

S6L3

L'obiettivo di questo esercizio è utilizzare John the Ripper, uno strumento avanzato per il cracking delle password, per decifrare gli hash MD5 presenti nella slide.

```
(kali㉿kali)-[~/Desktop]
$ john --format=raw-md5 --incremental lista.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=2
Press 'q' or Ctrl-C to abort, almost any other key for status
abc123          (?)
charley         (?)
password        (?)
letmein         (?)
4g 0:00:00:01 DONE (2024-05-15 09:43) 2.083g/s 1330Kp/s 1330Kc/s 1561KC/s letero1..letmish
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]
$ john --show --format=raw-md5 lista.txt
?:password
?:abc123
?:charley
?:letmein
?:password

5 password hashes cracked, 0 left
```

Comandi utilizzati:

john --format=raw-md5 --incremental lista.txt

Questo comando utilizza John the Ripper in modalità incrementale, specificando che gli hash sono in formato MD5 (--format=raw-md5). La modalità incrementale tenta tutte le combinazioni possibili di caratteri, rendendola molto potente ma anche molto lenta. Questa modalità è particolarmente utile quando le password non sono presenti in wordlist comuni.

john --show lista.txt

Questo comando mostra le password craccate finora. John the Ripper legge il file lista.txt e visualizza le corrispondenze trovate. Questo passaggio è utile per verificare quali password sono state decifrate con successo.