Основы информационной безопасности

Индивидуальный проект № 3. Использование Hydra

Смирнов-Мальцев Егор Дмитриевич

Содержание

# 1 Цель работы

Научиться взламывать пользователя с помощью Hydra.

# 2 Теоретическое введение

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

Пример работы:

1. 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.
2. 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"

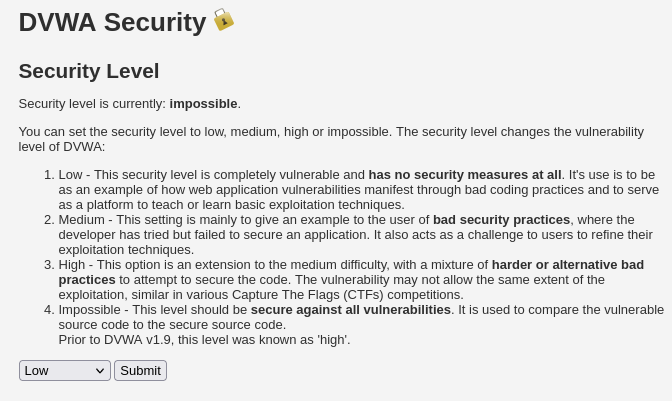
1. Используется http-post-form потому, что авторизация происходит по http методом post. После указания этого модуля идёт строка /cgi-bin/luci:username=USER&password=PASS:Invalid username, у которой через двоеточие (:) указывается:

* 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).

Более подробно про Unix см. в [1–4].

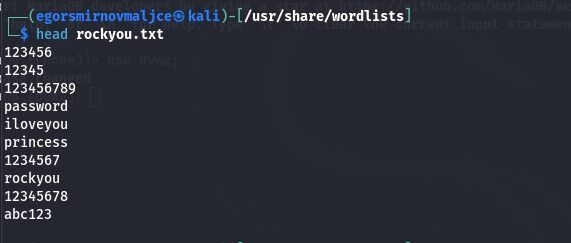
# 3 Выполнение лабораторной работы

Установил низкий уровень безопасности в DVWA (рис. ??).



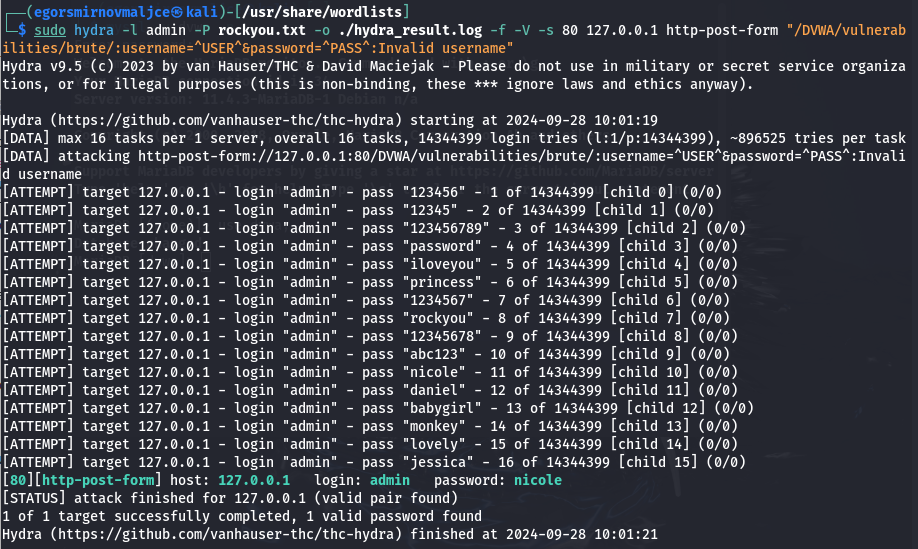
Окно DVWA с установкой уровня безопасности

Нашел файл с наиболее частыми паролями (рис. ??).



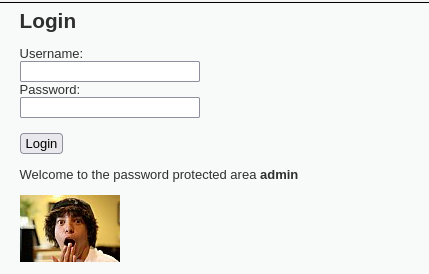
Наиболее частые пароли

Использовал найденный файл, чтобы гидра смогла найти нужный пароль (рис. ??).



Запрос к Hydra

Проверил правильность пароля (рис. ??).



Вход в учетную запись DVWA

# 4 Выводы

Мы смогли с помощью Hydra взломать пользователя в DVWA.

# Список литературы

1. Таненбаум Э., Бос Х. Современные операционные системы. 4-е изд. СПб.: Питер, 2015. 1120 с.

2. Robbins A. Bash Pocket Reference. O’Reilly Media, 2016. 156 с.

3. Zarrelli G. Mastering Bash. Packt Publishing, 2017. 502 с.

4. Newham C. [Learning the bash Shell: Unix Shell Programming](http://www.amazon.com/Learning-bash-Shell-Programming-Nutshell/dp/0596009658). O’Reilly Media, 2005. 354 с.