Password-Cracking Campaign

(Ethical-hacking Lab)

Group 5

Amanda Henningsohn	Oscar Reinoso Bosch
Elin Lennartsson	Abdul Qadeer Ahmady

Table of Contents

Introduction

Organizations rely on passwords as a primary authentication factor, yet user-chosen passwords are often weak, reused, or predictable. This report documents a controlled password cracking exercise performed on synthetic data to evaluate how password strength, user behavior patterns, and hash algorithms affect resistance to offline attacks.

The findings are used to derive practical recommendations for password policy, user guidance, and the use of modern cracking tools in security assessments.

Objectives

- To evaluate how quickly weak, medium, and strong passwords can be cracked using common offline attack techniques.
- To compare crack rates across three hash algorithms (MD5, SHA-256, SHA-512).
- To identify common patterns in cracked passwords.
- Propose an updated password policy and user guidance based on empirical results.
- Experiment with LLM support for script generation, reporting, and policy drafting.

Scope and limitations

- All passwords and hashes are synthetic; no real user data was used.
- The exercise focuses on offline cracking of known hashes, not online attack scenarios.
- Time and hardware resources are limited, so “uncracked” does not mean “uncrackable,” only “not cracked within the test window.”

Test dataset and environment

This section introduces the test dataset and experimental environment. Dataset design is detailed in the following subsection.

Dataset design

- **Passwords:** 30 synthetic passwords:
    - 10 weak (short, common words, simple patterns).
    - 10 medium (slightly longer, some complexity).
    - 10 strong (longer, some complexity).

- **Hash algorithms:** MD5, SHA-256 and SHA-512
- **Hash files:** hashes_md5.txt, hashes_sha256.txt, hashes_sha512.txt, one hash per line.

Environment

• **Operating System:**	Kali GNU/Linux (kali-rolling snapshot 2023.3)
	Kernel: Linux 6.3.0-kali1-amd64 (Debian 6.3.7-1kali1)
	Architecture: x86_64
• **Tools:**	Hashcat v6.2.6, John the Ripper 1.9.0-jumbo (bleeding)
• **Hardware:**	CPU: 2 vCPUs (x86_64, KVM virtualized)
	RAM: 4 GB

Cracking methodology

This section outlines the cracking methodology employed in the experiment. The cracking strategy followed a staged approach designed to simulate realistic attacker behavior using widely available tools, wordlists, and rule sets. The goal was not exhaustive cracking, but to evaluate how different passwords strengths and hash algorithms respond to common offline attack techniques.

Hashcat Methodology

Hashcat was used as one of the primary cracking tools due to its performance, flexibility, and support for multiple attack modes. The methodology emphasized repeatability, controlled scope, and transparent documentation of each cracking session.

The following Hashcat attack modes were used:

Attack Mode	**Purpose**
-a 0 (Dictionary)	Baseline testing of weak and commonly used passwords.
-a 0 + Rules (Dictionary + Rule Attack)	Capture predictable user variations such as capitalization, appended digits, and simple symbol substitutions.
-a 1 (Combinator Attack)	To test multi-word combinations.

John the Ripper Methodology

John the Ripper (JtR) was used alongside Hashcat to provide tool diversity and cross validation of results. JtR supports multiple cracking modes and is well suited for CPU based attacks and rule driven transformations.

The following JtR attack modes were used:

Attack Mode	Purpose
--wordlist	Equivalent to Hashcat's dictionary attack; used to establish baseline crackability.
--wordlist --rules	Apply JtR's built-in and custom rules to generate common password variations.

JtR sessions were run separately for each hash type (MD5, SHA256, SHA512) to maintain clear separation of results.

Scope

Hashcat was tested using all three attack strategies (dictionary, rules, combinator), while John the ripper was tested using two attack strategies (dictionary and rules).

This allowed us to compare the crack rates, time to crack, tool performance differences, and impact of password strength against the two different password cracking tools.

Each cracking attempt was executed as a separate Hashcat session to ensure clean logging and reproducibility. **Full logs and screenshots are included in Appendix A.**

Wordlists and Rule Sets

- Primary wordlist: rockyou.txt
- Standard Hashcat and John the Ripper rule files included in Kali Linux best64.rule.
- Combinator lists: A small custom text file combinatorsymbols.txt containing digits and special characters was created and used as the second input list for combinator attacks.

Results

The following section presents the results obtained from executing multiple password-cracking attacks using Hashcat and John the Ripper across three hashing algorithms. The outcomes are summarized in a comparative table to highlight the effectiveness and performance of each attack mode.

Overview of the Results

The table below shows the performance of three attack modes (dictionary, rules, and combinator) across three hashing algorithms (MD5, SHA-256, SHA-512). Each attack mode builds on the previous one, and the “Recovered” column reflects cumulative cracked passwords.

Logging Table for Hashcat Cracking Results

Algorithm	Total Hashes	Attack Mode	Time in seconds	Success Rate (%)	Recovered	Sessions Name
MD5	30	Dictionary	5	30	9	Hashcat MD5 dictionary
SHA256	30	Dictionary	6	30	9	Hashcat 256 dictionary
SHA512	30	Dictionary	16	30	9	Hashcat 512 dictionary
MD5	30	Rules	82	43	13	Hashcat MD5 rules
SHA256	30	Rules	155	43	13	Hashcat 256 rules
SHA512	30	Rules	316	43	13	Hashcat 512 rules
MD5	30	Combinator	38	50	15	Hashcat MD5 combinator
SHA256	30	Combinator	10	43	13	Hashcat 256 combinator
SHA512	30	Combinator	67	50	15	Hashcat 512 combinator

Logging Table for John the Ripper Cracking Results

Algorithm	Total Hashes	Attack Mode	Time (s)	Success Rate (this attack	Recovered (this attack)	Sessions Name
MD5	30	Dictionary	1	33 %	10	John the Ripper MD5 wordlist
SHA256	30	Dictionary	4	27 %	9	John the Ripper SHA256 wordlists
SHA512	30	Dictionary	9	30 %	9	John the Ripper SHA512 wordlists
MD5	30	Rules	1	10 %	3	John the Ripper MD5 rules
SHA256	30	Rules	66	10 %	3	John the Ripper SHA256 rules
SHA512	30	Rules	80	10 %	3	John the Ripper SHA512 rules

- Dictionary → cracks the simplest passwords
- Rules → cracks additional mutated versions
- Combinator → cracks more complex combinations

Dictionary Attack Analysis

Across all the algorithms, the dictionary attack recovered 9-10 out of 30. This indicates that a significant portion of the passwords exist in rockyou wordlist. Dictionary attacks are effective for weak and common passwords. The hashing algorithm does not affect the success rate, only the speed.

Rule-Based Attack Analysis

The rule attack increased the total cracked passwords to 13 out of 30 (43%) for all algorithms. In the Hashcat table, it is represented as cumulative, in the John the Ripper table, it is presented per attack. The result for both is the same (3 more cracked). This shows that rule mutations successfully generated additional password variants. The increase from 9-10 to 13 demonstrates the values of rule-based attack in practical password cracking.

Combinator Attack Analysis

The combinator attack only represents the Hashcat. This attack mode produced different results depending on algorithm.

- **MD5:** 15/30 (50%)
- **SHA-256:** 13/30 (43%)
- **SHA-512:** 15/30 (50%)

This tells us that combinator attack could crack two more passwords for MD5 and SHA-512.

Algorithm Performance comparison.

MD5 was cracked the fastest, while SHA-256 and especially SHA-512 took longer. This difference reflects the computational cost of each algorithm: fast hashes like MD5 make cracking easier for attackers, whereas slower algorithms increase the time required to test each password guess. In practice, this means that slower hashing algorithms offer stronger protection because they make large-scale cracking attempts more difficult.

Conclusion and Recommended Password policy

Based on the results of password-cracking experiments, it is evident that weak and moderately complex passwords are highly vulnerable to offline attacks, even when modern hash algorithms are used. Dictionary attacks alone recovered up to one-third of all passwords, and rule-based mutations significantly increased this success rate by generating simple variations of common words. Even more combinator attacks were able to uncover passwords by combining two dictionary terms.

To mitigate these risks, the following password policy is recommended:

1. **Minimum Password Length**
   Passwords should be at least **14 characters long**. The results show that longer passwords significantly increase resistance to dictionary, rule-based, and combinator attacks.
2. **Password Composition**
   Users should be encouraged to create **passphrases** composed of multiple unrelated words rather than short passwords with predictable substitutions. Mandatory complexity rules alone (such as requiring numbers or symbols) are insufficient if passwords remain short or predictable.
3. **Avoid Predictable Patterns**
   Passwords must not contain common words, keyboard patterns, or simple transformations (e.g., “Password123!”, capitalization of the first letter, or

appending digits). These patterns were consistently exploited by rule-based attacks.

4. **Hashing and Storage**
   Insecure hash algorithms such as **MD5 must not be used** for password storage. Passwords should be stored using **modern, adaptive hashing algorithms.**
5. **Multi-Factor Authentication (MFA)**
   Where possible, **multi-factor authentication** should be enforced. MFA significantly reduces the impact of password compromise, even if an attacker successfully cracks a password hash.
6. **Password Reuse and Rotation**
   Users should be discouraged from reusing passwords across services. Password changes should be required when compromise is suspected, rather than on frequent fixed intervals that may encourage weak password choices.
7. **User Awareness and Training**
   Regular security awareness training should be provided to educate users on creating strong passwords and understanding common attack techniques such as dictionary and rule-based cracking.

Implementing these measures would substantially improve resistance to offline password-cracking attacks and reduce the likelihood of successful compromise, even in the event of password database breach.

Appendix A: Cracking Logs and Evidence

Session Name: Hashcat MD5 dictionary

Hash Type: MD5 (Hashcat mode 0)

Hash File: hashes_md5.txt

Attack Mode: Dictionary (-a 0)

Wordlist: /usr/share/wordlists/rockyou.txt

Start Time: 20251203 12:03:41

End Time: 20251203 12:03:46

Total Duration: ~5 seconds

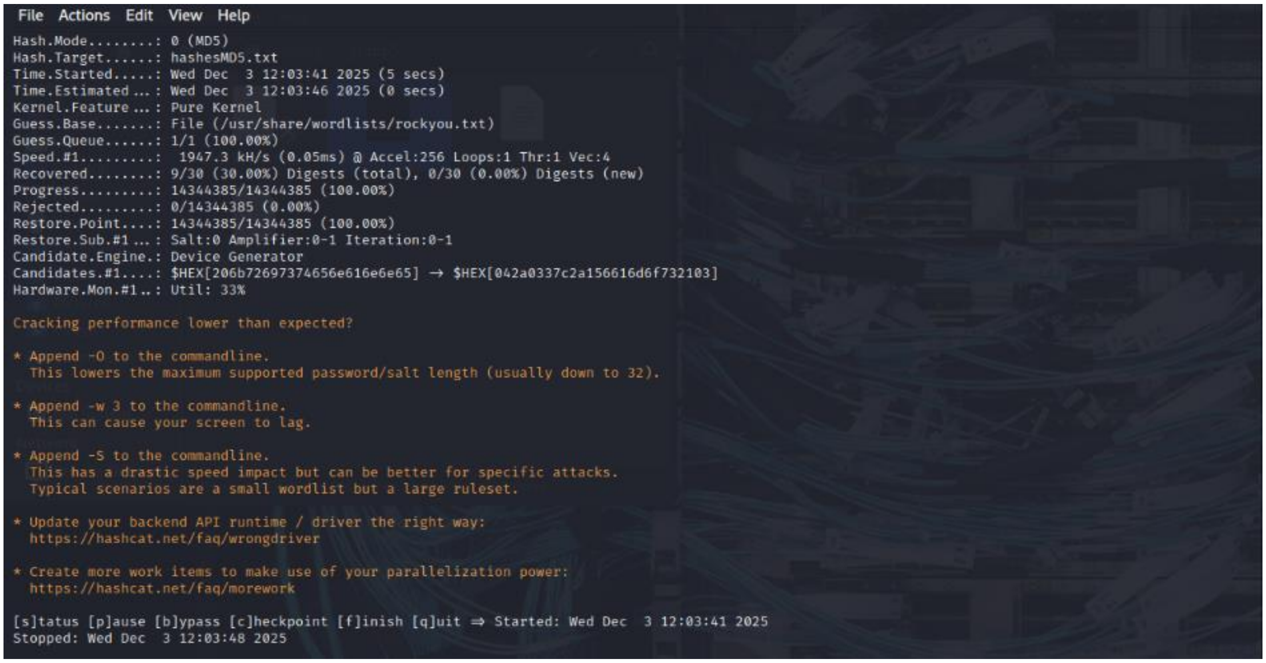
Progress: 14,344,385 candidates tested (100%)

Recovered: 9/30 hashes (30%)

Rejected: 0

Notes:

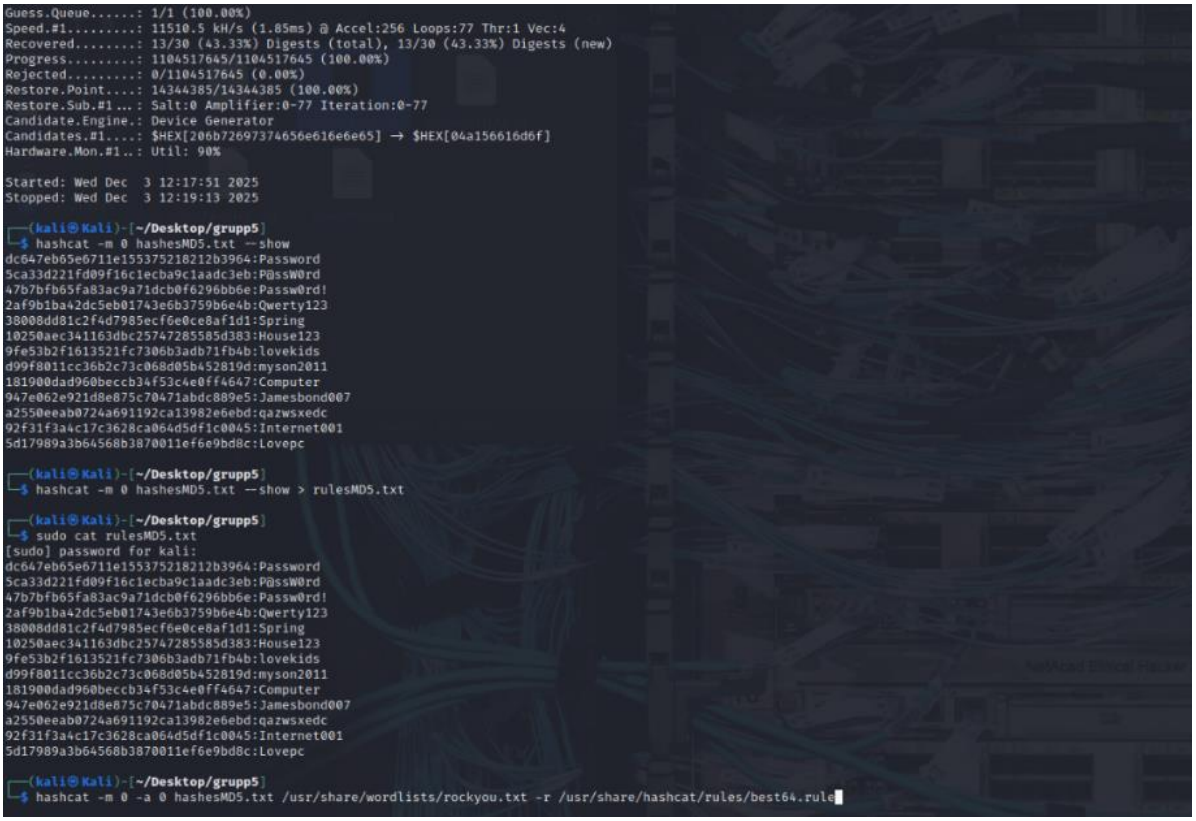
Command: hashcat -m 0 -a 0 -o crackedmd5.txt hashesMD5.txt /usr/share/wordlists/rockyou.txt



```
Hash.Mode........: 0 (MD5)
Hash.Target......: hashesMD5.txt
Time.Started.....: Wed Dec  3 12:03:41 2025 (5 secs)
Time.Estimated...: Wed Dec  3 12:03:46 2025 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:  1947.3 kH/s (0.05ms) @ Accel:256 Loops:1 Thr:1 Vec:4
Recovered........: 9/30 (30.00%) Digests (total), 0/30 (0.00%) Digests (new)
Progress.........: 14344385/14344385 (100.00%)
Rejected.........: 0/14344385 (0.00%)
Restore.Point....: 14344385/14344385 (100.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: $HEX[206b72697374656e616e6e65] → $HEX[042a0337c2a156616d6f732103]
Hardware.Mon.#1..: Util: 33%

Cracking performance lower than expected?

* Append -O to the commandline.
  This lowers the maximum supported password/salt length (usually down to 32).

* Append -w 3 to the commandline.
  This can cause your screen to lag.

* Append -S to the commandline.
  This has a drastic speed impact but can be better for specific attacks.
  Typical scenarios are a small wordlist but a large ruleset.

* Update your backend API runtime / driver the right way:
  https://hashcat.net/faq/wrongdriver

* Create more work items to make use of your parallelization power:
  https://hashcat.net/faq/morework

[s]tatus [p]ause [b]ypass [c]heckpoint [f]inish [q]uit ⇒ Started: Wed Dec  3 12:03:41 2025
Stopped: Wed Dec  3 12:03:48 2025
```

Session Name:	Hashcat MD5 rules
Hash Type:	MD5 (Hashcat mode 0)
Hash File:	hashesmd5.txt
Attack Mode:	Dictionary (-a 0)
Wordlist:	/usr/share/wordlists/rockyou.txt
Start Time:	12:17:51
End Time:	12:19:13
Total Duration:	~82 seconds
Progress:	14,344,385 candidates tested (100%)
Recovered:	13/30 hashes (43%)
Rejected:	0

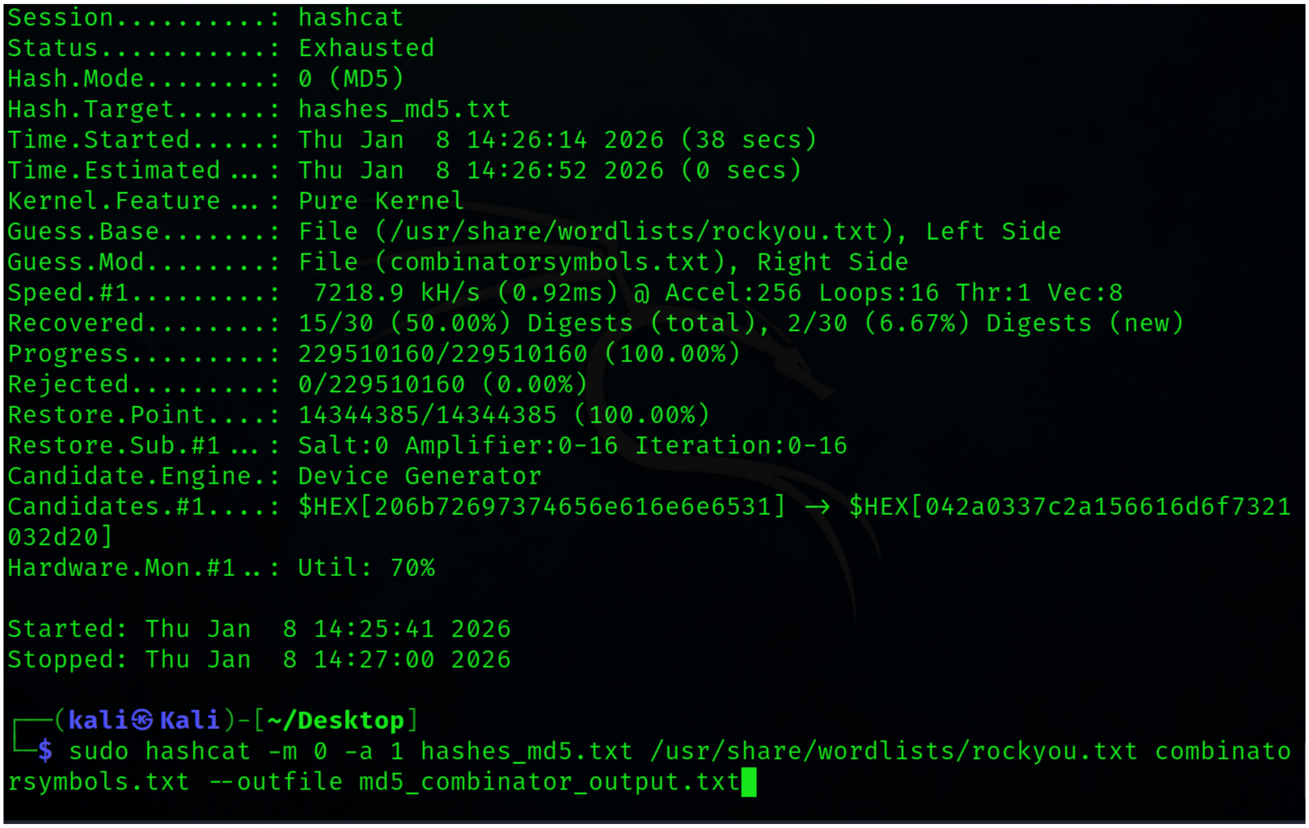
Command: Hashcat -m 0 -a 0 hashesMD5.txt /usr/share/wordlists/rockyou.txt -r /usr/share/hashcat/rules/best64.rules



```
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........: 11510.5 kH/s (1.85ms) @ Accel:256 Loops:77 Thr:1 Vec:4
Recovered........: 13/30 (43.33%) Digests (total), 13/30 (43.33%) Digests (new)
Progress.........: 1104517645/1104517645 (100.00%)
Rejected.........: 0/1104517645 (0.00%)
Restore.Point....: 14344385/14344385 (100.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-77 Iteration:0-77
Candidate.Engine.: Device Generator
Candidates.#1....: $HEX[206b72697374656e616e6e65] → $HEX[04a156616d6f]
Hardware.Mon.#1..: Util: 90%

Started: Wed Dec  3 12:17:51 2025
Stopped: Wed Dec  3 12:19:13 2025

┌──(kali㉿Kali)-[~/Desktop/grupp5]
└─$ hashcat -m 0 hashesMD5.txt --show
dc647eb65e6711e155375218212b3964:Password
5ca33d221fd09f16c1ecba9c1aadc3eb:P@ssW0rd
47b7bfb65fa83ac9a71dcb0f6296bb6e:Passw0rd!
2af9b1ba42dc5eb01743e6b3759b6e4b:Qwerty123
38008dd81c2f4d7985ecf6e0ce8af1d1:Spring
10250aec341163dbc25747285585d383:House123
9fe53b2f1613521fc7306b3adb71fb4b:lovekids
d99f8011cc36b2c73c068d05b452819d:myson2011
181900dad960beccb34f53c4e0ff4647:Computer
947e062e921d8e875c70471abdc889e5:Jamesbond007
a2550eeab0724a691192ca13982e6ebd:qazwsxedc
92f31f3a4c17c3628ca064d5df1c0045:Internet001
5d17989a3b64568b3870011ef6e9bd8c:Lovepc

┌──(kali㉿Kali)-[~/Desktop/grupp5]
└─$ hashcat -m 0 hashesMD5.txt --show > rulesMD5.txt

┌──(kali㉿Kali)-[~/Desktop/grupp5]
└─$ sudo cat rulesMD5.txt
[sudo] password for kali:
dc647eb65e6711e155375218212b3964:Password
5ca33d221fd09f16c1ecba9c1aadc3eb:P@ssW0rd
47b7bfb65fa83ac9a71dcb0f6296bb6e:Passw0rd!
2af9b1ba42dc5eb01743e6b3759b6e4b:Qwerty123
38008dd81c2f4d7985ecf6e0ce8af1d1:Spring
10250aec341163dbc25747285585d383:House123
9fe53b2f1613521fc7306b3adb71fb4b:lovekids
d99f8011cc36b2c73c068d05b452819d:myson2011
181900dad960beccb34f53c4e0ff4647:Computer
947e062e921d8e875c70471abdc889e5:Jamesbond007
a2550eeab0724a691192ca13982e6ebd:qazwsxedc
92f31f3a4c17c3628ca064d5df1c0045:Internet001
5d17989a3b64568b3870011ef6e9bd8c:Lovepc

┌──(kali㉿Kali)-[~/Desktop/grupp5]
└─$ hashcat -m 0 -a 0 hashesMD5.txt /usr/share/wordlists/rockyou.txt -r /usr/share/hashcat/rules/best64.rule
```

Session Name:	Hashcat MD5 combinator
Hash Type:	MD5 (Hashcat mode 0)
Hash File:	combinatorMD5.txt
Attack Mode:	Combinator (-a 1)
Wordlist:	/usr/share/wordlists/rockyou.txt
Start Time:	2025-01-08 14:26:14
End Time:	2025-01-08 14:26:52
Total Duration:	~38 seconds
Progress:	229510160 (100%)
Recovered:	15/30 hashes (50%)
Rejected:	0

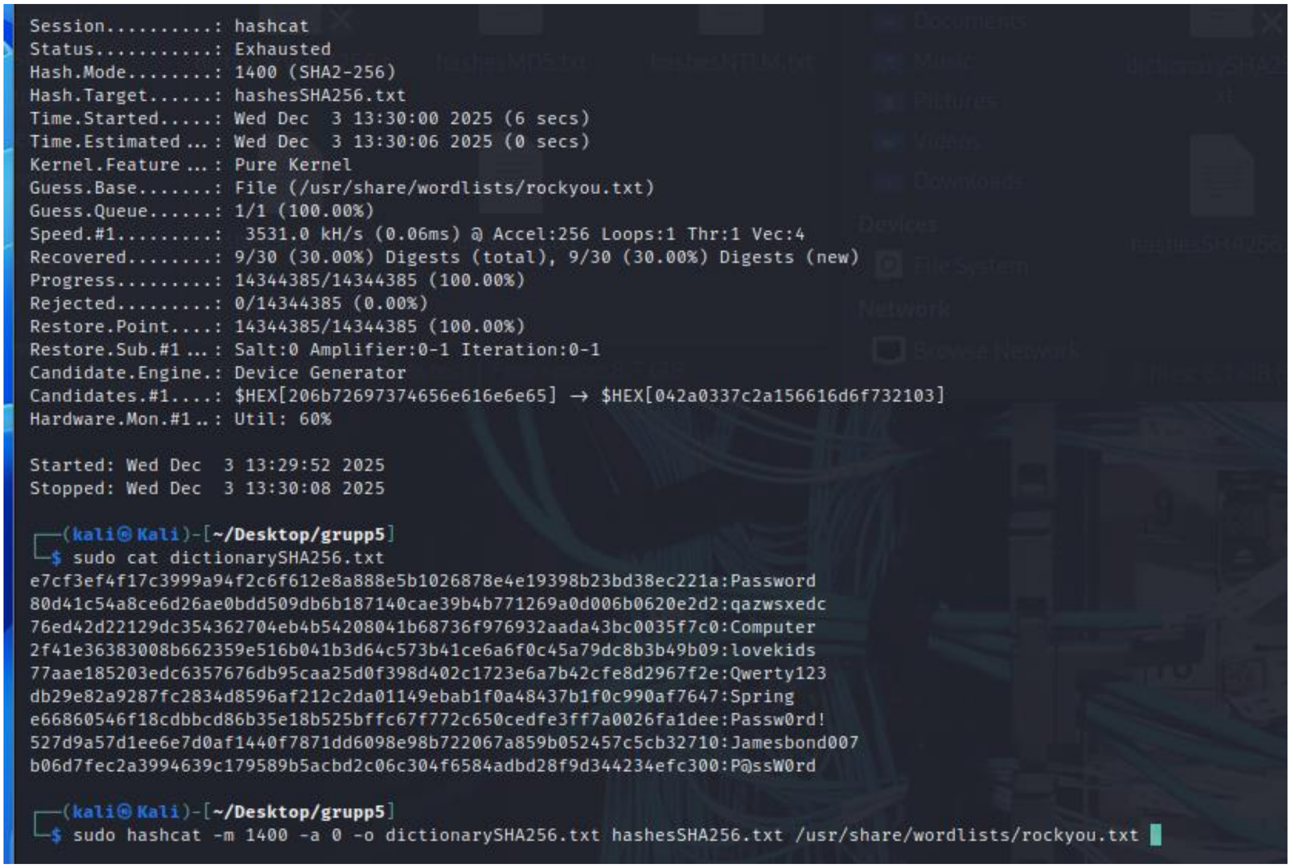
Command: hashcat -m 0 -a 1 hashes_md5.txt /usr/share/wordlists/rockyou.txt combinatorsymbols.txt --outfile md5_combinator_output.txt



```
Session..........: hashcat
Status...........: Exhausted
Hash.Mode........: 0 (MD5)
Hash.Target......: hashes_md5.txt
Time.Started.....: Thu Jan  8 14:26:14 2026 (38 secs)
Time.Estimated ...: Thu Jan  8 14:26:52 2026 (0 secs)
Kernel.Feature ...: Pure Kernel
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt), Left Side
Guess.Mod........: File (combinatorsymbols.txt), Right Side
Speed.#1.........:  7218.9 kH/s (0.92ms) @ Accel:256 Loops:16 Thr:1 Vec:8
Recovered........: 15/30 (50.00%) Digests (total), 2/30 (6.67%) Digests (new)
Progress.........: 229510160/229510160 (100.00%)
Rejected.........: 0/229510160 (0.00%)
Restore.Point....: 14344385/14344385 (100.00%)
Restore.Sub.#1 ...: Salt:0 Amplifier:0-16 Iteration:0-16
Candidate.Engine.: Device Generator
Candidates.#1....: $HEX[206b72697374656e616e6e6531] → $HEX[042a0337c2a156616d6f7321
032d20]
Hardware.Mon.#1 ..: Util: 70%

Started: Thu Jan  8 14:25:41 2026
Stopped: Thu Jan  8 14:27:00 2026

┌──(kali㉿Kali)-[~/Desktop]
└─$ sudo hashcat -m 0 -a 1 hashes_md5.txt /usr/share/wordlists/rockyou.txt combinato
rsymbols.txt --outfile md5_combinator_output.txt
```

Session Name:	Hashcat SHA256 dictionary
Hash Type:	SHA256 (hashcat mode 1400)
Hash File:	hashesSHA256.txt
Attack Mode:	Dictionary (-a 0)
Wordlist:	/usr/share/wordlists/rockyou.txt
Start Time:	13:30:00
End Time:	13:30:06
Total Duration:	6 seconds
Progress:	14344385 (100.00%)
Recovered:	9/30 (30.00%)
Rejected:	0

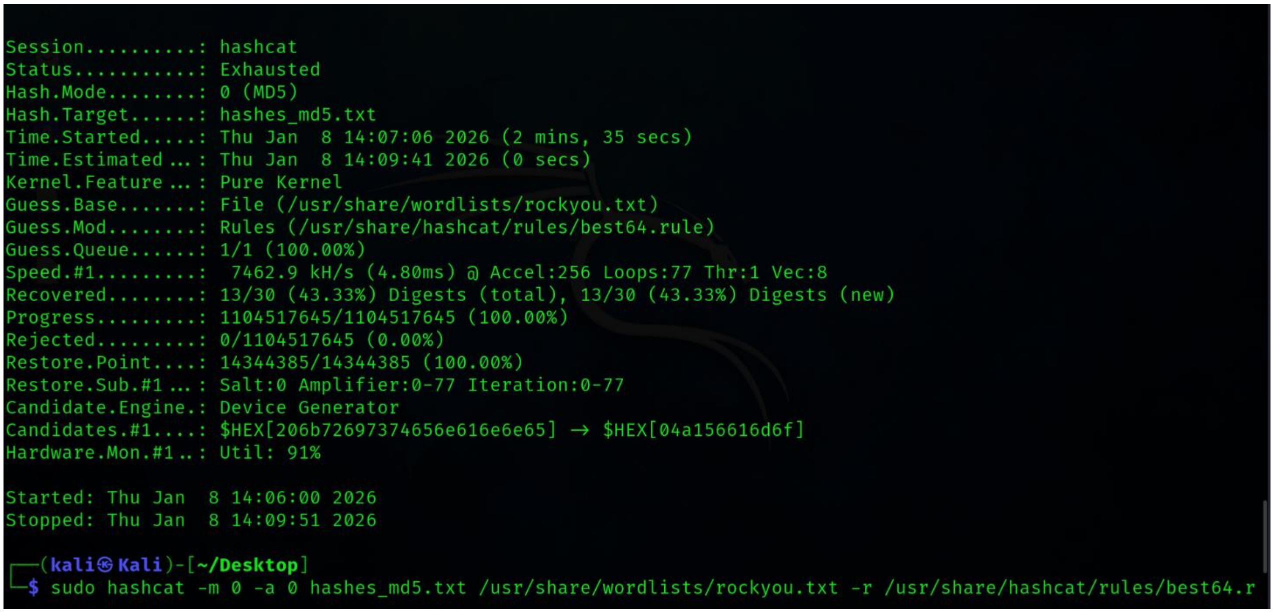
Command: sudo hashcat -m 1400 -a 0 -o dictionarySHA256.txt hashesSHA256.txt /usr/share/wordlists/rockyou.txt



```
Session..........: hashcat
Status...........: Exhausted
Hash.Mode........: 1400 (SHA2-256)
Hash.Target......: hashesSHA256.txt
Time.Started.....: Wed Dec  3 13:30:00 2025 (6 secs)
Time.Estimated...: Wed Dec  3 13:30:06 2025 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:  3531.0 kH/s (0.06ms) @ Accel:256 Loops:1 Thr:1 Vec:4
Recovered........: 9/30 (30.00%) Digests (total), 9/30 (30.00%) Digests (new)
Progress.........: 14344385/14344385 (100.00%)
Rejected.........: 0/14344385 (0.00%)
Restore.Point....: 14344385/14344385 (100.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: $HEX[206b72697374656e616e6e65] → $HEX[042a0337c2a156616d6f732103]
Hardware.Mon.#1..: Util: 60%

Started: Wed Dec  3 13:29:52 2025
Stopped: Wed Dec  3 13:30:08 2025

┌──(kali㉿Kali)-[~/Desktop/grupp5]
└─$ sudo cat dictionarySHA256.txt
e7cf3ef4f17c3999a94f2c6f612e8a888e5b1026878e4e19398b23bd38ec221a:Password
80d41c54a8ce6d26ae0bdd509db6b187140cae39b4b771269a0d006b0620e2d2:qazwsxedc
76ed42d22129dc354362704eb4b54208041b68736f976932aada43bc0035f7c0:Computer
2f41e36383008b662359e516b041b3d64c573b41ce6a6f0c45a79dc8b3b49b09:lovekids
77aae185203edc6357676db95caa25d0f398d402c1723e6a7b42cfe8d2967f2e:Qwerty123
db29e82a9287fc2834d8596af212c2da01149ebab1f0a48437b1f0c990af7647:Spring
e66860546f18cdbbcd86b35e18b525bffc67f772c650cedfe3ff7a0026fa1dee:Passw0rd!
527d9a57d1ee6e7d0af1440f7871dd6098e98b722067a859b052457c5cb32710:Jamesbond007
b06d7fec2a3994639c179589b5acbd2c06c304f6584adbd28f9d344234efc300:P@ssW0rd

┌──(kali㉿Kali)-[~/Desktop/grupp5]
└─$ sudo hashcat -m 1400 -a 0 -o dictionarySHA256.txt hashesSHA256.txt /usr/share/wordlists/rockyou.txt
```

Session Name:	Hashcat SHA256_rule
Hash Type:	SHA256 (Hashcat mode 1400)
Hash File:	hashes_sha256.txt
Attack Mode:	Dictionary (-a 0)
Wordlist:	/usr/share/wordlists/rockyou.txt
Start Time:	2026-01-08 14:07:06
End Time:	2026-01-08 14:09:41
Total Duration:	~2 min and 35 seconds
Progress:	1104517645 candidates tested (100%)
Recovered:	13/30 hashes (43%)
Rejected:	0

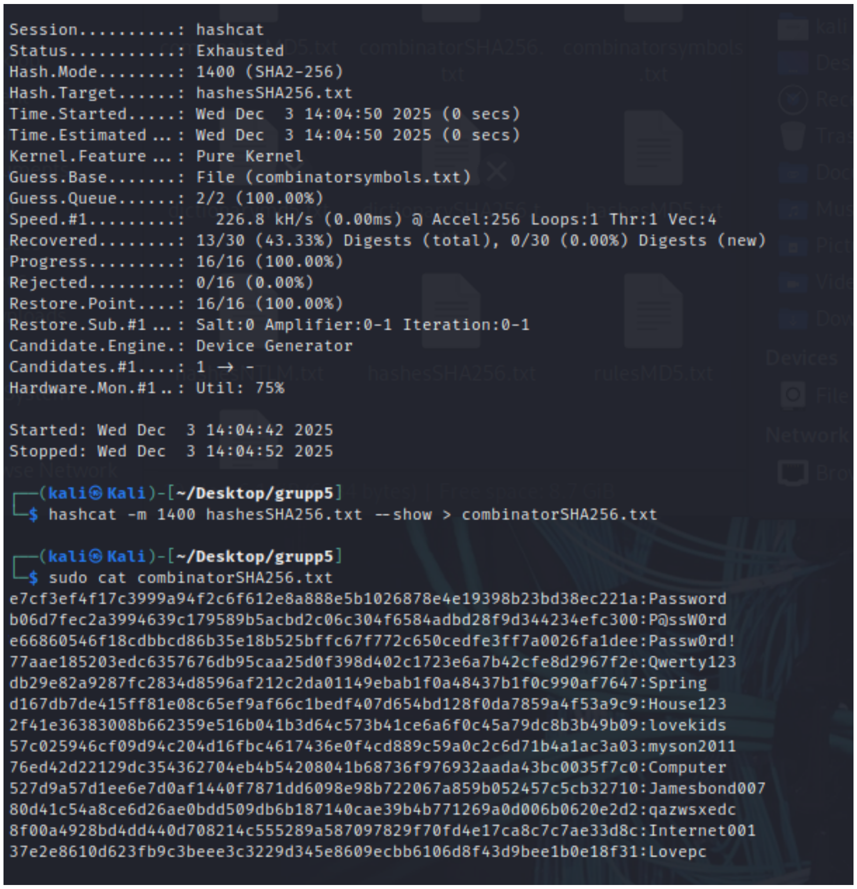
Command: sudo hashcat -m 0 -a 0 hashes_md5.txt /usr/share/wordlists/rockyou.txt -r /usr/share/hashcat/rules/best64.rule



```
Session..........: hashcat
Status...........: Exhausted
Hash.Mode........: 0 (MD5)
Hash.Target......: hashes_md5.txt
Time.Started.....: Thu Jan  8 14:07:06 2026 (2 mins, 35 secs)
Time.Estimated ...: Thu Jan  8 14:09:41 2026 (0 secs)
Kernel.Feature ...: Pure Kernel
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Mod........: Rules (/usr/share/hashcat/rules/best64.rule)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:  7462.9 kH/s (4.80ms) @ Accel:256 Loops:77 Thr:1 Vec:8
Recovered........: 13/30 (43.33%) Digests (total), 13/30 (43.33%) Digests (new)
Progress.........: 1104517645/1104517645 (100.00%)
Rejected.........: 0/1104517645 (0.00%)
Restore.Point....: 14344385/14344385 (100.00%)
Restore.Sub.#1 ...: Salt:0 Amplifier:0-77 Iteration:0-77
Candidate.Engine.: Device Generator
Candidates.#1....: $HEX[206b72697374656e616e6e65] → $HEX[04a156616d6f]
Hardware.Mon.#1..: Util: 91%

Started: Thu Jan  8 14:06:00 2026
Stopped: Thu Jan  8 14:09:51 2026

┌──(kali㉿Kali)-[~/Desktop]
└─$ sudo hashcat -m 0 -a 0 hashes_md5.txt /usr/share/wordlists/rockyou.txt -r /usr/share/hashcat/rules/best64.r
```

Session Name:	Hashcat SHA256 combinator
Hash Type:	SHA-256 (Hashcat mode 1400)
Hash File:	hashes256.txt
Attack Mode:	Combinator (a -1)
Wordlist:	Combinatorsymbols.txt
Start Time:	2025-12-03 14:04:42
End Time:	2025-12-03 14:04:52
Total Duration:	~ 10 seconds
Progress:	16/16 (100%)
Recovered:	13/30 hashes (30%)
Rejected:	0

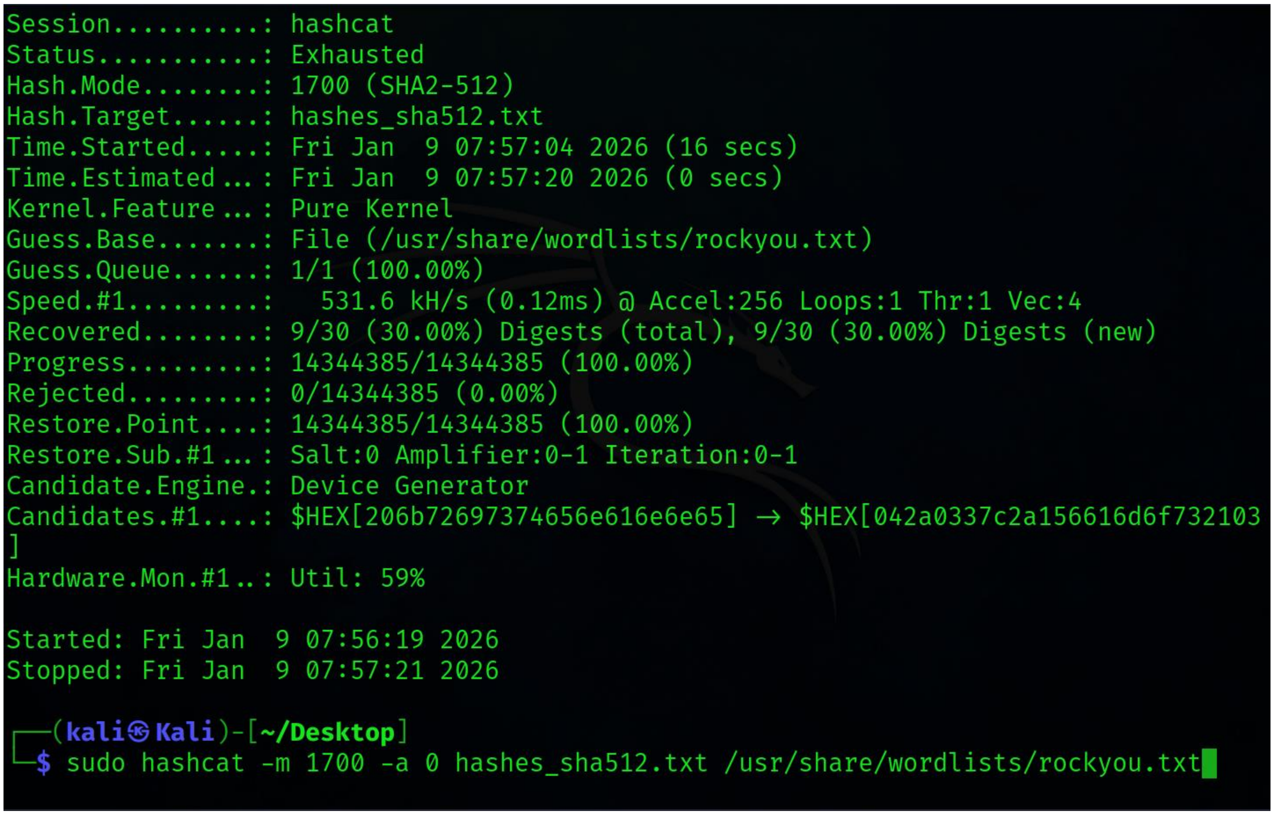
Command: sudo hashcat -m 1400 -a 1 hashesSHA256.txt combinatorsymbols.txt



```
Session..........: hashcat
Status...........: Exhausted
Hash.Mode........: 1400 (SHA2-256)
Hash.Target......: hashesSHA256.txt
Time.Started.....: Wed Dec  3 14:04:50 2025 (0 secs)
Time.Estimated ...: Wed Dec  3 14:04:50 2025 (0 secs)
Kernel.Feature ...: Pure Kernel
Guess.Base.......: File (combinatorsymbols.txt)
Guess.Queue......: 2/2 (100.00%)
Speed.#1.........:   226.8 kH/s (0.00ms) @ Accel:256 Loops:1 Thr:1 Vec:4
Recovered........: 13/30 (43.33%) Digests (total), 0/30 (0.00%) Digests (new)
Progress.........: 16/16 (100.00%)
Rejected.........: 0/16 (0.00%)
Restore.Point....: 16/16 (100.00%)
Restore.Sub.#1 ...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: 1 → -
Hardware.Mon.#1 ..: Util: 75%

Started: Wed Dec  3 14:04:42 2025
Stopped: Wed Dec  3 14:04:52 2025

┌──(kali㉿Kali)-[~/Desktop/grupp5]
└─$ hashcat -m 1400 hashesSHA256.txt --show > combinatorSHA256.txt

┌──(kali㉿Kali)-[~/Desktop/grupp5]
└─$ sudo cat combinatorSHA256.txt
e7cf3ef4f17c3999a94f2c6f612e8a888e5b1026878e4e19398b23bd38ec221a:Password
b06d7fec2a3994639c179589b5acbd2c06c304f6584adbd28f9d344234efc300:P@ssW0rd
e66860546f18cdbbcd86b35e18b525bffc67f772c650cedfe3ff7a0026fa1dee:Passw0rd!
77aae185203edc6357676db95caa25d0f398d402c1723e6a7b42cfe8d2967f2e:Qwerty123
db29e82a9287fc2834d8596af212c2da01149ebab1f0a48437b1f0c990af7647:Spring
d167db7de415ff81e08c65ef9af66c1bedf407d654bd128f0da7859a4f53a9c9:House123
2f41e36383008b662359e516b041b3d64c573b41ce6a6f0c45a79dc8b3b49b09:lovekids
57c025946cf09d94c204d16fbc4617436e0f4cd889c59a0c2c6d71b4a1ac3a03:myson2011
76ed42d22129dc354362704eb4b54208041b68736f976932aada43bc0035f7c0:Computer
527d9a57d1ee6e7d0af1440f7871dd6098e98b722067a859b052457c5cb32710:Jamesbond007
80d41c54a8ce6d26ae0bdd509db6b187140cae39b4b771269a0d006b0620e2d2:qazwsxedc
8f00a4928bd4dd440d708214c555289a587097829f70fd4e17ca8c7c7ae33d8c:Internet001
37e2e8610d623fb9c3beee3c3229d345e8609ecbb6106d8f43d9bee1b0e18f31:Lovepc
```

Session Name:	Hashcat SHA512 dictionary
Hash Type:	SHA-512 (Hashcat mode 1700)
Hash File:	hashes_sha512.txt
Attack Mode:	Dictionary (-a 0)
Wordlist:	/usr/share/wordlists/rockyou.txt
Start Time:	2026-01-09 07:57:04
End Time:	2026-01-09 07:57:20
Total Duration:	~16 seconds
Progress:	14,344,385 candidates tested (100%)
Recovered:	9/30 hashes (30%)
Rejected:	0

Command: sudo hashcat -m 1700 -a 0 hashes_sha512.txt /usr/share/wordlists/rockyou.txt



```
Session..........: hashcat
Status...........: Exhausted
Hash.Mode........: 1700 (SHA2-512)
Hash.Target......: hashes_sha512.txt
Time.Started.....: Fri Jan  9 07:57:04 2026 (16 secs)
Time.Estimated...: Fri Jan  9 07:57:20 2026 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:   531.6 kH/s (0.12ms) @ Accel:256 Loops:1 Thr:1 Vec:4
Recovered........: 9/30 (30.00%) Digests (total), 9/30 (30.00%) Digests (new)
Progress.........: 14344385/14344385 (100.00%)
Rejected.........: 0/14344385 (0.00%)
Restore.Point....: 14344385/14344385 (100.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: $HEX[206b72697374656e616e6e65] → $HEX[042a0337c2a156616d6f732103
]
Hardware.Mon.#1..: Util: 59%

Started: Fri Jan  9 07:56:19 2026
Stopped: Fri Jan  9 07:57:21 2026

┌──(kali㉿Kali)-[~/Desktop]
└─$ sudo hashcat -m 1700 -a 0 hashes_sha512.txt /usr/share/wordlists/rockyou.txt
```

Session Name: Hashcat SHA512 rules

Hash Type: SHA-512(Hashcat mode 1700)

Hash File: hashes_sha512.txt

Attack Mode: Dictionary (-a 0 with best64.rule)

Wordlist: /usr/share/wordlists/rockyou.txt

Start Time: 2026-01-09 08:01:13

End Time: 2026-01-09 08:06:29

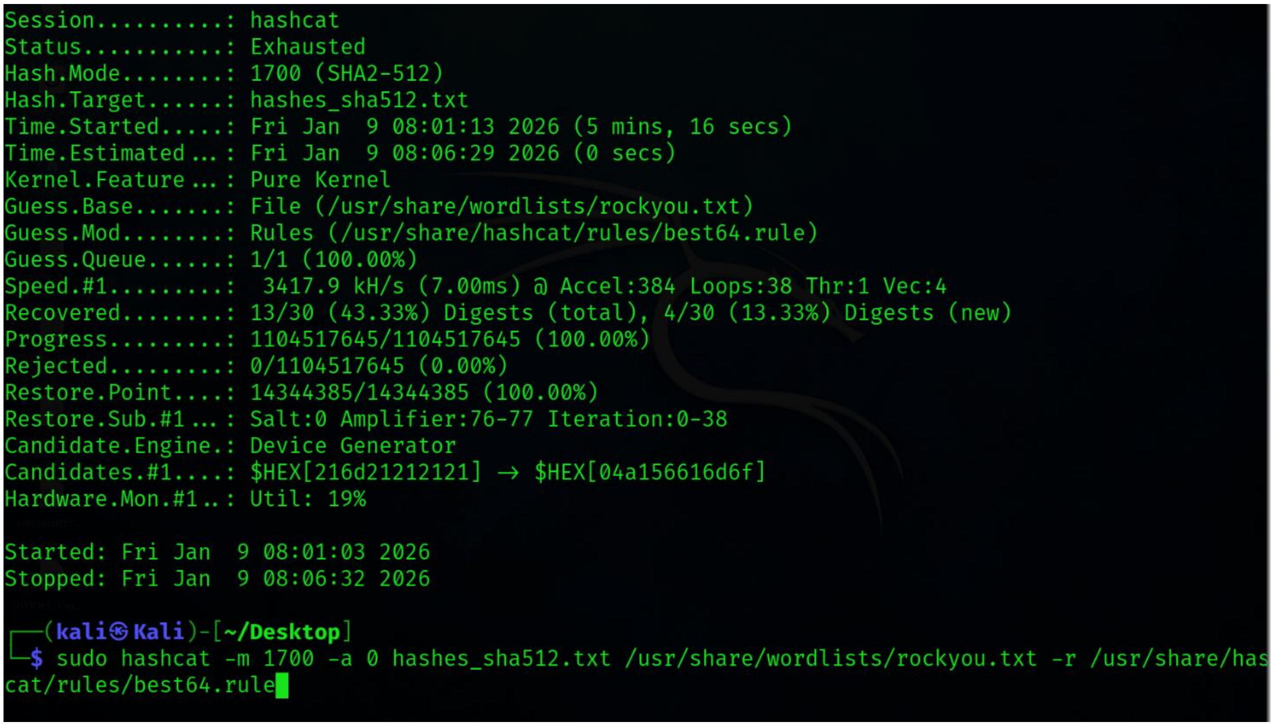
Total Duration: ~5 min 16 seconds

Progress: 110,451,764 candidates tested (100%)

Recovered: 13/30 hashes (43.33%)

Rejected: 0

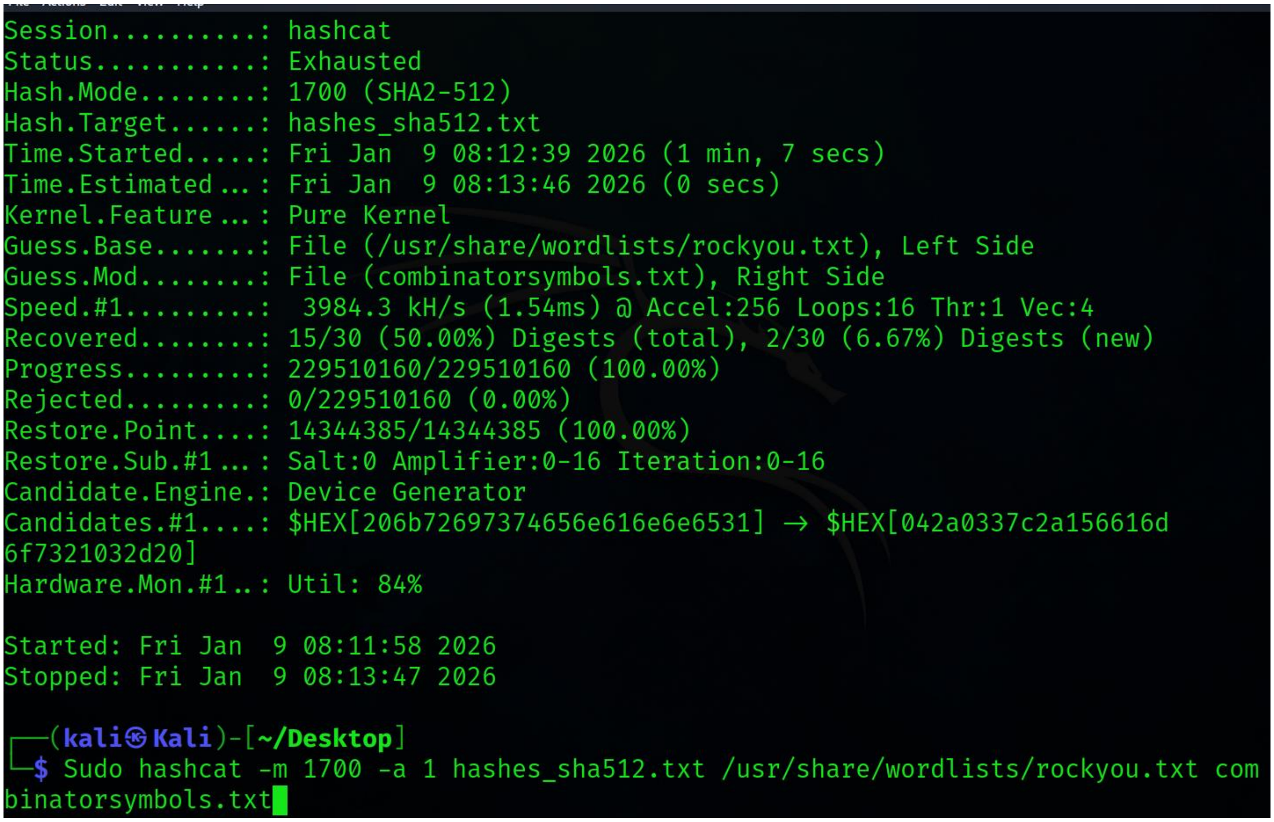
Command: sudo hashcat -m 1700 -a 0 hashes_sha512.txt /usr/share/wordlists/rockyou.txt -r /usr/share/hashcat/rules/best64.rule



```
Session..........: hashcat
Status...........: Exhausted
Hash.Mode........: 1700 (SHA2-512)
Hash.Target......: hashes_sha512.txt
Time.Started.....: Fri Jan  9 08:01:13 2026 (5 mins, 16 secs)
Time.Estimated...: Fri Jan  9 08:06:29 2026 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Mod........: Rules (/usr/share/hashcat/rules/best64.rule)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:  3417.9 kH/s (7.00ms) @ Accel:384 Loops:38 Thr:1 Vec:4
Recovered........: 13/30 (43.33%) Digests (total), 4/30 (13.33%) Digests (new)
Progress.........: 1104517645/1104517645 (100.00%)
Rejected.........: 0/1104517645 (0.00%)
Restore.Point....: 14344385/14344385 (100.00%)
Restore.Sub.#1...: Salt:0 Amplifier:76-77 Iteration:0-38
Candidate.Engine.: Device Generator
Candidates.#1....: $HEX[216d21212121] → $HEX[04a156616d6f]
Hardware.Mon.#1..: Util: 19%

Started: Fri Jan  9 08:01:03 2026
Stopped: Fri Jan  9 08:06:32 2026

┌──(kali㉿Kali)-[~/Desktop]
└─$ sudo hashcat -m 1700 -a 0 hashes_sha512.txt /usr/share/wordlists/rockyou.txt -r /usr/share/has
cat/rules/best64.rule
```

Session Name:	Hashcat SHA512 combinator
Hash Type:	SHA512 (Hashcat mode 1700)
Hash File:	hashes_sha512.txt
Attack Mode:	Combinator (-a 1)
Wordlist:	/usr/share/wordlists/rockyou.txt
Start Time:	2026-01-09 08:12:39
End Time:	2026-01-09 08:13:46
Total Duration:	~67 seconds
Progress:	229510160 (100%)
Recovered:	15/30 hashes (50%)
Rejected:	0

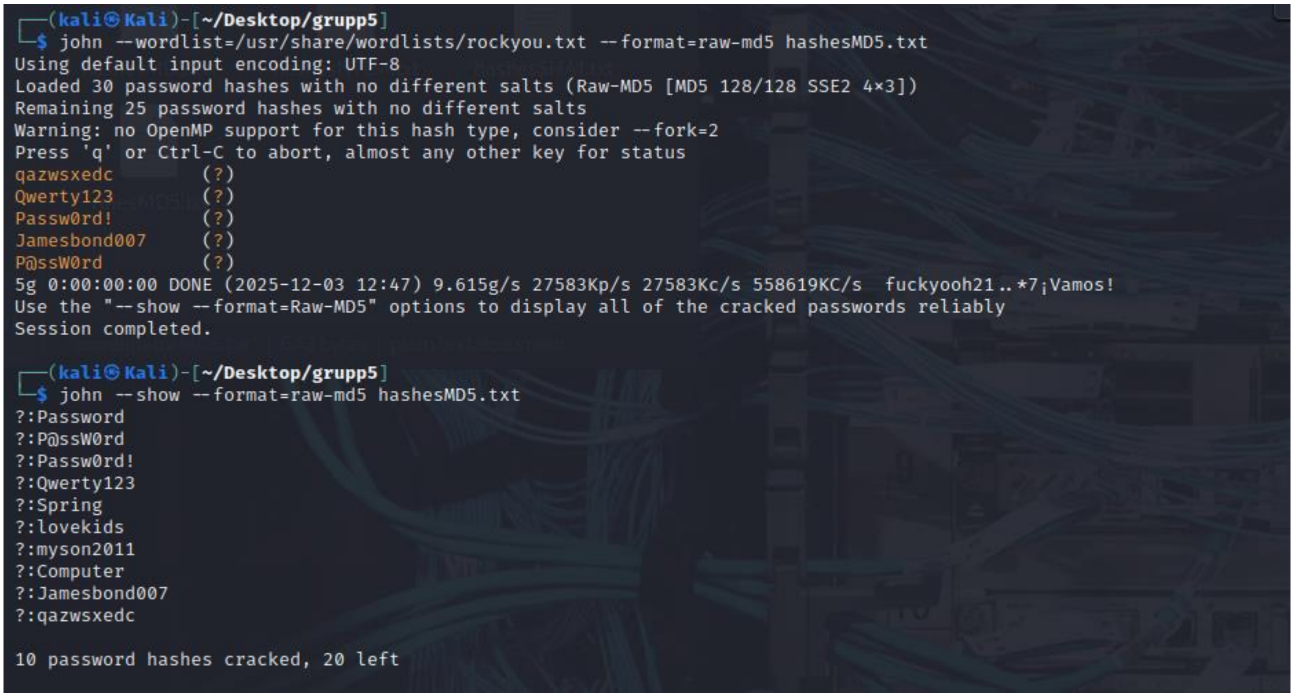
Command: sudo hashcat -m 1700 -a 1 hashes_sha512.txt /usr/share/wordlists/rockyou.txt combinatorsymbols.txt



```
Session..........: hashcat
Status...........: Exhausted
Hash.Mode........: 1700 (SHA2-512)
Hash.Target......: hashes_sha512.txt
Time.Started.....: Fri Jan  9 08:12:39 2026 (1 min, 7 secs)
Time.Estimated...: Fri Jan  9 08:13:46 2026 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt), Left Side
Guess.Mod........: File (combinatorsymbols.txt), Right Side
Speed.#1.........:  3984.3 kH/s (1.54ms) @ Accel:256 Loops:16 Thr:1 Vec:4
Recovered........: 15/30 (50.00%) Digests (total), 2/30 (6.67%) Digests (new)
Progress.........: 229510160/229510160 (100.00%)
Rejected.........: 0/229510160 (0.00%)
Restore.Point....: 14344385/14344385 (100.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-16 Iteration:0-16
Candidate.Engine.: Device Generator
Candidates.#1....: $HEX[206b72697374656e616e6e6531] -> $HEX[042a0337c2a156616d
6f7321032d20]
Hardware.Mon.#1..: Util: 84%

Started: Fri Jan  9 08:11:58 2026
Stopped: Fri Jan  9 08:13:47 2026

┌──(kali㉿Kali)-[~/Desktop]
└─$ Sudo hashcat -m 1700 -a 1 hashes_sha512.txt /usr/share/wordlists/rockyou.txt com
binatorsymbols.txt
```

Session Name:	John the Ripper MD5 wordlist
Hash Type:	Raw-MD5 (Hashcat mode 0)
Hash File:	hashesMD5.txt
Attack Mode:	Wordlist (--wordlist)
Wordlist:	/usr/share/wordlists/rockyou.txt
Start Time:	20251203 12:47:00
End Time:	20251203 12:47:00
Total Duration:	>1 second (instant completion)
Recovered:	10/30 hashes (33%)

Command: john --wordlists=/usr/share/wordlists/rockyou.txt –format=raw-md5 hashesMD5.txt



```
┌──(kali㉿Kali)-[~/Desktop/grupp5]
└─$ john --wordlist=/usr/share/wordlists/rockyou.txt --format=raw-md5 hashesMD5.txt
Using default input encoding: UTF-8
Loaded 30 password hashes with no different salts (Raw-MD5 [MD5 128/128 SSE2 4×3])
Remaining 25 password hashes with no different salts
Warning: no OpenMP support for this hash type, consider --fork=2
Press 'q' or Ctrl-C to abort, almost any other key for status
qazwsxedc        (?)
Qwerty123        (?)
Passw0rd!        (?)
Jamesbond007     (?)
P@ssW0rd         (?)
5g 0:00:00:00 DONE (2025-12-03 12:47) 9.615g/s 27583Kp/s 27583Kc/s 558619KC/s  fuckyooh21..*7¡Vamos!
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed.

┌──(kali㉿Kali)-[~/Desktop/grupp5]
└─$ john --show --format=raw-md5 hashesMD5.txt
?:Password
?:P@ssW0rd
?:Passw0rd!
?:Qwerty123
?:Spring
?:lovekids
?:myson2011
?:Computer
?:Jamesbond007
?:qazwsxedc

10 password hashes cracked, 20 left
```

Session Name: John the Ripper MD5 Rules

Hash Type: Raw-MD5 (Hashcat mode 0)

Hash File: hashesMD5.txt

Attack Mode: Wordlist (--wordlist)

Wordlist: /usr/share/wordlists/rockyou.txt

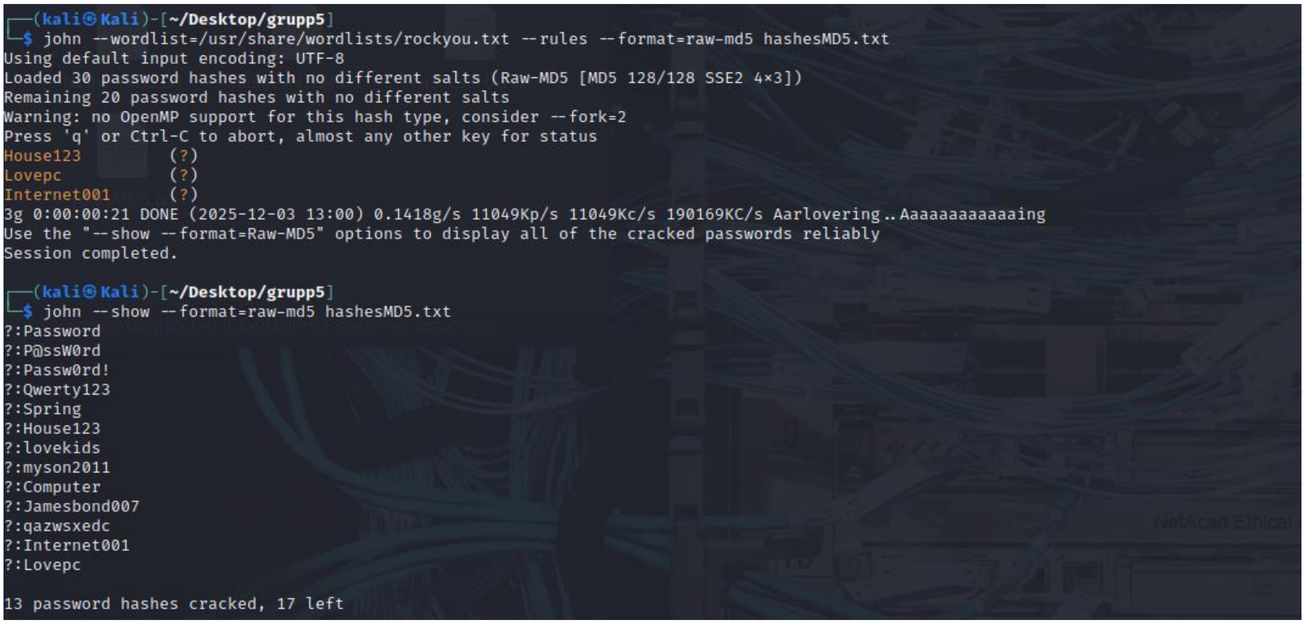
Start Time: 20251203 13:00:00

End Time: 20251203 13:00:21

Total Duration: >1 second (instant completion)

Recovered: 3/30 hashes (10%)

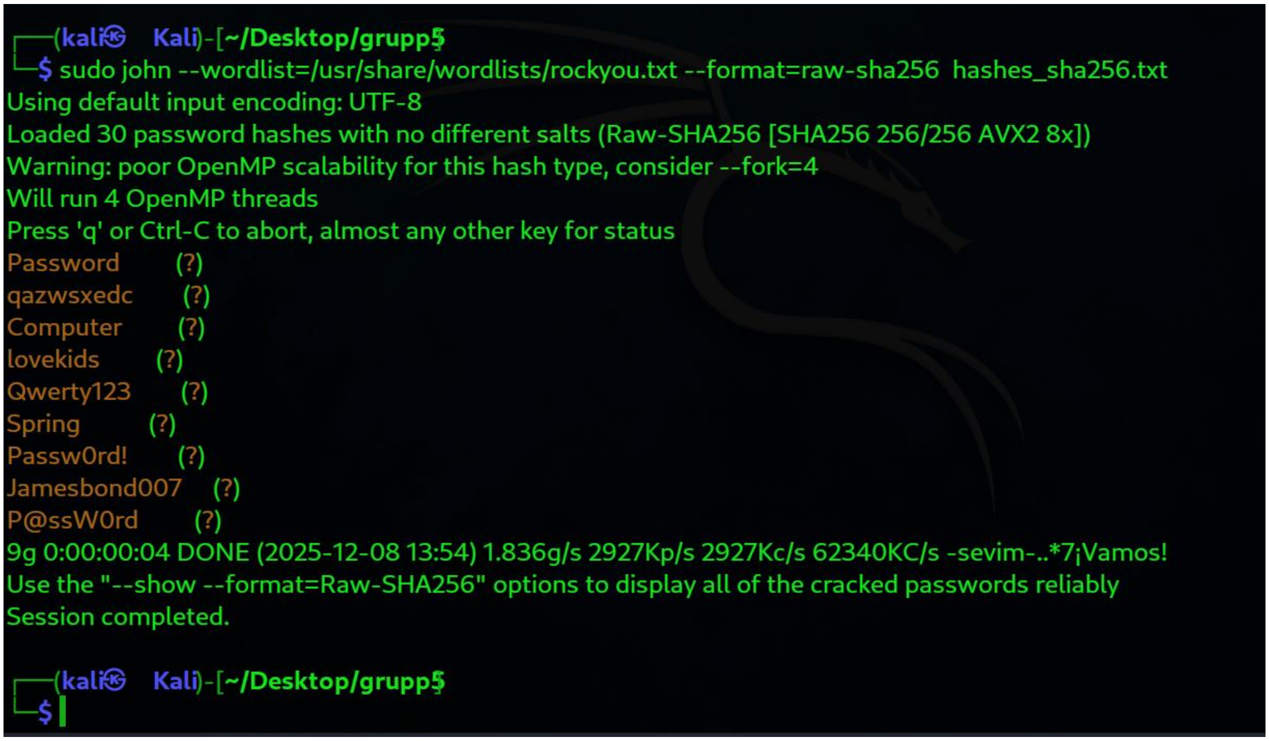
Command: john --wordlist=/usr/share/wordlists/rockyou.txt --rules --format=raw-md5 hashesMD5.txt



```
┌──(kali㉿Kali)-[~/Desktop/grupp5]
└─$ john --wordlist=/usr/share/wordlists/rockyou.txt --rules --format=raw-md5 hashesMD5.txt
Using default input encoding: UTF-8
Loaded 30 password hashes with no different salts (Raw-MD5 [MD5 128/128 SSE2 4×3])
Remaining 20 password hashes with no different salts
Warning: no OpenMP support for this hash type, consider --fork=2
Press 'q' or Ctrl-C to abort, almost any other key for status
House123         (?)
Lovepc           (?)
Internet001      (?)
3g 0:00:00:21 DONE (2025-12-03 13:00) 0.1418g/s 11049Kp/s 11049Kc/s 190169KC/s Aarlovering..Aaaaaaaaaaaaing
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed.

┌──(kali㉿Kali)-[~/Desktop/grupp5]
└─$ john --show --format=raw-md5 hashesMD5.txt
?:Password
?:P@ssW0rd
?:Passw0rd!
?:Qwerty123
?:Spring
?:House123
?:lovekids
?:myson2011
?:Computer
?:Jamesbond007
?:qazwsxedc
?:Internet001
?:Lovepc

13 password hashes cracked, 17 left
```

Session Name:	John the Ripper SHA256 wordlist
Hash Type:	Raw-SHA256 (Hashcat mode 1400)
Hash File:	hashes_sha256.txt
Attack Mode:	Wordlist (--wordlist)
Wordlist:	/usr/share/wordlists/rockyou.txt
Start Time:	20251208 13:54:00
End Time:	20251208 13:54:04
Total Duration:	4 seconds
Recovered:	9/30 hashes (27%)

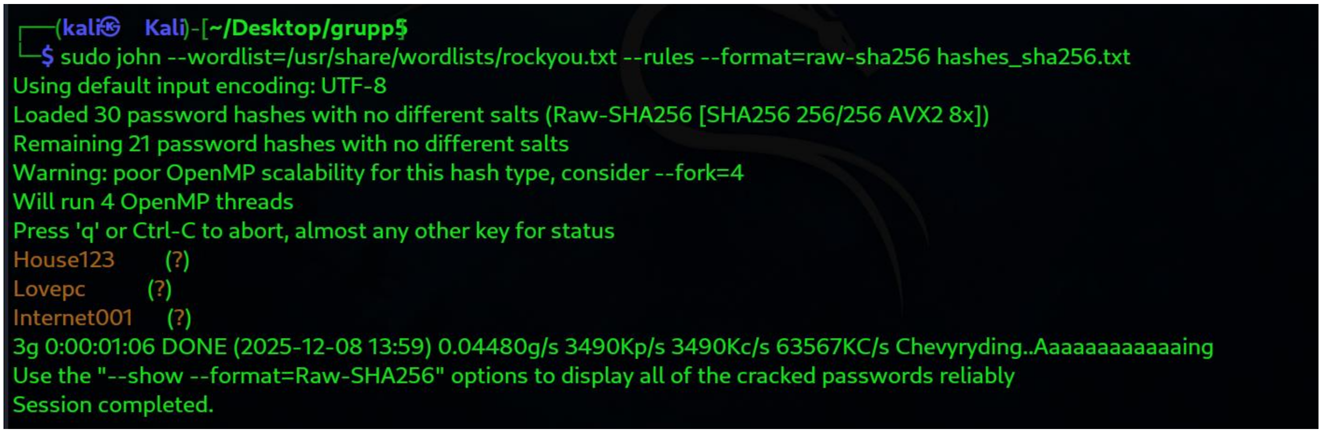
Command: sudo john –wordlist=/usr/share/wordlists/rockyou.txt –format=raw-sha256 hashes_sha256.txt



```
┌──(kali㉿Kali)-[~/Desktop/grupp5]
└─$ sudo john --wordlist=/usr/share/wordlists/rockyou.txt --format=raw-sha256  hashes_sha256.txt
Using default input encoding: UTF-8
Loaded 30 password hashes with no different salts (Raw-SHA256 [SHA256 256/256 AVX2 8x])
Warning: poor OpenMP scalability for this hash type, consider --fork=4
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
Password         (?)
qazwsxedc        (?)
Computer         (?)
lovekids         (?)
Qwerty123        (?)
Spring           (?)
Passw0rd!        (?)
Jamesbond007     (?)
P@ssW0rd         (?)
9g 0:00:00:04 DONE (2025-12-08 13:54) 1.836g/s 2927Kp/s 2927Kc/s 62340KC/s -sevim-..*7¡Vamos!
Use the "--show --format=Raw-SHA256" options to display all of the cracked passwords reliably
Session completed.

┌──(kali㉿Kali)-[~/Desktop/grupp5]
└─$ 
```

Session Name:	John the Ripper SHA256 Rules
Hash Type:	Raw-sha256 (Hashcat mode 1400)
Hash File:	hashes256.txt
Attack Mode:	Wordlist (--wordlist)
Wordlist:	/usr/share/wordlists/rockyou.txt
Start Time:	20251208 13:59:00
End Time:	20251208 14:00:06
Total Duration:	66 seconds
Recovered:	3/30 hashes (10%)

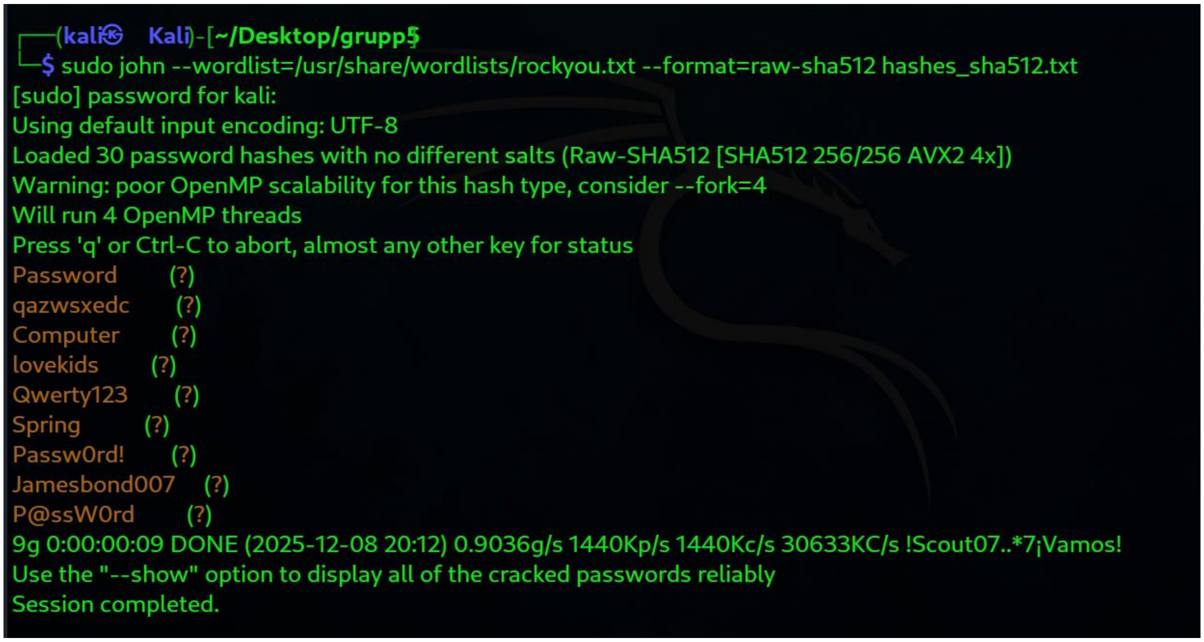
Command: sudo john –wordlist=/usr/share/wordlists/rockyou.txt --rules -- format=raw-sha256 hashes_sha256.txt



```
┌──(kali㉿ Kali)-[~/Desktop/grupp5
└─$ sudo john --wordlist=/usr/share/wordlists/rockyou.txt --rules --format=raw-sha256 hashes_sha256.txt
Using default input encoding: UTF-8
Loaded 30 password hashes with no different salts (Raw-SHA256 [SHA256 256/256 AVX2 8x])
Remaining 21 password hashes with no different salts
Warning: poor OpenMP scalability for this hash type, consider --fork=4
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
House123        (?)
Lovepc          (?)
Internet001     (?)
3g 0:00:01:06 DONE (2025-12-08 13:59) 0.04480g/s 3490Kp/s 3490Kc/s 63567KC/s Chevyryding..Aaaaaaaaaaaaing
Use the "--show --format=Raw-SHA256" options to display all of the cracked passwords reliably
Session completed.
```

Session Name:	John the Ripper SHA512 Wordlists
Hash Type:	Raw-sha512 (Hashcat mode 1700)
Hash File:	hashes_sha512.txt
Attack Mode:	Wordlist (--wordlist)
Wordlist:	/usr/share/wordlists/rockyou.txt
Start Time:	20251208 20:12:00
End Time:	20251208 20:12:09
Total Duration:	9 seconds (instant completion)
Recovered:	9/30 hashes (30%)

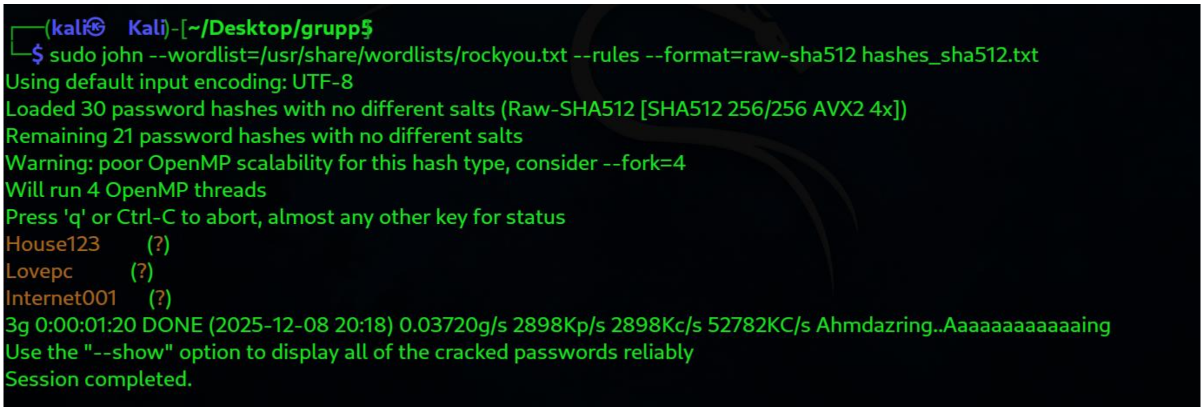
Command: sudo john –wordlist=/usr/share/wordlists/rockyou.txt –format=raw-sha512 hashes_sha512.txt



```
┌──(kali㉿ Kali)-[~/Desktop/grupp5
└─$ sudo john --wordlist=/usr/share/wordlists/rockyou.txt --format=raw-sha512 hashes_sha512.txt
[sudo] password for kali:
Using default input encoding: UTF-8
Loaded 30 password hashes with no different salts (Raw-SHA512 [SHA512 256/256 AVX2 4x])
Warning: poor OpenMP scalability for this hash type, consider --fork=4
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
Password         (?)
qazwsxedc        (?)
Computer         (?)
lovekids         (?)
Qwerty123        (?)
Spring           (?)
Passw0rd!        (?)
Jamesbond007     (?)
P@ssW0rd         (?)
9g 0:00:00:09 DONE (2025-12-08 20:12) 0.9036g/s 1440Kp/s 1440Kc/s 30633KC/s !Scout07..*7¡Vamos!
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Session Name:	John the Ripper SHA512 Rules
Hash Type:	Raw-SHA512 (Hashcat mode 1700)
Hash File:	hashes_sha512.txt
Attack Mode:	Wordlist (--wordlist)
Wordlist:	/usr/share/wordlists/rockyou.txt
Start Time:	20251208 20:18:00
End Time:	20251203 20:19:20
Total Duration:	80 seconds
Recovered:	3/30 hashes (10%)

Command: sudo john --wordlist=/usr/share/wordlists/rockyou.txt --rules --format=raw-sha512 hashes_sha512.txt



```
┌──(kali㉿Kali)-[~/Desktop/grupp5]
└─$ sudo john --wordlist=/usr/share/wordlists/rockyou.txt --rules --format=raw-sha512 hashes_sha512.txt
Using default input encoding: UTF-8
Loaded 30 password hashes with no different salts (Raw-SHA512 [SHA512 256/256 AVX2 4x])
Remaining 21 password hashes with no different salts
Warning: poor OpenMP scalability for this hash type, consider --fork=4
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
House123        (?)
Lovepc          (?)
Internet001     (?)
3g 0:00:01:20 DONE (2025-12-08 20:18) 0.03720g/s 2898Kp/s 2898Kc/s 52782KC/s Ahmdazring..Aaaaaaaaaaaaing
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Appendix B – Use of AI Assistance

This project made limited and transparent use of AI tools to support the completion of the assignment. AI assistance was used in two main areas:

1. Technical Guidance

AI was used to help verify and refine command line syntax for Hashcat and John the Ripper. This included confirming correct attack modes, hash types, and general troubleshooting steps. All commands were executed, tested, and validated manually to ensure accuracy and reproducibility.

2. Writing Support

AI was used to improve the clarity and structure of written sections, including refining paragraph flow, correcting grammar, and helping articulate technical explanations in clear English. All content was reviewed, edited, and finalised by the author to ensure it accurately reflects the work performed.

No AI tools were used to generate results, perform cracking operations, or manipulate data. All experimental work, screenshots, logs, and analysis were carried out manually.