Индивидуальный проект. Этап 3

Дисциплина: Основы информационной безопасности

Жибицкая Евгения Дмитриевна

Содержание

# 1 Цель работы

Продолжение выполнения проекта. Брутфорсинг пароля на созданном ранее DVWA, использование Hydra.

# 2 Выполнение работы

Для брутфорсинга пароля используем настроенное ранее DVWA. Запустим сервер, перейдем на вкладку Brute Force и получим сообщение о неверно введенных даннных(рис. 1).

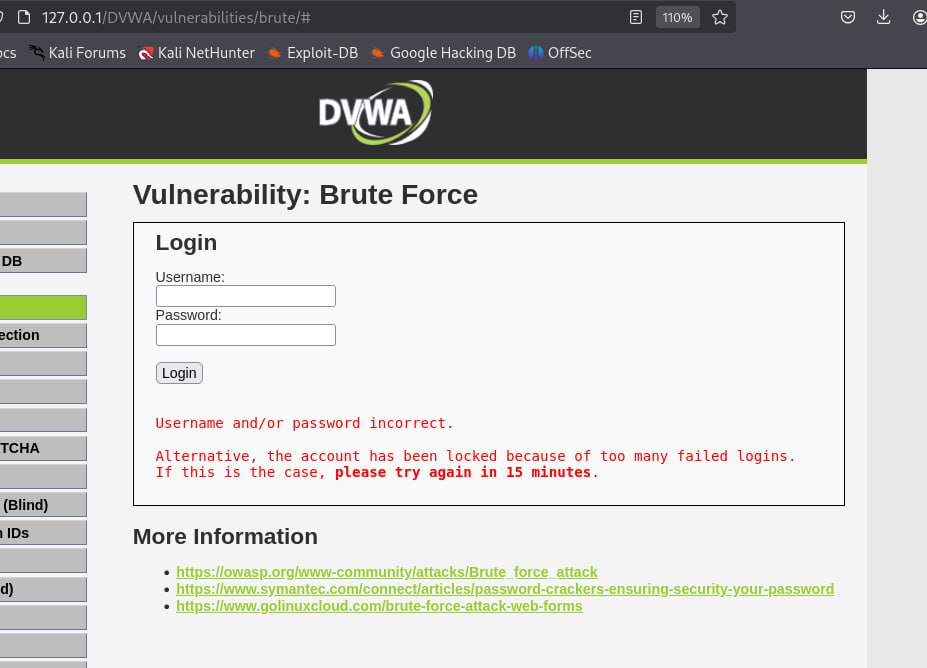


Рис. 1: Попытка авторизации

Далее скачаем список паролей, необходимый для дальнейшего пароля. Я использую rockyou.txt(рис. 2).

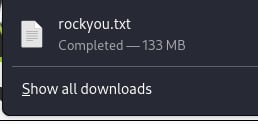


Рис. 2: Файл паролей

Далее сформируем сам запрос к hydra( на kali она предустановлена). Укажем сначала имя пользователя, к которому подбирается запроси файл для поиска паролей. Используем http-post-form потому, что авторизация происходит по http методом post.

После указания этого модуля идёт строка /cgi-bin/luci:username=USER&password=PASS:“…”” путь до скрипта, который обрабатывает процесс аутентификации (/cgi-bin/luci);строка, которая передаётся методом POST, в которой логин и пароль заменены на USER и PASS соответственно (username=USER&password=PASS); строка, которая присутствует на странице при неудачной аутентификации; при её отсутствии Hydra поймёт, что мы успешно вошли(рис. 3).

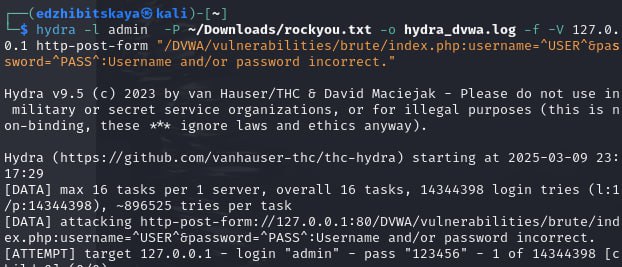


Рис. 3: Запрос к hydra

Далее происходит перебор и поиск пароля(рис. 4).

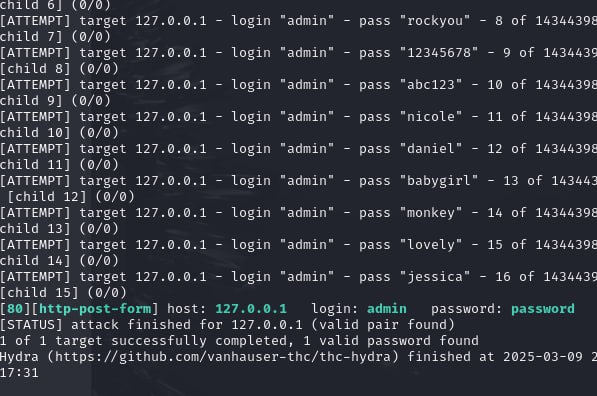


Рис. 4: Поиск и нахождение пароля

Проверка и попытка войти(рис. 5).

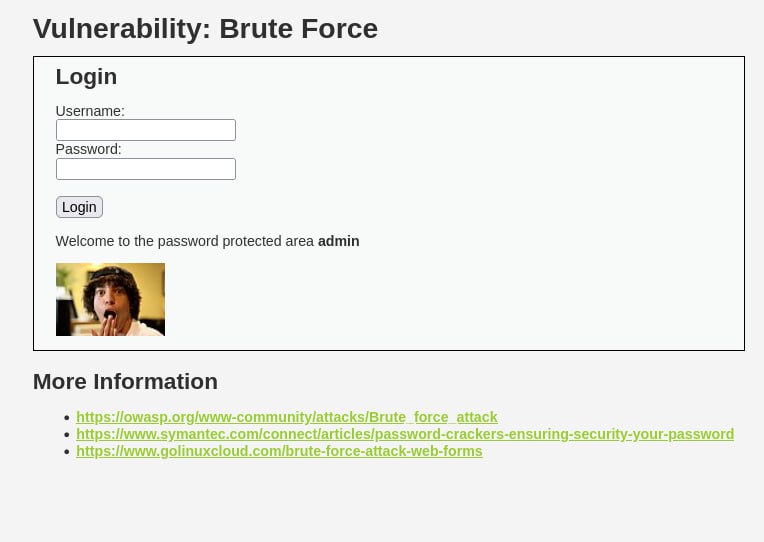


Рис. 5: Вход

# 3 Выводы

В ходе работы были приобретены навыки по работе с hydra, была произведена попытка брутфорса паролей на DVWA.

# Список литературы

* [ТУИС](https://esystem.rudn.ru/mod/page/view.php?id=1220336)
* Парасрам, Ш. Kali Linux: Тестирование на проникновение и безопасность : Для профессионалов. Kali Linux / Ш. Парасрам, А. Замм, Т. Хериянто, и др. – Санкт-Петербург : Питер, 2022. – 448 сс.