**Password Cracking Using John-The Ripper**

**┌──(kali㉿kali)-[~]**

**└─$ echo "Hello\nPooja" > abc.txt**

**┌──(kali㉿kali)-[~]**

**└─$ zip --password secret123 word.zip abc.txt**

**adding: abc.txt (stored 0%)**

**┌──(kali㉿kali)-[~]**

**└─$ zip2john word.zip > ziphash.txt**

**Created directory: /home/kali/.john**

**ver 1.0 efh 5455 efh 7875 word.zip/abc.txt PKZIP Encr: 2b chk, TS\_chk, cmplen=24, decmplen=12, crc=1DD4B43C ts=6730 cs=6730 type=0**

**┌──(kali㉿kali)-[~]**

**└─$ sudo apt install wordlists**

**wordlists is already the newest version (2023.2.0).**

**wordlists set to manually installed.**

**Summary:**

**Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 2034**

**┌──(kali㉿kali)-[~]**

**└─$ sudo gzip -d /usr/share/wordlists/rockyou.txt.gz**

**┌──(kali㉿kali)-[~]**

**└─$ john ziphash.txt --wordlist=/usr/share/wordlists/rockyou.txt**

**Using default input encoding: UTF-8**

**Loaded 1 password hash (PKZIP [32/64])**

**Will run 2 OpenMP threads**

**Press 'q' or Ctrl-C to abort, almost any other key for status**

**secret123 (word.zip/abc.txt)**

**1g 0:00:00:00 DONE (2025-04-23 13:01) 33.33g/s 682666p/s 682666c/s 682666C/s christal..michelle4**

**Use the "--show" option to display all of the cracked passwords reliably**

**Session completed.**

**┌──(kali㉿kali)-[~]**

**└─$ john --show ziphash.txt**

**word.zip/abc.txt:secret123:abc.txt:word.zip::word.zip**

**1 password hash cracked, 0 left**

**Password Cracking using Hashcat**

**┌──(kali㉿kali)-[~]**

**└─$ sudo apt install hashcat -y**

**[sudo] password for kali:**

**hashcat is already the newest version (6.2.6+ds2-1).**

**Summary:**

**Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 2123**

**┌──(kali㉿kali)-[~]**

**└─$ hashcat --version**

**v6.2.6**

**┌──(kali㉿kali)-[~]**

**└─$ hashid 5f4dcc3b5aa765d61d8327deb882cf99**

**Analyzing '5f4dcc3b5aa765d61d8327deb882cf99'**

**[+] MD2**

**[+] MD5**

**[+] MD4**

**[+] Double MD5**

**[+] LM**

**[+] RIPEMD-128**

**[+] Haval-128**

**[+] Tiger-128**

**[+] Skein-256(128)**

**[+] Skein-512(128)**

**[+] Lotus Notes/Domino 5**

**[+] Skype**

**[+] Snefru-128**

**[+] NTLM**

**[+] Domain Cached Credentials**

**[+] Domain Cached Credentials 2**

**[+] DNSSEC(NSEC3)**

**[+] RAdmin v2.x**

**┌──(kali㉿kali)-[~]**

**└─$ echo "5f4dcc3b5aa765d61d8327deb882cf99" > hash.txt**

**┌──(kali㉿kali)-[~]**

**└─$ hashcat -m 0 -a 0 hash.txt /usr/share/wordlists/rockyou.txt**

**hashcat (v6.2.6) starting**

**OpenCL API (OpenCL 3.0 PoCL 6.0+debian Linux, None+Asserts, RELOC, LLVM 17.0.6, SLEEF, DISTRO, POCL\_DEBUG) - Platform #1 [The pocl project]**

**============================================================================================================================================**

**\* Device #1: cpu-haswell-12th Gen Intel(R) Core(TM) i5-1235U, 1324/2713 MB (512 MB allocatable), 2MCU**

**Minimum password length supported by kernel: 0**

**Maximum password length supported by kernel: 256**

**Hashes: 1 digests; 1 unique digests, 1 unique salts**

**Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates**

**Rules: 1**

**Optimizers applied:**

**\* Zero-Byte**

**\* Early-Skip**

**\* Not-Salted**

**\* Not-Iterated**

**\* Single-Hash**

**\* Single-Salt**

**\* Raw-Hash**

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

**Pure kernels can crack longer passwords, but drastically reduce performance.**

**If you want to switch to optimized kernels, append -O to your commandline.**

**See the above message to find out about the exact limits.**

**Watchdog: Temperature abort trigger set to 90c**

**Host memory required for this attack: 0 MB**

**Dictionary cache built:**

**\* Filename..: /usr/share/wordlists/rockyou.txt**

**\* Passwords.: 14344392**

**\* Bytes.....: 139921507**

**\* Keyspace..: 14344385**

**\* Runtime...: 3 secs**

**5f4dcc3b5aa765d61d8327deb882cf99:password**

**Session..........: hashcat**

**Status...........: Cracked**

**Hash.Mode........: 0 (MD5)**

**Hash.Target......: 5f4dcc3b5aa765d61d8327deb882cf99**

**Time.Started.....: Wed Apr 23 13:42:51 2025 (1 sec)**

**Time.Estimated...: Wed Apr 23 13:42:52 2025 (0 secs)**

**Kernel.Feature...: Pure Kernel**

**Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)**

**Guess.Queue......: 1/1 (100.00%)**

**Speed.#1.........: 5222 H/s (0.08ms) @ Accel:256 Loops:1 Thr:1 Vec:8**

**Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)**

**Progress.........: 512/14344385 (0.00%)**

**Rejected.........: 0/512 (0.00%)**

**Restore.Point....: 0/14344385 (0.00%)**

**Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1**

**Candidate.Engine.: Device Generator**

**Candidates.#1....: 123456 -> letmein**

**Hardware.Mon.#1..: Util: 51%**

**Started: Wed Apr 23 13:42:10 2025**

**Stopped: Wed Apr 23 13:42:54 2025**

**┌──(kali㉿kali)-[~]**

**└─$ hashcat -m 0 -a 0 hash.txt /usr/share/wordlists/rockyou.txt --show**

**5f4dcc3b5aa765d61d8327deb882cf99:password**