Отчет по индивидуальному проекту. Этап 3

Hydra. Bruteforce, DVWA

Вакутайпа Милдред

Содержание

Список иллюстраций

Список таблиц

# 1 Цель работы

Получить практические навыки по использованию hydra для брутфорса паролей.

# 2 Задание

Реализовать эксплуатацию уязвимости с помощью bruteforce паролей.

# 3 Выполнение лабораторной работы

Перед началой работы, я установила список часто всречающихся паролей. Прверяю ,что список есть и продолжаю работу:

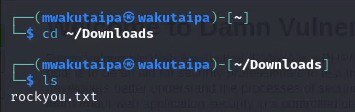


Рис. 1: Загрузка список паролей

Потом войду в аккаунт DVWA, который создала в предыдущой работы и нажимаю brute force:

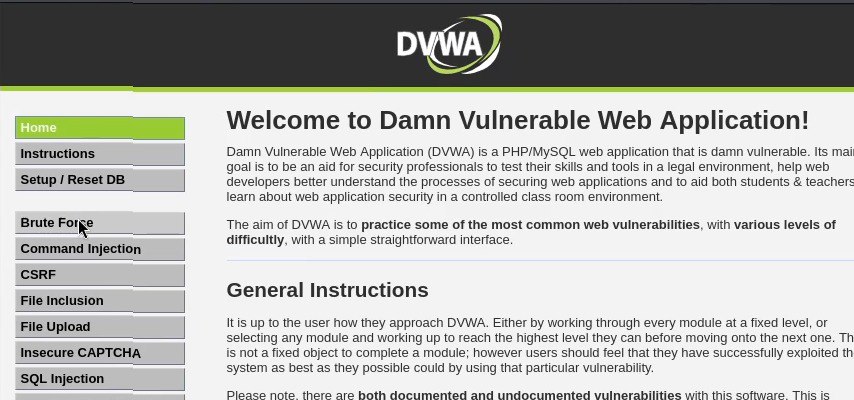


Рис. 2: DVWA домашняя страница

С помощью man читаю справку по hydra, чтобы понять чуть подробнее с чем он работает. Мне понадобится опции -l (логин) и -p(пароль):

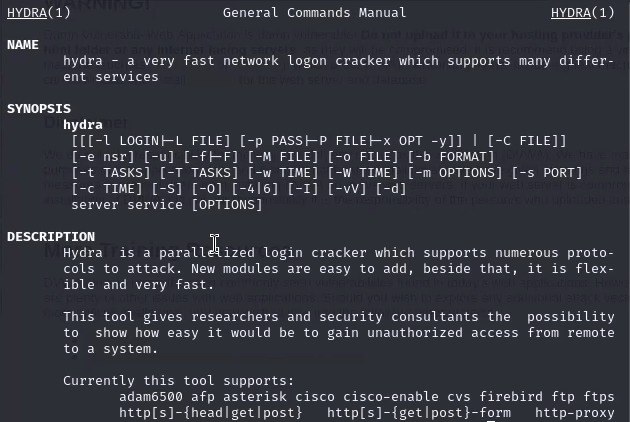


Рис. 3: информация по hydra

Пароль побираю для пользователя admin с файла rockyou.txt используя get-запрос с параметрами cookie и PHPSESSID. При использовании -p, выводится пароль как имя и место положение файла (home/mwakutaipa/rockyou.txt):

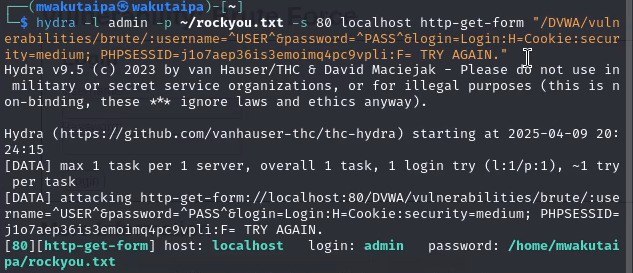


Рис. 4: Попытка 1 взломать пароль

При использовании -P пароль выводится:

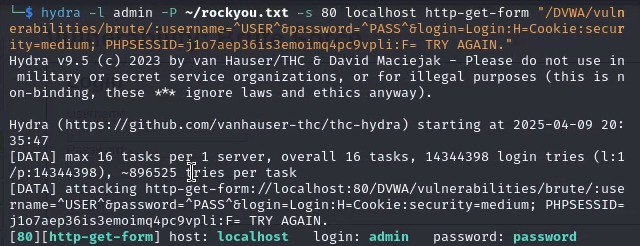


Рис. 5: Попытка 2 взломать пароль

Вхожу в систему с данной паролей чтобы проверят ,что пароль правилный:



Рис. 6: Проверка

# 4 Выводы

Получила практические навыки по использованию hydra для брутфорса паролей.

# Список литературы