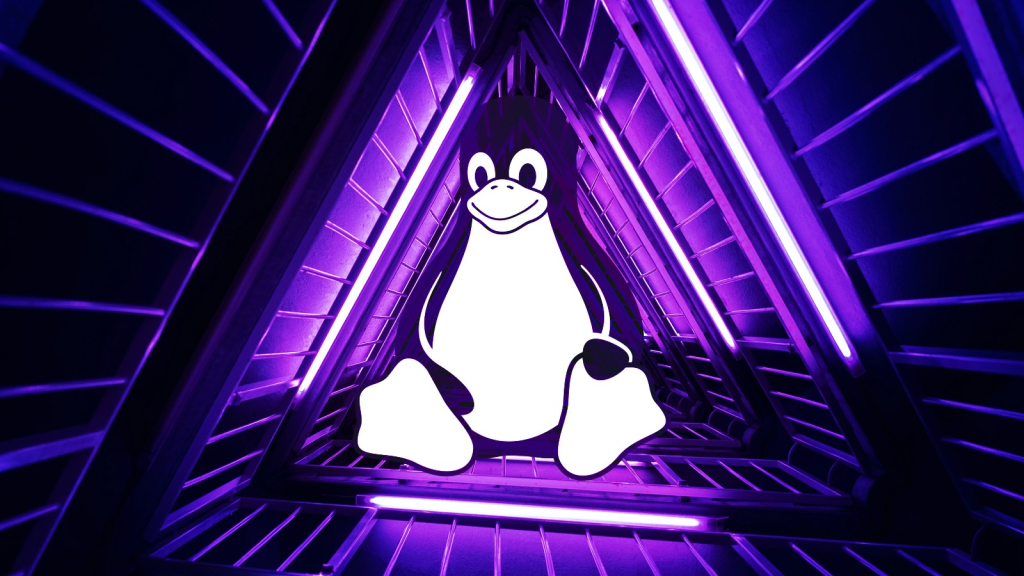
1 ASIX

**MÒDUL 11: SEGURETAT I ALTA DISPONIBILITAT**

ACTIVITAT 1.6: Atacs de força bruta a Linux

línea horizontal

# 



**Alumne**: Daniel Mascarilla del Olmo

**Professor**: Sergi Andrés

**Curs**: 1 ASIX

**Centre**: Jaume Viladoms

**ÍNDEX**

[**Exercici 1 – Usuaris Linux**](#_x0lza7x074yn) **3**

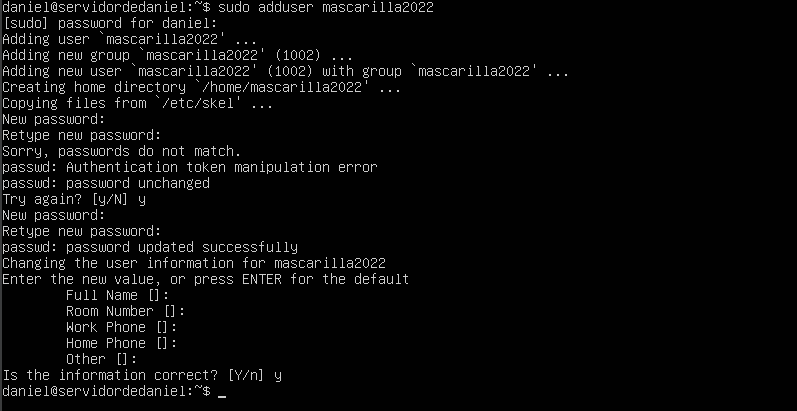
[**Exercici 2 – Hashcat**](#_ypr8k2wnb6on) **5**

[**Exercici 3 – John The Ripper**](#_grcm0or2wju2) **7**

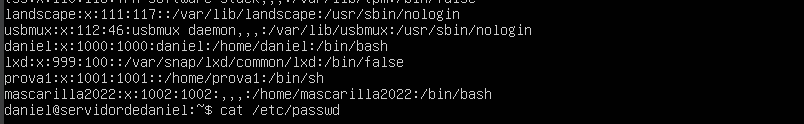
[**Exercici 4 – Hydra**](#_e6qz4upw5w3q) **7**

# Exercici 1 – Usuaris Linux

Crea un usuari anomenat cognom2022:



Mostra tots els usuaris del sistema mostrant el contingut del fitxer /etc/passwd



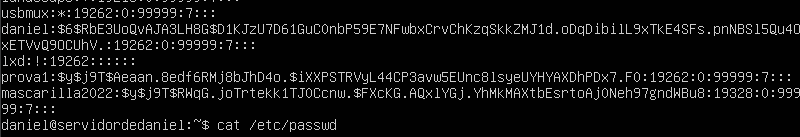
Què significa l’últim paràmetre de /bin/bash que tenen alguns usuaris?

Indica on es troba l'intèrpret d'ordres al nostre sistema.

Què significa el /nologin que tenen altres usuaris?

nologin mostra un missatge que indica que un compte no està disponible i surt diferent de zero. Està dissenyat com un camp d'intèrpret d'ordres per refusar l'accés d'inici de sessió a un compte.

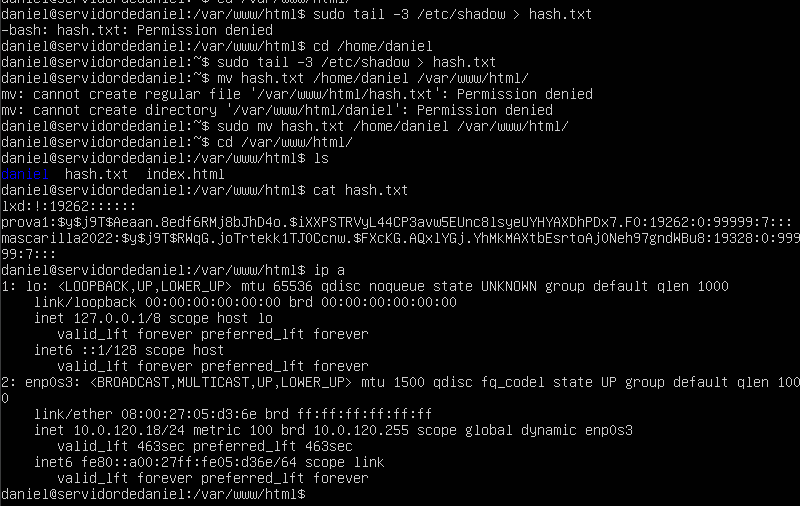
Mostra els hashes dels usuaris mostrant el fitxer /etc/shadow



Amb quina encriptació estan els hashes dels usuaris que poden fer sessió? Raona la resposta

Està en format $6$ (què és el format d’encriptació que s’utilitza només per el primer usuari creat durant la instal·lació de la màquina) i $y$ (què és el format d’encriptació per la resta d’usuaris que no s’han fet durant la instal·lació).

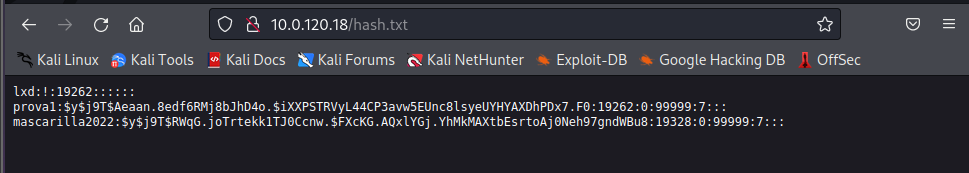
Guarda en un fitxer els hashes dels passwords que vulguis crackejar.

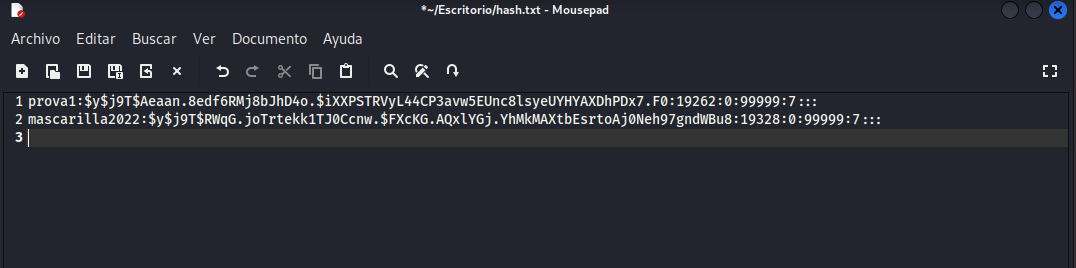


# Exercici 2 – Hashcat

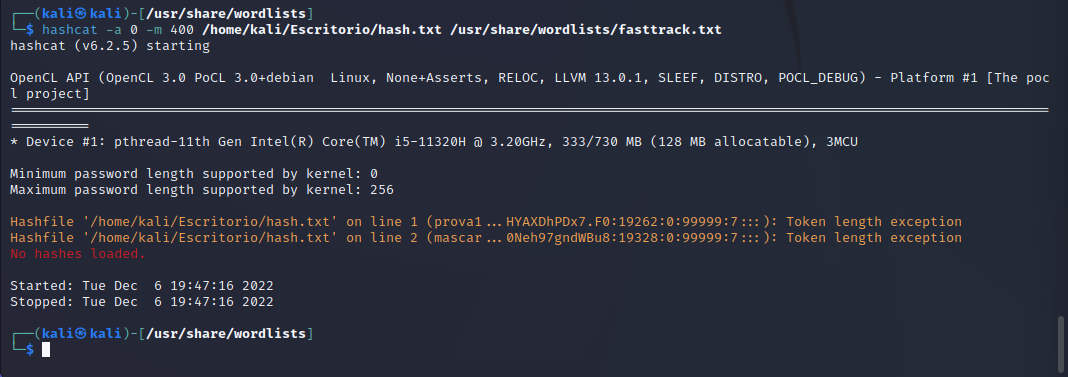
Des d’una màquina Kali Linux, utilitzant Hashcat i algun diccionari de passwords, extreu per força bruta el password dels usuaris que poden fer sessió

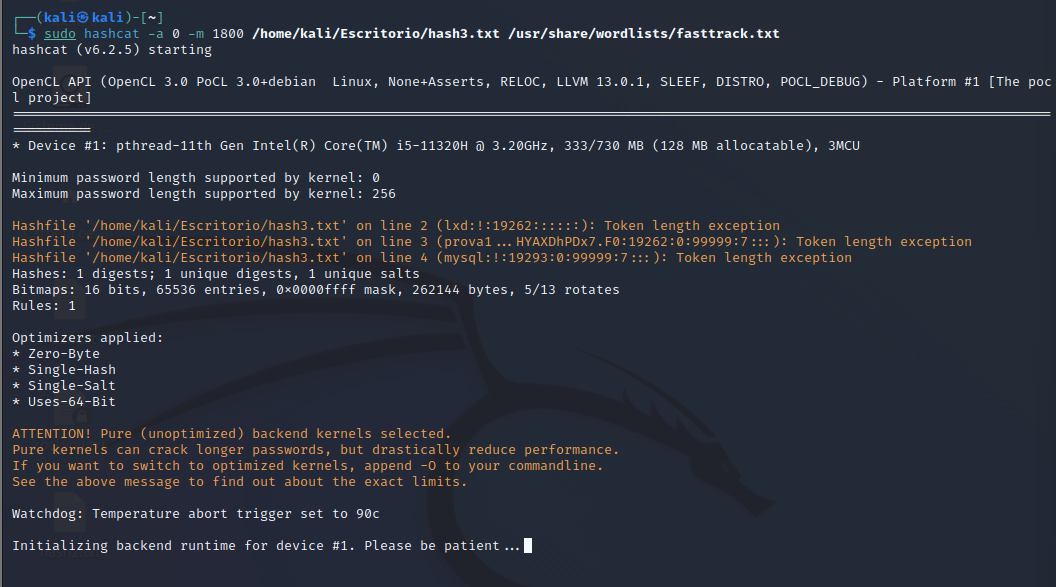
Copiarem els hash de la màquina ubuntu server a un document al escriptori.



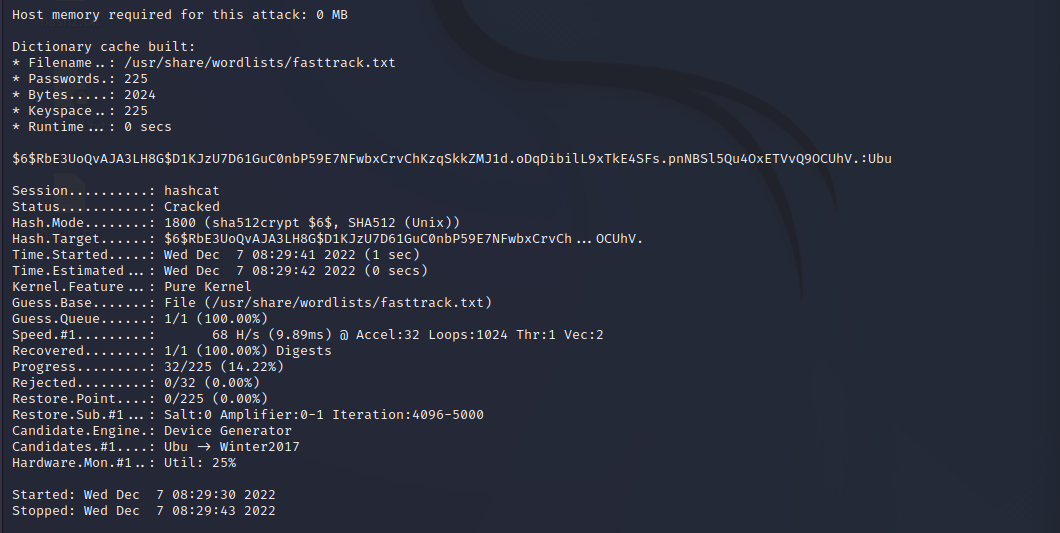


Executarem la següent comanda:

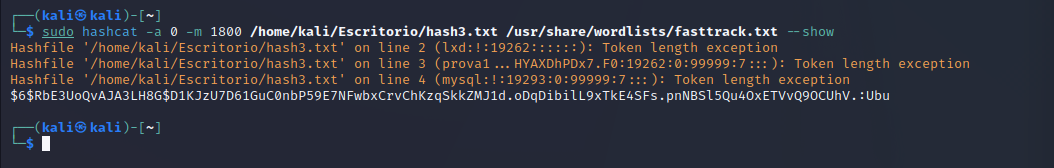
  
Ens diu que no es pot, ja que els formats dels hashes són $y$, y no hi ha hashcat per aquest format. Probarem amb el usuari inicial del Ubuntu Server:



Probarem amb aquesta comanda que es on hi ha el hash encriptat del primer usuari, que està en format $6$



Ens diu que els candidats estan entre el Ubu (la contrasenya) i Winter2017. Ens diu que el hash es cracked. Ara probarem el mateix pero posant – show:



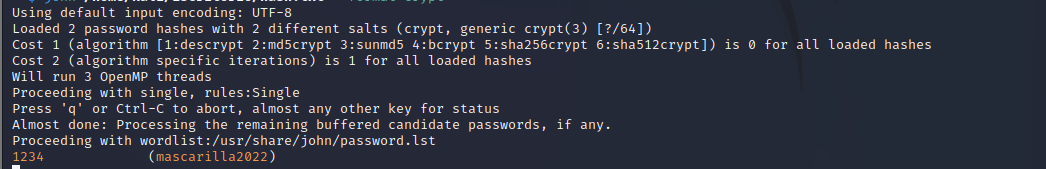
Ens ha trobat el password com podem observar

# Exercici 3 – John The Ripper

Executarem la següent comanda:

(El format crypt es perquè trobi la password a través del hash encriptat)

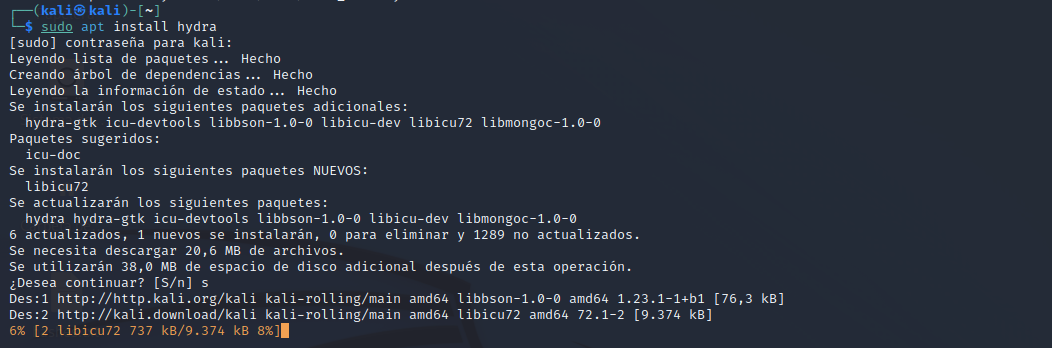




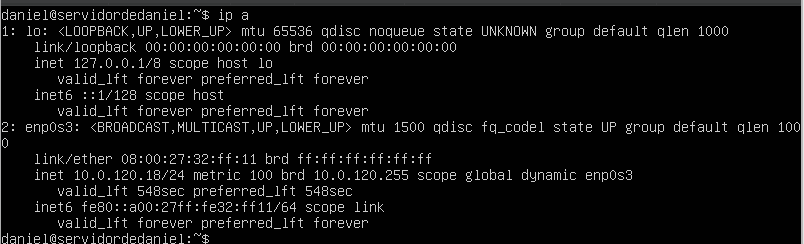
Podem observar que ens ha trobat la contrasenya del usuari creat abans en l’exercici 1.

# Exercici 4 – Hydra

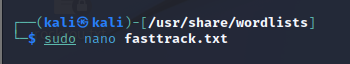
Instal·larem hydra amb la següent comanda:

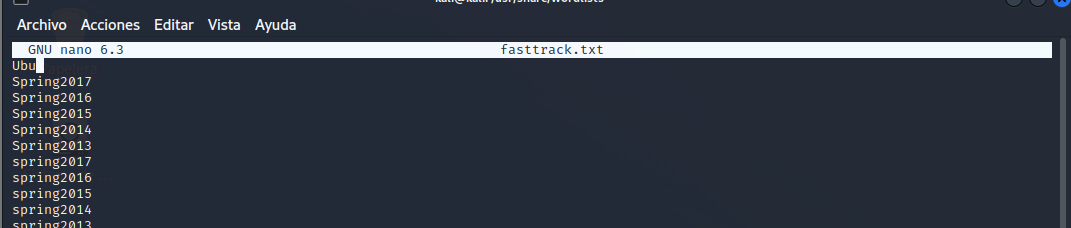


Un cop instal·lat, abans d’iniciar la comanda, haurem de veure quina ip té la màquina a la qual volem atacar:



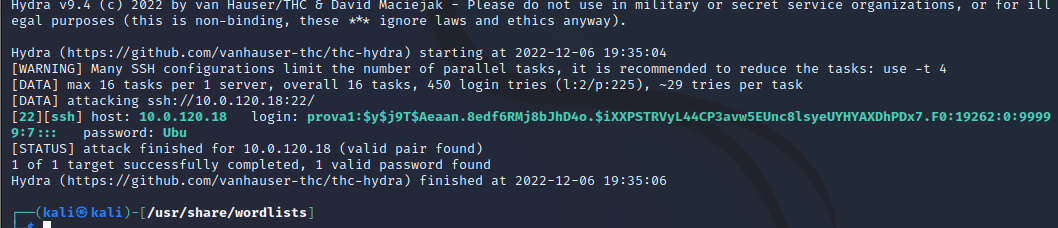
(En el meu cas, la contrasenya no estava, així que vaig modificar un arxiu de wordlists perquè trobés la contrasenya):





Un cop modificat, executarem la següent comanda:





Podem veure que ha trobat el host, amb el login, el hash de la contrasenya i per ultim la contrasenya del usuari. (Encara que no ha trobat la de l’usuari mascarilla2022)

També ho podem fer amb la següent comanda (què és amb força bruta, directament amb els noms dels usuaris en comptes dels hashes):

