По автомату стоит Impossible, в таком режиме Brute Force бесполезен. Поэтому нужно поменять уровень защиты на medium (рис. 3).

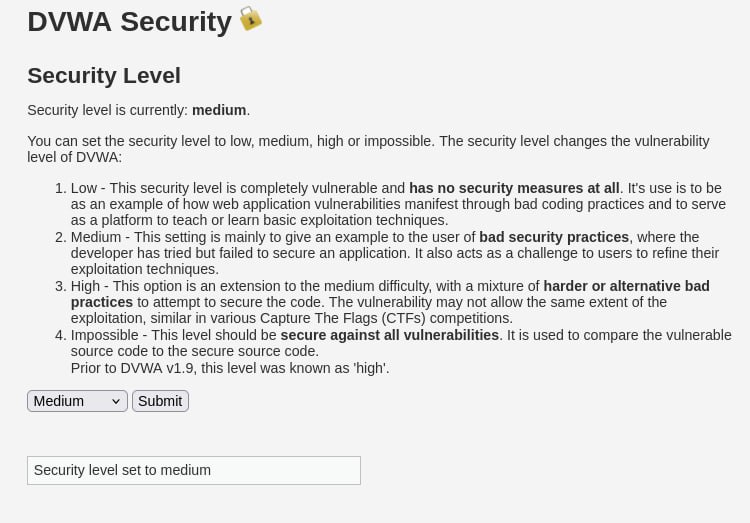


Рис. 3: DVWA security level: Medium

Захожу на страничку про Brute Force, пытаюсь войти с случайным паролем. Не выходит, для работы с Hydra нам потребуется Cookie нашего веб приложения. Нужные нам куки можно найти, открыв инструменты разработчика в браузере (рис. 4).

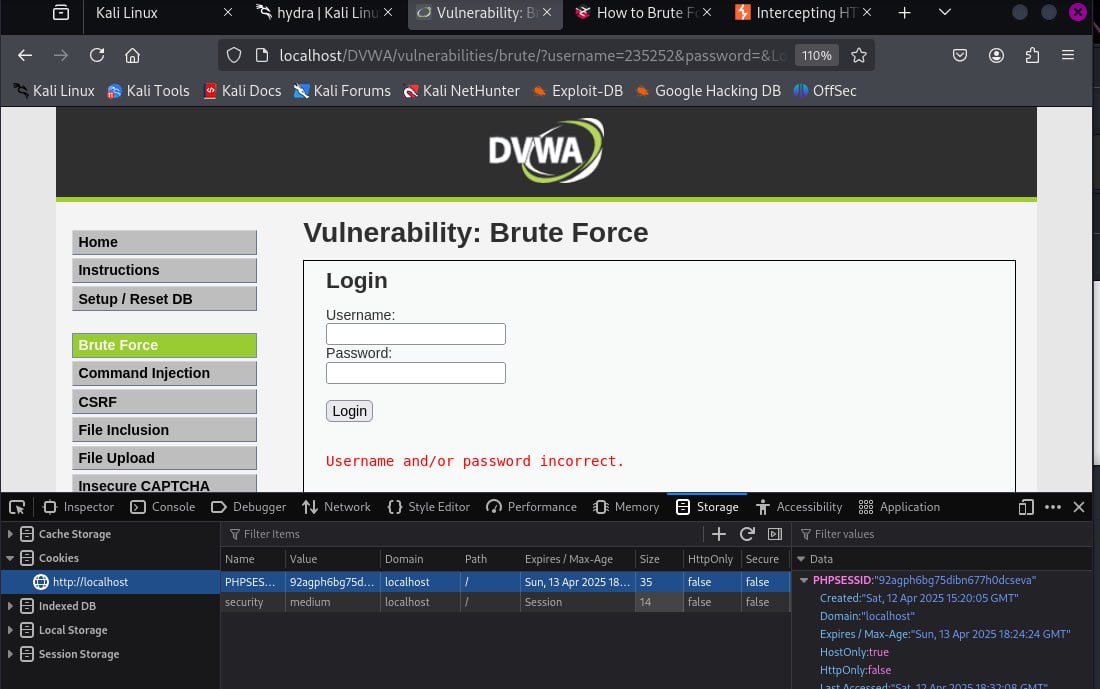


Рис. 4: Нахожу Cookie

После этого пишу следующую команду (рис. 5):

hydra -l admin -P /usr/share/wordlists/rockyou.txt localhost http-get-form "/DVWA/vulnerabilities/brute/:username=^USER^&password=^PASS^&Login=Login:H=Cookie: PHPSESSID=92agph6bg75dibn677h0dcseva; security=medium:F=Username and/or password incorrect." -V

* -l admin - логин всегда будет admin
* -p /путь/ - указываем пароли и подаём путь к файлу со списком
* http-get-form - используем http GET-request, также существует POST-Request, и Hydra его поддерживает, но на уровне защиты medium такой реквест не сработает.

Теперь сам реквест: “/DVWA/vulnerabilities/brute/:username=USER&password=PASS&Login=Login:H=Cookie: PHPSESSID=92agph6bg75dibn677h0dcseva; security=medium:F=Username and/or password incorrect.” -V”

* Мы указываем путь к нашей веб-страничке: /DVWA/vulnerabilities/brute/
* Указываем, что username и пароль те, что мы подали в начале команды,
* Подаём H= наши куки,
* а F= - текст, который выводится при неправильном логине - так Hydra будет понимать, что попытка подобрать пароль не было успешной, если в веб-страничке встречается такой текст.
* -V пишу, чтобы команда выводила более детальную информацию

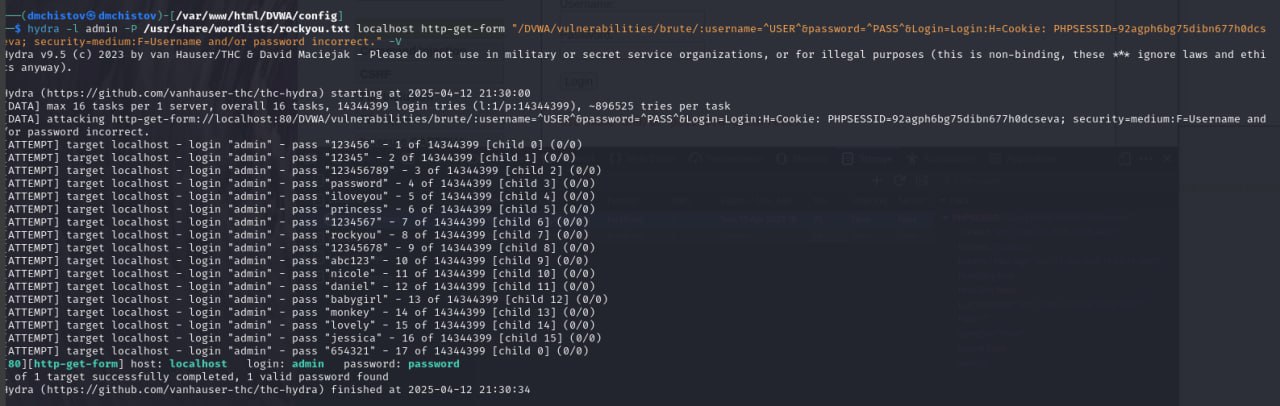


Рис. 5: Работа Hydra

После того, как Hydra закончила работу. Она нам сообщила, что подоходящий пароль - password. Воспользуемся им при входе. Всё успешно! Мы взломали аккаунт Brute Force’ом и теперь имеем доступ (рис. 6).

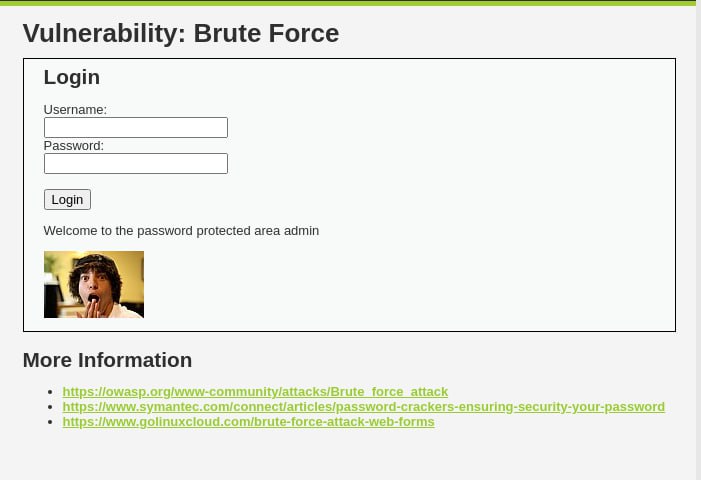


Рис. 6: Аккаунт взломан

# 3 Выводы

При выполнении данной работы я успешно получил навыки работы с Hydra, а также изучил метод уязвимости - Brute Force

# 4 Список литературы

[Индивидуальный проект](https://esystem.rudn.ru/mod/page/view.php?id=1220137#citeproc_bib_item_1)

[о Hydra в Kali Linux](https://www.kali.org/tools/hydra/)

[Список паролей в Kali Linux](https://www.kali.org/tools/wordlists/)