1 ASIX

**MÒDUL 11: SEGURETAT I ALTA DISPONIBILITAT**

ACTIVITAT 1.4: Atacs de força bruta

línea horizontal

# 



**Alumne**: Daniel Mascarilla del Olmo

**Professor**: Sergi Andrés

**Curs**: 1 ASIX

**Centre**: Jaume Viladoms

**ÍNDEX**

[**Exercici 1 – Atac de força bruta a un fitxer .zip amb diccionari**](#_b0im62s1zg92) **3**

[a. Crea un fitxer .zip amb un password fàcil de 6 caràcters (només numeros) Exemple à zip --password 123456 fitxer1.zip /home/usuari/\*](#_66fq9jtb45xk) 3

[b. Crea un altre fitxer .zip amb un password de 4 caràcters (només lletres minúscules)](#_gnnit9dn0hhr) 3

[c. Amb la eina zip2john, extreu el hash de cada fitxer Exemple à zip2john fitxer.zip > hash.txt](#_wk5d3ejbksp1) 3

[d. Intenta’ls crackejar utilitzant John The Ripper a partir del diccionari fasttrack.txt o rockyou.txt que pots trobar a la carpeta /usr/share/wordlists john hash.txt --wordlist=/usr/share/wordlists/fasttrack.txt](#_ose1cc1n76ux) 5

[e. Torna a provar de fer l’exercici amb algun password més complicat](#_aonoyz507fxb) 5

[f. Fes el teu diccionari de paraules i torna a intentar crackejar-lo](#_fjo03urrvzxk) 6

[**Exercici 2 – Creació d’un diccionari amb l’eina crunch**](#_nt4nirsvdhwi) **7**

[a. Crea un diccionari que contingui totes les combinacions possibles de passwords de llargada 6, utilitzant només números](#_b4141qd2imcy) 7

[b. Crea un diccionari que contingui totes les combinacions possibles de passwords de llargada 4, utilitzant lletres minúscules](#_9n3r1qgz96zi) 8

[c. Amb els 2 diccionaris creats, prova de crackejar els fitxers .zip de l’exercici anterior.](#_e0o96wvzygnw) 9

[d. Com faries un diccionari de 8 xifres utilitzant minúscules, majúscules i números? Quin espai ocuparia?](#_gakl8sgna3p6) 9

[**Exercici 3 – Atac de força bruta amb la eina fcrackzip**](#_8cl1owphtzfr) **11**

[a. Per a instal·lar à sudo apt install fcrackzip](#_o432amkf40w3) 11

[b. Per a veure l’ajuda à fcrackzip -h](#_9rif4230ase9) 11

[c. Posa un password de 4 caràcters a un fitxer .ZIP utilitzant només lletres i prova de crackejar-lo](#_grycsxt70gu5) 11

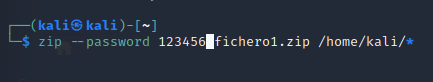
[d. Posa un password de 6 caràcters amb només números i prova de crackejar-lo](#_r407wzcu8gy7) 12

[e. Posa un password de 8 caràcters amb lletres majúscules, minúscules i números i prova de crackejar-lo](#_hu4oklm7ecjj) 14

# Exercici 1 – Atac de força bruta a un fitxer .zip amb diccionari

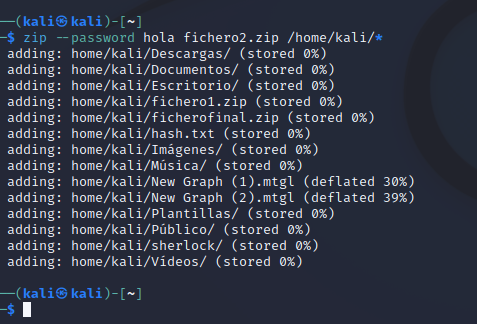
Des d’una màquina Kali Linux utilitzarem la eina John The Ripper (john) per a trobar el password d’un fitxer comprimit .zip Per a fer-ho, cal seguir els següents passos:

### a. Crea un fitxer .zip amb un password fàcil de 6 caràcters (només numeros) Exemple à zip --password 123456 fitxer1.zip /home/usuari/\*

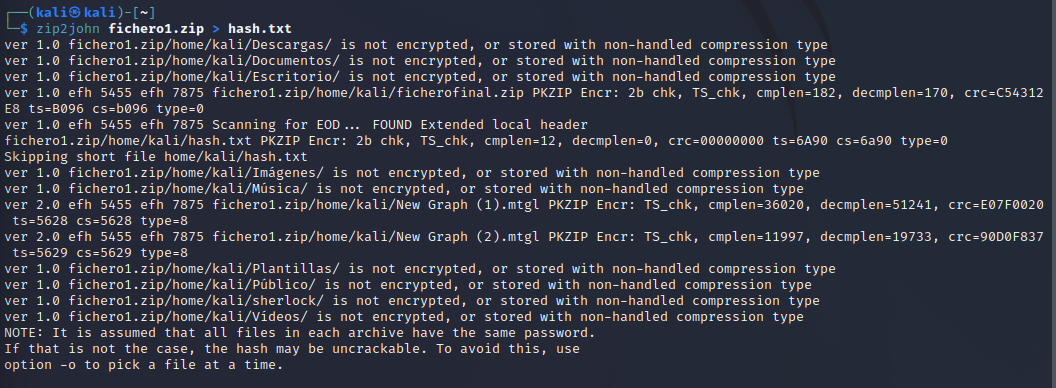


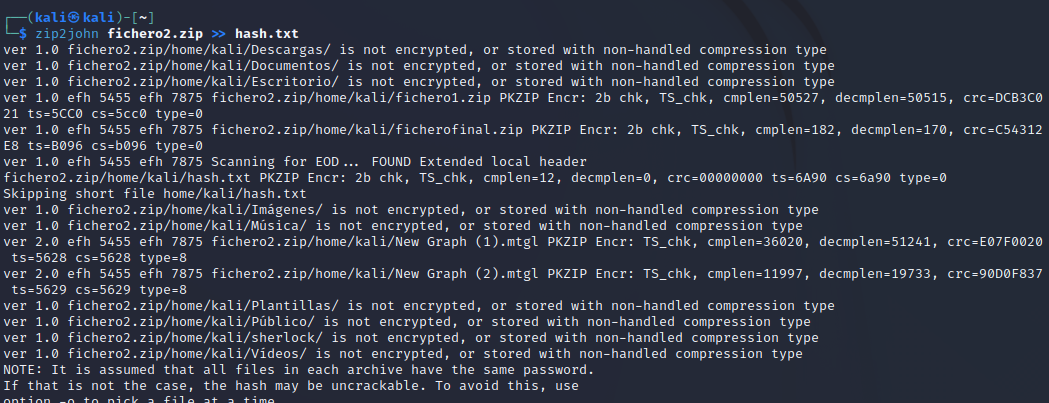


### b. Crea un altre fitxer .zip amb un password de 4 caràcters (només lletres minúscules)



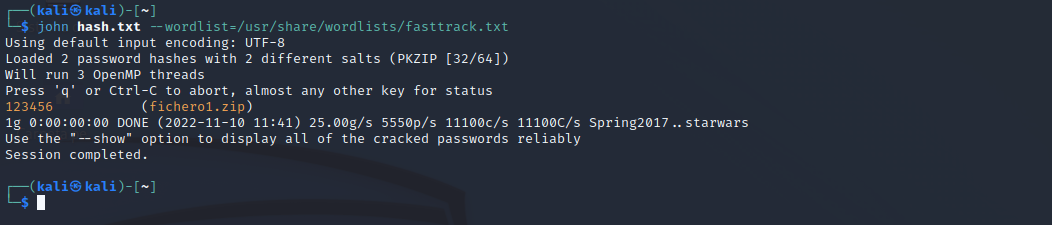
### c. Amb la eina zip2john, extreu el hash de cada fitxer Exemple à zip2john fitxer.zip > hash.txt

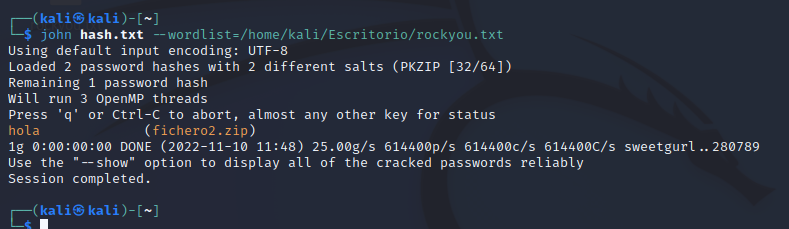




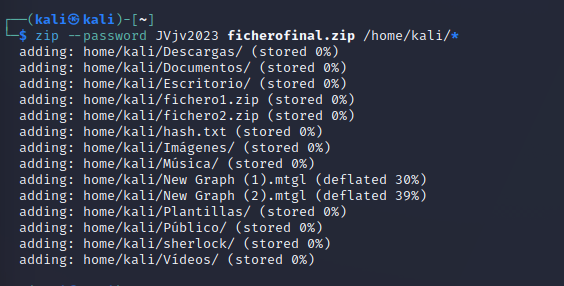
### 

### d. Intenta’ls crackejar utilitzant John The Ripper a partir del diccionari fasttrack.txt o rockyou.txt que pots trobar a la carpeta /usr/share/wordlists john hash.txt --wordlist=/usr/share/wordlists/fasttrack.txt

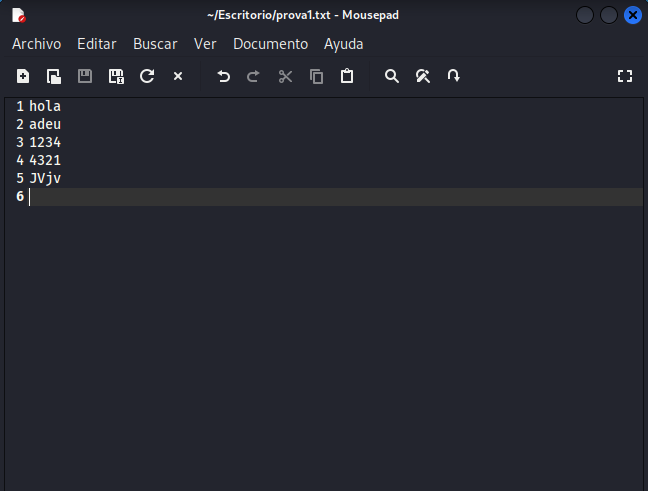


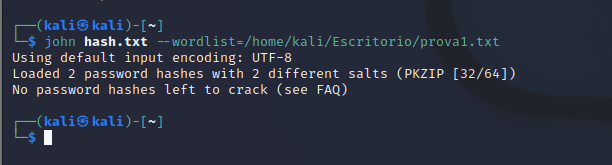


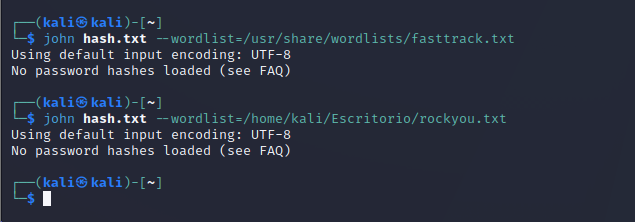
### e. Torna a provar de fer l’exercici amb algun password més complicat



### f. Fes el teu diccionari de paraules i torna a intentar crackejar-lo





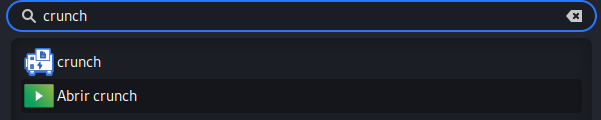


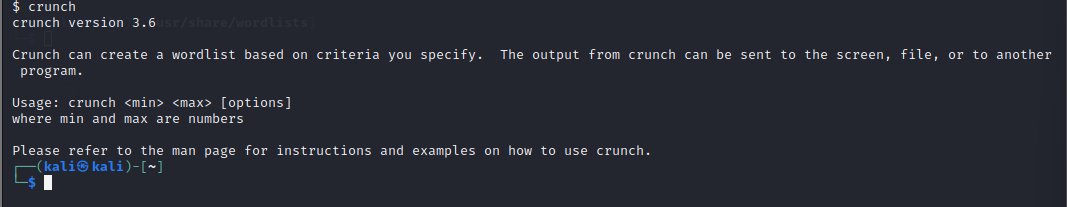
### 

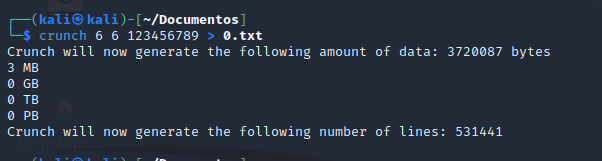
# Exercici 2 – Creació d’un diccionari amb l’eina crunch

Utilitzant la eina crunch, crea els següents diccionaris:

### a. Crea un diccionari que contingui totes les combinacions possibles de passwords de llargada 6, utilitzant només números

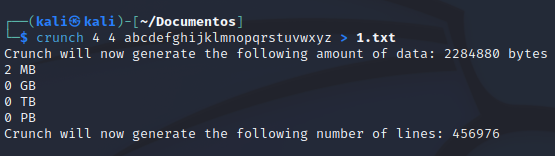








### b. Crea un diccionari que contingui totes les combinacions possibles de passwords de llargada 4, utilitzant lletres minúscules



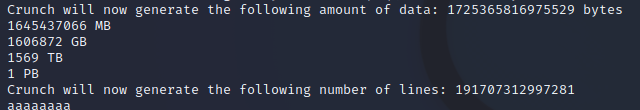
### c. Amb els 2 diccionaris creats, prova de crackejar els fitxers .zip de l’exercici anterior.

### d. Com faries un diccionari de 8 xifres utilitzant minúscules, majúscules i números? Quin espai ocuparia?

El faria de la següent manera:



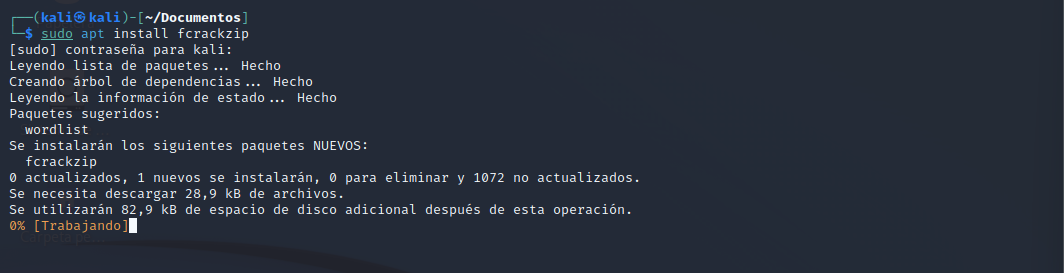
Ocuparia el següent:



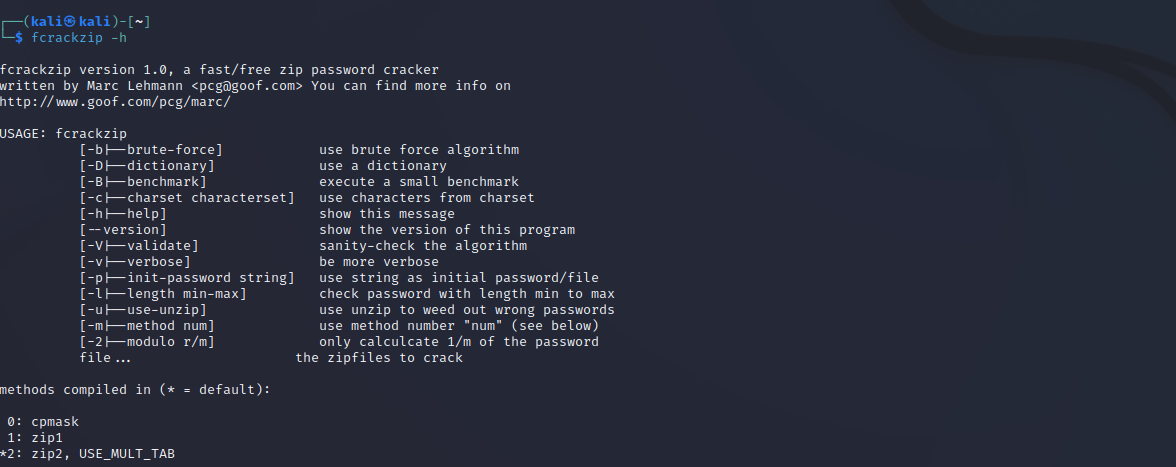
# Exercici 3 – Atac de força bruta amb la eina fcrackzip

Per a no haver de guardar diccionaris que ocupen molt espai, existeixen aplicacions que permeten anar generant els passwords “on the fly” i anar-los provant Instal·la la eina fcrackzip per a crackejar un fitxer .zip amb un diccionari que vas generant:

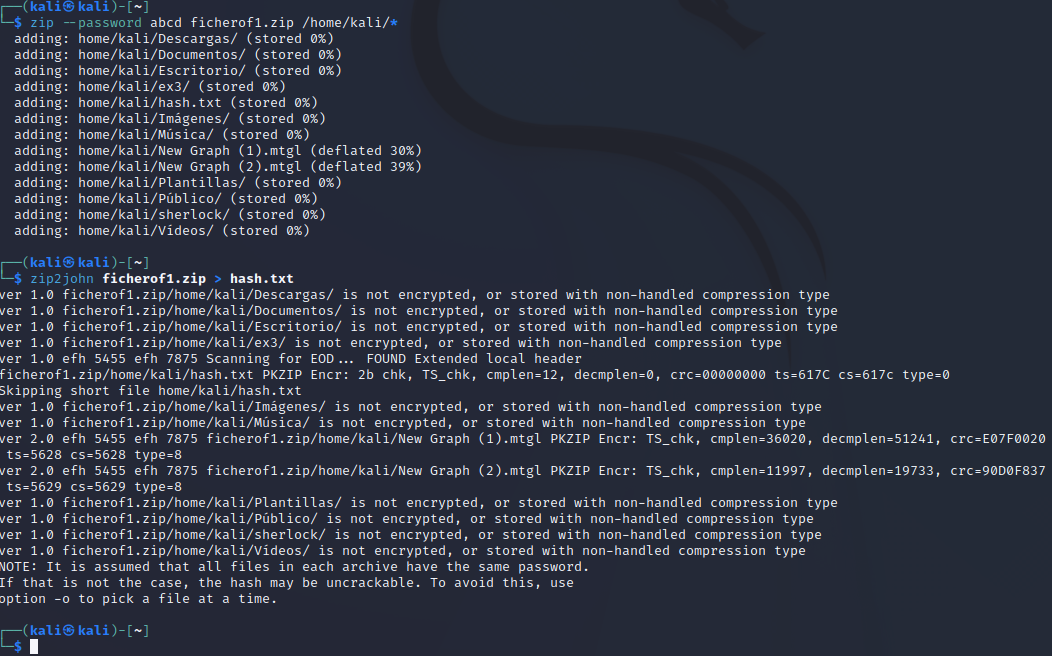
### a. Per a instal·lar à sudo apt install fcrackzip



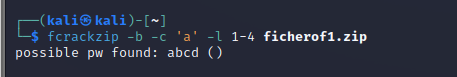
### b. Per a veure l’ajuda à fcrackzip -h



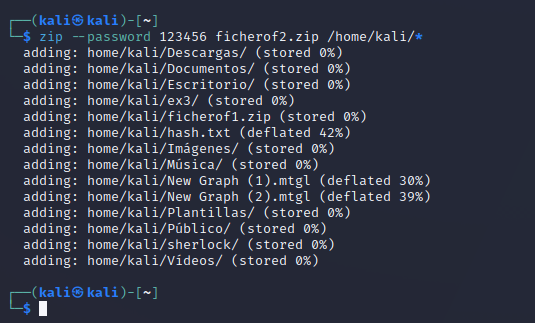
### c. Posa un password de 4 caràcters a un fitxer .ZIP utilitzant només lletres i prova de crackejar-lo

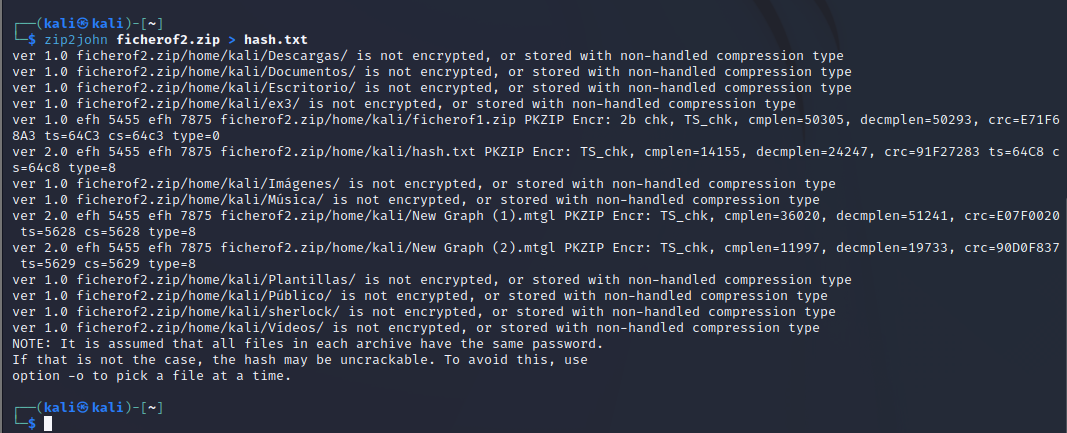


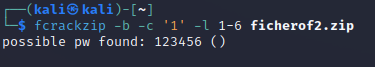




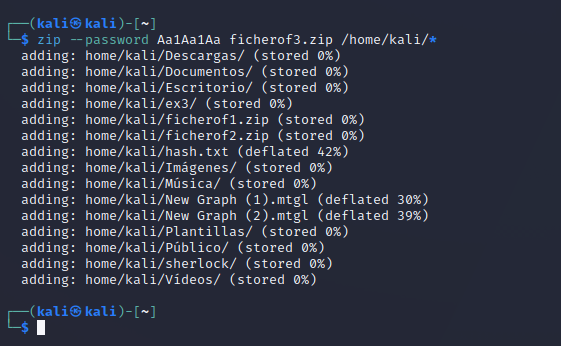
### d. Posa un password de 6 caràcters amb només números i prova de crackejar-lo

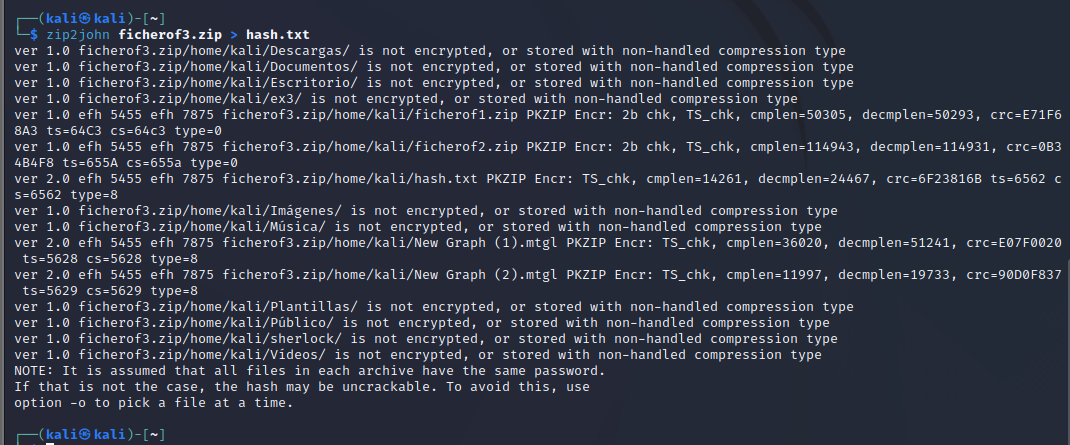


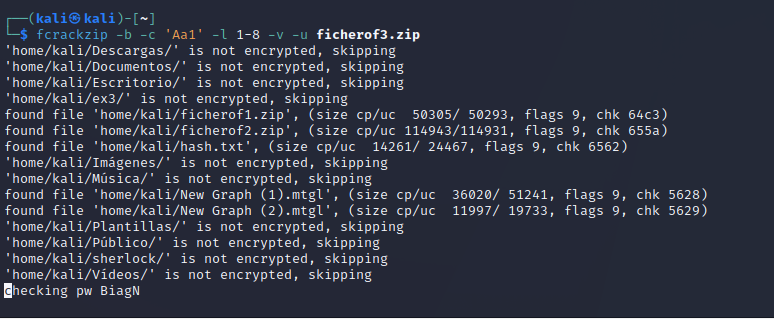




### e. Posa un password de 8 caràcters amb lletres majúscules, minúscules i números i prova de crackejar-lo







Trigarà molt en trobar el password, ja que es un rang molt extens i ha de fer check a cada una de les passwords,.