Отчет по третьему этапу индивидуального проекта

Основы информационной безопасности

Чванова Ангелина Дмитриевна, НПИбд02-21

Содержание

Список иллюстраций

Список таблиц

Цель работы

Приобретение практических навыков по использованию инструмента Hydra для брут-форса паролей.

Задание

1. Необходимо реализовать эксплуатацию уязвимости с помощью брутфорса паролей.

Теоретическое введение

- Hydra используется для подбора или взлома имени пользователя и пароля.
- Поддерживает подбор для большого набора приложений [@brute, @force, @parasram].

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 неудачной 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=
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).

Выполнение лабораторной работы

Чтобы пробрутфорсить пароль, необходимо сначала найти большой список частоиспользуемых паролей. Его можно найти в открытых источниках, в рамках данного этапа был взят стандартный список паролей `rockyou.txt` для kali linux (рис. 1).

Рис. 1: Распаковка архива со списком паролей

Сайт DVWA, полученный в ходе предыдущего этапа проекта. Для запроса hydra нужны параметры cookie с этого сайта (рис. 2).

Рис. 2: Сайт, с которого получаем информацию о параметрах Cookie

Для того чтобы получить информацию о параметрах cookie я было установлено соответствующее расширение для браузера [@cookies], теперь можно не только посмотреть параметры cookie, но и скопировать их (рис. 3).

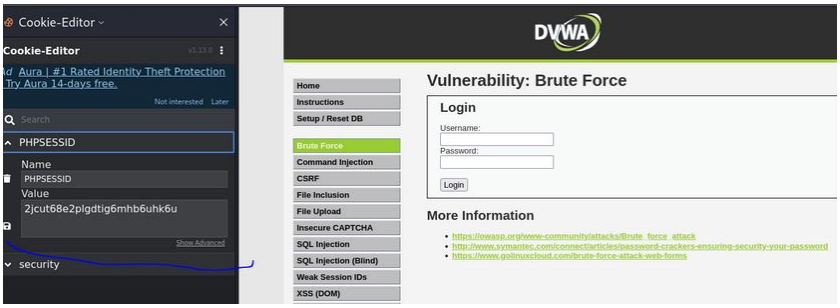

Рис. 3: Информация о параметрах Cookie

Hydra запрос с нужной информацией. Пароль будем подбирать для пользователя admin, используем GET-запрос с двумя параметрами cookie: безопасность и PHPSESSID, найденными в прошлом пункте (рис. 4).

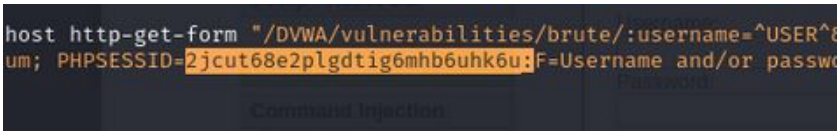

Рис. 4: Запрос Hydra

Спустя некоторое время в результат запроса появится результат с подходящим паролем (рис. 5).

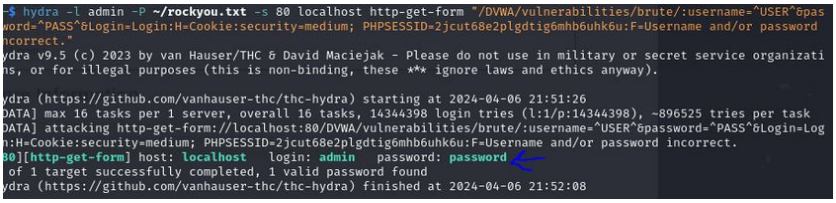

Рис. 5: Результат запроса

Полученные данные были введены на сайт для проверки (рис. 6).

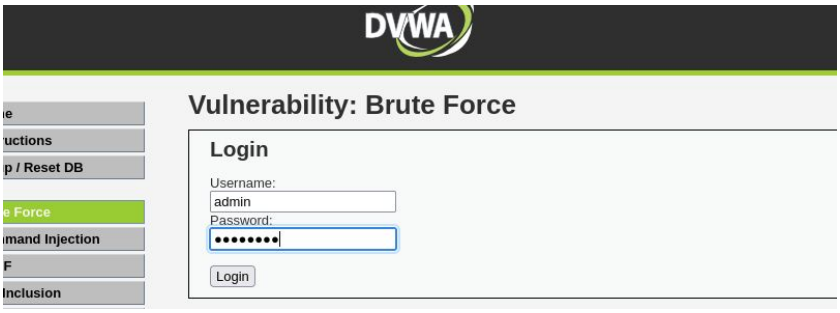

Рис. 6: Ввод полученного результата в уязвимую форму

Был получен положительный результат проверки пароля. Все сделано верно (рис. 7).

Рис. 7: Результат

Выводы

Приобрела практические навыки по использованию инструмента Hydra для брутфорса паролей

Список литературы

[1] Документация по Virtual Box: https://www.virtualbox.org/wiki/Documentation