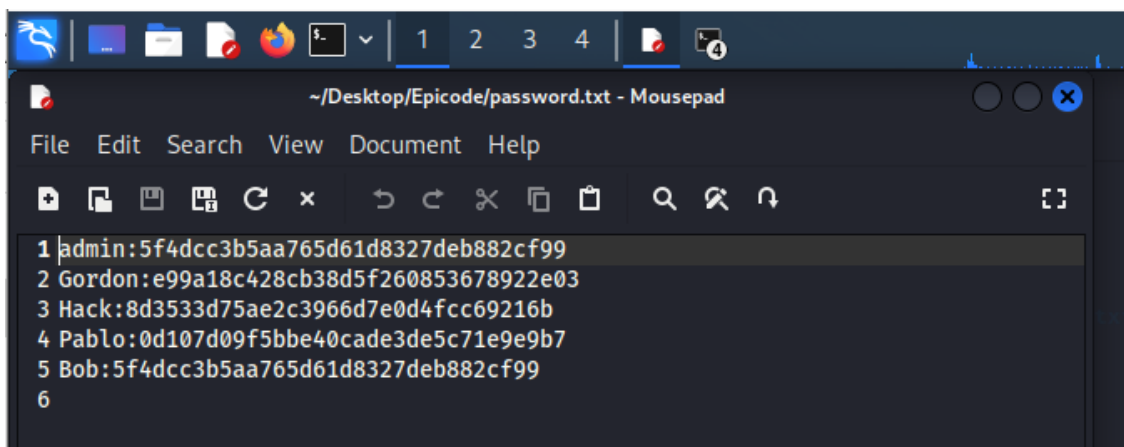


CRACKARE HASH DELLE PASSWORD

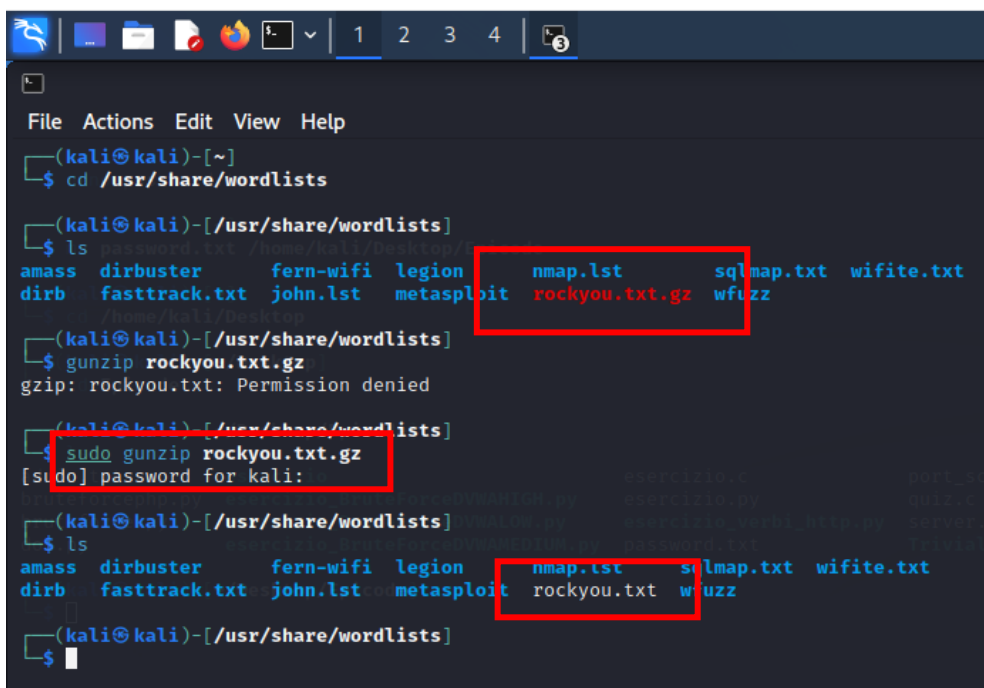
Partiamo innanzitutto dagli hashing delle password trovate ieri tramite attacco di SQL Injection:



In questa guida per poter crackare una password in hash, useremo il tool John the Ripper; come prima cosa creiamo un file (in questo caso ho creato un .txt perché a mio avviso era più facile la procedura) con l'abbinamento username e password:



Per ridurre il tempo di cracking del tool, usiamo una wordlist, che già si trova all'interno del nostro Kali, chiamata rockyou.txt; per poterla usare però la dobbiamo unzippare come nell'immagine sottostante:



```
(kali@kali)-[~]
$ cd /usr/share/wordlists

(kali@kali)-[/usr/share/wordlists]
$ ls
amass  dirbuster  fern-wifi  legion  nmap.lst  sqlmap.txt  wifite.txt
dirb   fasttrack.txt john.lst  metasploit  rockyou.txt.gz  wfuzz

(kali@kali)-[/usr/share/wordlists]
$ gunzip rockyou.txt.gz
gzip: rockyou.txt: Permission denied

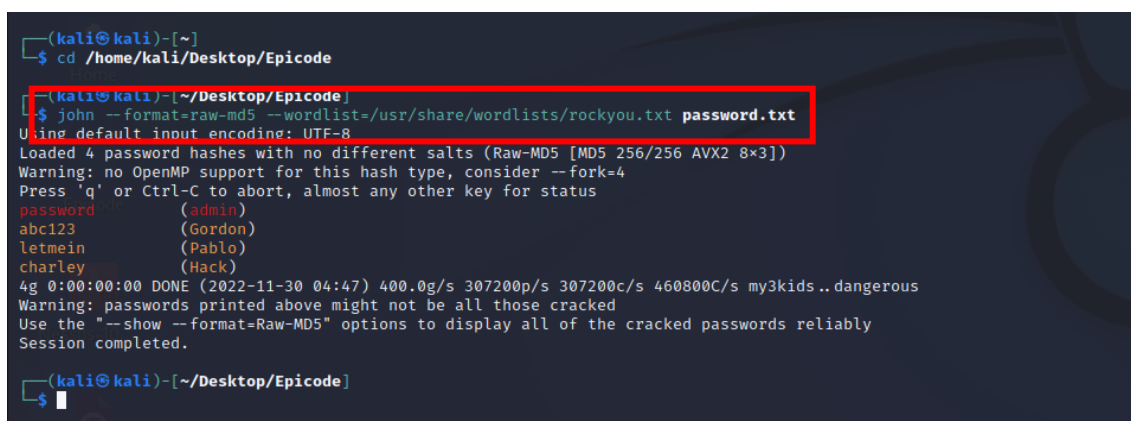
(kali@kali)-[/usr/share/wordlists]
$ sudo gunzip rockyou.txt.gz
[sudo] password for kali:

(kali@kali)-[/usr/share/wordlists]
$ ls
amass  dirbuster  fern-wifi  legion  nmap.lst  sqlmap.txt  wifite.txt
dirb   fasttrack.txt john.lst  metasploit  rockyou.txt  wfuzz

(kali@kali)-[/usr/share/wordlists]
$
```

Possiamo ora lanciare il tool John the Ripper che, come già detto, ci permette di decodificare gli hash delle password sia con metodi brute force che tramite l'assegnazione di un elenco di password (come nel nostro caso).

Il comando da usare lo troviamo nell'immagine:



```
(kali@kali)-[~]
$ cd /home/kali/Desktop/Epicode

(kali@kali)-[~/Desktop/Epicode]
$ john --format=raw-md5 --wordlist=/usr/share/wordlists/rockyou.txt password.txt
Using default input encoding: UTF-8
Loaded 4 password hashes with no different salts (Raw-MD5 [MD5 256/256 AVX2 8x3])
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 (Gordon)
letmein (Pablo)
charley (Hack)
4g 0:00:00:00 DONE (2022-11-30 04:47) 400.0g/s 307200p/s 307200c/s 460800C/s my3kids..dangerous
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.

(kali@kali)-[~/Desktop/Epicode]
$
```

Procediamo quindi con l'inserimento dell'username e della password trovata nel login di DVWA; lo ho usato Pablo e la sua password che è "letmein".

Welcome to Damn Vulnerable Web App!

Damn Vulnerable Web App (DVWA) is a PHP/MySQL web application that is damn vulnerable. Its main goals are to be an aid for security professionals to test their skills and tools in a legal environment, help web developers better understand the processes of securing web applications and aid teachers/students to teach/learn web application security in a class room environment.

WARNING!

Damn Vulnerable Web App is damn vulnerable! Do not upload it to your hosting provider's public html folder or any internet facing web server as it will be compromised. We recommend downloading and installing [XAMPP](#) onto a local machine inside your LAN which is used solely for testing.

Disclaimer

We do not take responsibility for the way in which any one uses this application. We have made the purposes of the application clear and it should not be used maliciously. We have given warnings and taken measures to prevent users from installing DVWA on to live web servers. If your web server is compromised via an installation of DVWA it is not our responsibility it is the responsibility of the person/s who uploaded and installed it.

General Instructions

The help button allows you to view hits/tips for each vulnerability and for each security level on their respective page.

You have logged in as 'Pablo'

Username: Pablo
Security Level: high
PHPIDS: disabled

Damn Vulnerable Web Application (DVWA) v1.0.7

Qui possiamo vedere che siamo loggati come Pablo.