



Phase 2: Password Cracking Report



Cracked Password List

Using: hashcat -m 0 hashfile.txt rockyou.txt

Hash	Password
d50ba4dd3fe42e17e9faa9ec29f89708	iamironman
a0e8402fe185455606a2ae870dcbc4cd	carrots123
d730fc82effd704296b5bbcbff45f323e	donuts4life
706ab9fc256efabf4cb4cf9d31ddc8eb	darkside42

```
audith@lap:~/IT00AK39-3005-Cybersecurity-and-data-privacy/Phase2$ hashcat -m 0 hashfile.txt rockyou.txt
Dictionary cache hit:
  * Filename..: rockyou.txt
  * Passwords.: 14344384
  * Bytes.....: 139921497
  * Keyspace...: 14344384

d50ba4dd3fe42e17e9faa9ec29f89708:iamironman
a0e8402fe185455606a2ae870dcbc4cd:carrots123
d730fc82effd704296b5bbcbff45f323e:donuts4life
706ab9fc256efabf4cb4cf9d31ddc8eb:darkside42
Approaching final keyspace - workload adjusted.

Session.....: hashcat
Status.....: Exhausted
Hash.Mode.....: 0 (MD5)
Hash.Target.....: hashfile.txt
Time.Started.....: Mon Dec 8 23:48:19 2025 (3 secs)
Time.Estimated.....: Mon Dec 8 23:48:22 2025 (0 secs)
Kernel.Feature....: Pure Kernel
Guess.Base.....: File (rockyou.txt)
Guess.Queue.....: 1/1 (100.00%)
Speed.#1.....: 5945.0 kH/s (1.56ms) @ Accel:512 Loops:1 Thr:32 Vec:1
Recovered.....: 4/10 (40.00%) Digests
Progress.....: 14344384/14344384 (100.00%)
Rejected.....: 0/14344384 (0.00%)
Restore.Point.....: 14344384/14344384 (100.00%)
Restore.Sub.#1....: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine..: Device Generator
Candidates.#1....: $HEX(210272096e06261793838) -> $HEX(042a0337c2a156616d6f732103)
Hardware.Mon.#1...: Temp: 53C Util: 41% Core:1594MHz Mem:3504MHz Bus:4
Started: Mon Dec 8 23:48:19 2025
Stopped: Mon Dec 8 23:48:22 2025
audith@lap:~/IT00AK39-3005-Cybersecurity-and-data-privacy/Phase2$
```

Using: hashcat -m 0 hashfile.txt crackstation.txt

Hash	Password
f158d479ee181aac68b000a60e7a3d7a	chaos123!

Hash	Password
735f7f5e652d7697723893e1a5c04d90	iamvengeance

```

Phase2$ cat hashfile.txt
1 735f7f5e652d7697723893e1a5c04d90
2 7cb56c2b8615b797c7ff32eae97f7338
3 12c9cef0bf6b91c42b363b4cf02d8bb
4 f158d479ee181aac68b080a60e7a3d7a
5 ea261222d4867b3ebdfadbe2b35e19d5
6 ad171bd845000b11678ccbf94e135b56

muditha@lap:~/IT00AK39-3005-Cybersecurity-and-data-privacy/Phase2$ hashcat -m 0 -a 0 hashfile.txt crackstation.txt
* Create more work items to make use of your parallelization power:
  https://hashcat.net/faq/morework

f158d479ee181aac68b080a60e7a3d7a:chaos123!
735f7f5e652d7697723893e1a5c04d90:iamvengeance
Approaching final keyspace - workload adjusted.

Session.....: hashcat
Status.....: Exhausted
Hash.Mode.....: 0 (MD5)
Hash.Target.....: hashfile.txt
Time.Started.....: Wed Dec 10 14:21:47 2025 (4 mins, 5 secs)
Time.Estimated.....: Wed Dec 10 14:25:52 2025 (0 secs)
Kernel.Feature....: Pure Kernel
Guess.Base.....: File (crackstation.txt)
Guess.Queue.....: 1/1 (100.00%)
Speed.#1.....: 4413.2 MH/s (1.66ms) @ Accel:512 Loops:1 Thr:32 Vec:1
Recovered.....: 2/6 (33.33%) Digests
Progress.....: 1212336035/1212336035 (100.00%)
Rejected.....: 0/1212336035 (0.00%)
Restore.Point.....: 1212336035/1212336035 (100.00%)
Restore.Sub.#1....: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine..: Device Generator
Candidates.#1....: $HEX(e0b0c5a47e4bb99) -> $HEX(bfe9bea5d7b4)
Hardware.Mon.#1...: Temp: 82C Util: 29% Core:1594MHz Mem:3504MHz Bus:4

Started: Wed Dec 10 14:19:28 2025
Stopped: Wed Dec 10 14:25:53 2025

```



Report Answers

1 Main difference between Dictionary and Non-Dictionary attacks

Dictionary attack: Uses a predefined list of possible passwords (wordlist) to try against password hashes, making it fast if the password is common.

Non-dictionary attack: (e.g., brute-force or mask) tries all possible combinations of characters, which is much slower but can crack passwords not found in wordlists(in my machine can run just up to ?a 7 combination).

2 Advantage of having access to the system's database with users and password hashes

An attacker can target specific users, attempt to crack their password hashes offline, and use the information to impersonate users or escalate privileges. Knowing usernames and hashes allows for focused and efficient attacks (There for I could identify hashing with MD5 and directly attack using "-m 0").

3 Security benefits of longer passwords

Longer passwords increase the number of possible combinations, making brute-force and guessing attacks much more difficult and time-consuming. This greatly improves resistance against both dictionary and non-dictionary attacks (in my machine can run maximum 7 combinations and need too much time when compared with 3 sets).

```
muditha@lap:~/IT00AK39-3005-Cybersecurity-and-data-privacy$ psql -h localhost -p 5434 -U postgres -d postgres
Password for user postgres:
psql (14.20 (Ubuntu 14.20-0ubuntu0.22.04.1), server 18.1 (Debian 18.1-1.pgdg13+2))
WARNING: psql major version 14, server major version 18.
Some psql features might not work.
Type "help" for help.

postgres=# select
postgres=# \dt
          List of relations
Schema | Name          | Type | Owner
-----+-----+-----+-----
public | booking_admin_logs | table | postgres
public | booking_login_logs | table | postgres
public | booking_reservations | table | postgres
public | booking_resources | table | postgres
public | booking_users | table | postgres
(5 rows)

postgres=# select * from booking_users;
ERROR: syntax error at or near "select"
LINE 2: select * from booking_users;
          ^

postgres=# SELECT * FROM booking_users;
 user_id | username | password_hash | role | birthdate | user_token
-----+-----+-----+-----+-----+-----
1 | whatsupdoc@looneytunes.tv | a0e8402fe185455606a2ae870dcbc4cd | reserver | 1980-04-12 | b7a8d729-f5c3-4f5a-86e2-9cdb73511ad9
2 | doh@springfieldpower.net | d730fc82effd704296b5bbcff45f323e | administrator | 1975-05-10 | f3b93c24-8b55-4a0d-8b3c-97c4b8a1e728
3 | darkknight@gothamwatch.org | 735f7f5e652d7697723893e1a5c04d90 | reserver | 1988-09-15 | 94e30d50-4b2e-47b4-920a-0c5f6721a5a2
4 | chimichanga@fourthwall.com | 7cb56c2b86150b797cfff32eae97f338 | administrator | 1991-02-22 | de3d09e1-fc3a-4938-80c6-bef1b45b91b2
5 | iamyourfather@deathstar.gov | 706ab9fc256efabf4cb4cf9d31ddc8eb | reserver | 1960-06-01 | c02dd33f-198a-43e7-882f-b4a73b5dbf18
6 | elementary@221bbaker.uk | 12c9cef0bfb6b91c42b363b4cf02d8bb | administrator | 1982-01-07 | 9c6ffbe1-44eb-4428-b3fd-bcc44f38de31
7 | genius@starkindustries.com | d50ba4dd3fe42e17e9faa9ec29f89708 | reserver | 1970-05-29 | af9c8d38-9d8f-4b71-9b48-e67212a6355a
8 | whysoserious@gothamchaos.net | f158d479ee181aac68b000a60e7a3d7a | administrator | 1985-07-18 | dd0b5c4b-1e99-4193-98c8-317f48b4b6f6
9 | quackattack@duckburg.org | ea261222d4867b3ebdfadbe2b35e19d5 | reserver | 1992-11-25 | 4f5a3ef5-191e-4de0-a68e-53e349e6788b
10 | ruhroh@mysterymachine.com | ad17fbd845000b11678ccbf94e135b56 | reserver | 1987-03-30 | fb9d315b-d1f1-49a1-8717-f28db6b94989
11 | a@a.com | e10adc3949ba59abbe56e057f20f883e | reserver | 2025-12-01 | 71812c87-76a6-44e8-8a4b-be4028ee51ae
(11 rows)
```