Индивидуальный проект. Этап 3.

Использование Hydra

Диана Алексеевна Садова

Содержание

# 1 Цель работы

Разобратся в работе Hydra и взломать пользовательскую запись на DVWA.

# 2 Последовательность выполнения работы

1. Скачать словарь можно с GitHub. Архив весит 50.8мб. (рис. 1).

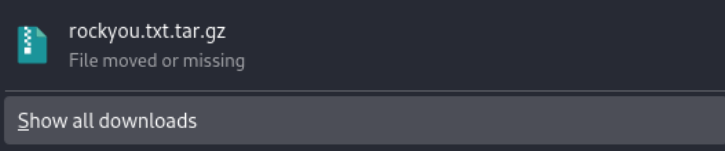


Рис. 1: Скачиваем словать

1. Разархивируем его на рабочий стол (рис. 2), (рис. 3).

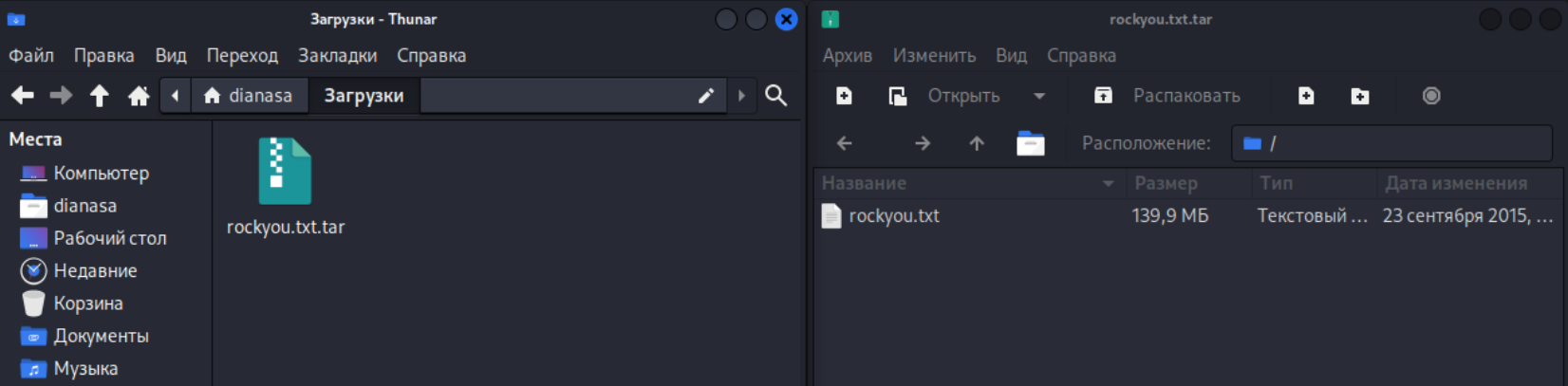


Рис. 2: Открываем сам арфив

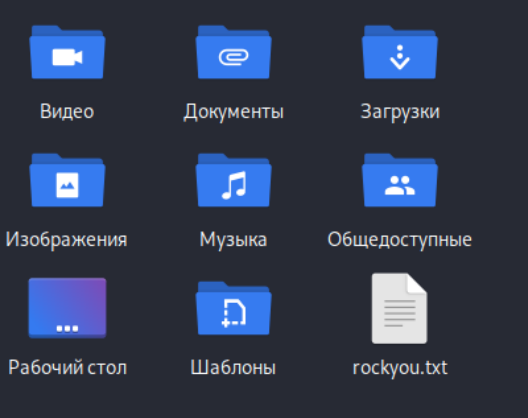


Рис. 3: Файл на рабочем столе

1. Переходим в окно DVWA и открываем панель кода страници (Важно: перед открытием обновите страницу). Нам нужна вкладка Cookies. Находим PHPSESSID и копируем строку Value (рис. 4).

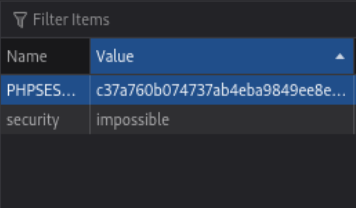


Рис. 4: PHPSESSID и Value

1. Переходим в консоль и используем заготовленую строку с ТУИС для работы Hydra. Добавляем на место PHPSESSID, полученный из предыдущего шага, код и запускаем программу. У нас должно вывестись логин и пароль от пользователя (меня) к сайту DVWA (рис. 5).

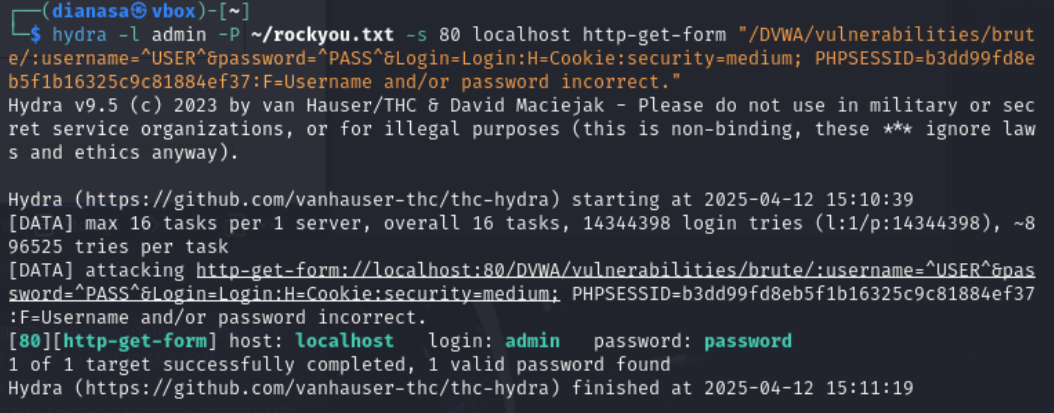


Рис. 5: Пароль для сайта

1. Проверяем правильность пароля и логина (рис. 6).

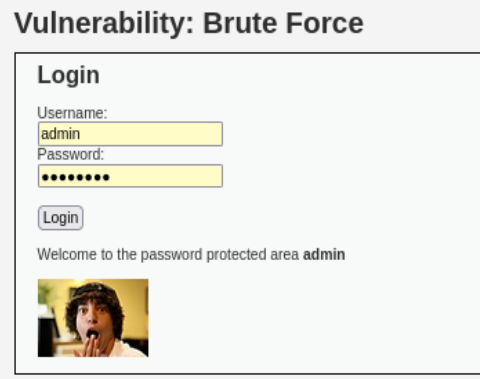


Рис. 6: Пароль подходит

# 3 Выводы

Мы смогли разобратся с работой Hydra и достать пароль и логин пользователя (меня).

# Список литературы