Индивидуальный проект. Третий этап

Чемоданова А.А.

Содержание

# 1 Цель работы

Использование Hydra.

# 2 Выполнение лабораторной работы

Hydra используется для подбора или взлома имени пользователя и пароля. Поддерживает подбор для большого набора приложений.

Установка Hydra. (рис. [1](#fig:001)).

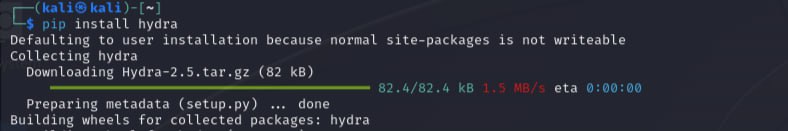


Figure 1: Установка Hydra

Пример работы:

Исходные данные: IP сервера 178.72.90.181; Сервис http на стандартном 80 порту; Для авторизации используется html форма, которая отправляет по адресу http://178.72.90.181/cgi-bin/luci методом POST запрос вида username=root&password=test\_password; В случае не удачной аутентификации пользователь наблюдает сообщение Invalid username and/or password! Please try again.

Запрос к Hydra будет выглядеть примерно так:

hydra -l root -P ~/pass\_lists/dedik\_passes.txt -o ./hydra\_result.log -f -V -s 80 178.72.90.181 http-post-form “/cgi-bin/luci:username=USER&password=PASS:Invalid username”

Используется http-post-form потому, что авторизация происходит по http методом post. После указания этого модуля идёт строка /cgi-bin/luci:username=USER&password=PASS:Invalid username, у которой через двоеточие (:) указывается: 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 (Invalid username).

Ввод запроса. (рис. [2](#fig:002)).



Figure 2: Запрос

# 3 Выводы

Мы применили Hydra.