Assignment – 7

HashCat-Password Cracking-Kali

┌──(kali㉿kali)-[~]

└─$ echo -n "password123" | md5sum > hashes.txt

┌──(kali㉿kali)-[~]

└─$ sudo apt install hashcat

[sudo] password for kali:

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

The following packages were automatically installed and are no longer required:

firebird3.0-common libfreerdp-client2-2t64 libgumbo2 libtag1v5 python3-pendulum

firebird3.0-common-doc libfreerdp2-2t64 libicu-dev libtag1v5-vanilla python3-pluggy

fonts-liberation2 libgail-common libimobiledevice6 libtagc0 python3-pytzdata

freerdp2-x11 libgail18t64 libiniparser1 libu2f-udev python3-setproctitle

hydra-gtk libgeos3.12.1t64 libjim0.82t64 libusbmuxd6 python3-setuptools-scm

icu-devtools libgl1-mesa-dev libjsoncpp25 libwebrtc-audio-processing1 python3-trove-classifiers

libabsl20230802 libglapi-mesa libmbedcrypto7t64 libwinpr2-2t64 python3.11

libassuan0 libgles-dev libmfx1 libzip4t64 python3.11-dev

libavfilter9 libgles1 libmsgraph-0-1 openjdk-17-jre python3.11-minimal

libbfio1 libglvnd-core-dev libopenh264-7 openjdk-17-jre-headless ruby-zeitwerk

libcapstone4 libglvnd-dev libpaper1 perl-modules-5.38 ruby3.1

libcephfs2 libgspell-1-2 libperl5.38t64 python3-appdirs ruby3.1-dev

libconfig++9v5 libgtk2.0-0t64 libplacebo338 python3-diskcache ruby3.1-doc

libconfig9 libgtk2.0-bin libplist3 python3-hatch-vcs rwho

libdirectfb-1.7-7t64 libgtk2.0-common libpostproc57 python3-hatchling rwhod

libegl-dev libgtksourceview-3.0-1 libpython3.11-dev python3-lib2to3 samba-vfs-modules

libflac12t64 libgtksourceview-3.0-common libre2-10 python3-mistune0

libfmt9 libgtksourceviewmm-3.0-0v5 libroc0.3 python3-pathspec

Use 'sudo apt autoremove' to remove them.

Summary:

Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 419

┌──(kali㉿kali)-[~]

└─$ gunzip /usr/share/wordlists/rockyou.txt.gz

gzip: /usr/share/wordlists/rockyou.txt.gz: No such file or directory

┌──(kali㉿kali)-[~]

└─$ hashcat --help | grep -i md5

```
      0 | MD5                                          | Raw Hash
   5100 | Half MD5                                     | Raw Hash
     70 | md5(utf16le($pass))                          | Raw Hash
     10 | md5($pass.$salt)                             | Raw Hash salted and/or
iterated
     20 | md5($salt.$pass)                             | Raw Hash salted and/or
iterated
   3800 | md5($salt.$pass.$salt)                       | Raw Hash salted and/or
iterated
   3710 | md5($salt.md5($pass))                        | Raw Hash salted and/or
iterated
   4110 | md5($salt.md5($pass.$salt))                  | Raw Hash salted
and/or iterated
   4010 | md5($salt.md5($salt.$pass))                  | Raw Hash salted
and/or iterated
  21300 | md5($salt.sha1($salt.$pass))                 | Raw Hash salted
and/or iterated
     40 | md5($salt.utf16le($pass))                    | Raw Hash salted and/or
iterated
   2600 | md5(md5($pass))                              | Raw Hash salted and/or
iterated
```

3910 | md5(md5($pass).md5($salt)) | Raw Hash salted and/or iterated

3500 | md5(md5(md5($pass))) | Raw Hash salted and/or iterated

4400 | md5(sha1($pass)) | Raw Hash salted and/or iterated

4410 | md5(sha1($pass).$salt) | Raw Hash salted and/or iterated

20900 | md5(sha1($pass).md5($pass).sha1($pass)) | Raw Hash salted and/or iterated

21200 | md5(sha1($salt).md5($pass)) | Raw Hash salted and/or iterated

4300 | md5(strtoupper(md5($pass))) | Raw Hash salted and/or iterated

30 | md5(utf16le($pass).$salt) | Raw Hash salted and/or iterated

4700 | sha1(md5($pass)) | Raw Hash salted and/or iterated

4710 | sha1(md5($pass).$salt) | Raw Hash salted and/or iterated

21100 | sha1(md5($pass.$salt)) | Raw Hash salted and/or iterated

18500 | sha1(md5(md5($pass))) | Raw Hash salted and/or iterated

20800 | sha256(md5($pass)) | Raw Hash salted and/or iterated

50 | HMAC-MD5 (key = $pass) | Raw Hash authenticated

60 | HMAC-MD5 (key = $salt) | Raw Hash authenticated

11900 | PBKDF2-HMAC-MD5 | Generic KDF

11400 | SIP digest authentication (MD5) | Network Protocol

5300 | IKE-PSK MD5 | Network Protocol

25100 | SNMPv3 HMAC-MD5-96 | Network Protocol

25000 | SNMPv3 HMAC-MD5-96/HMAC-SHA1-96 | Network Protocol

10200 | CRAM-MD5 | Network Protocol

4800 | iSCSI CHAP authentication, MD5(CHAP) | Network Protocol

6300 | AIX {smd5} | Operating System

19000 | QNX /etc/shadow (MD5) | Operating System

2410 | Cisco-ASA MD5 | Operating System

2400 | Cisco-PIX MD5 | Operating System

500 | md5crypt, MD5 (Unix), Cisco-IOS 1 (MD5) | Operating System

11100 | PostgreSQL CRAM (MD5) | Database Server

16400 | CRAM-MD5 Dovecot | FTP, HTTP, SMTP, LDAP Server

24900 | Dahua Authentication MD5 | FTP, HTTP, SMTP, LDAP Server

1600 | Apache $apr1$ MD5, md5apr1, MD5 (APR) | FTP, HTTP, SMTP, LDAP Server

4711 | Huawei sha1(md5($pass).$salt) | Enterprise Application Software (EAS)

9700 | MS Office <= 2003 $0/$1, MD5 + RC4 | Document

9710 | MS Office <= 2003 $0/$1, MD5 + RC4, collider #1 | Document

9720 | MS Office <= 2003 $0/$1, MD5 + RC4, collider #2 | Document

25600 | bcrypt(md5($pass)) / bcryptmd5 | Forums, CMS, E-Commerce

30000 | Python Werkzeug MD5 (HMAC-MD5 (key = $salt)) | Framework

22500 | MultiBit Classic .key (MD5) | Cryptocurrency Wallet

Wordlist + Rules | MD5 | hashcat -a 0 -m 0 example0.hash example.dict -r rules/best64.rule

Brute-Force | MD5 | hashcat -a 3 -m 0 example0.hash ?a?a?a?a?a?a

Combinator | MD5 | hashcat -a 1 -m 0 example0.hash example.dict example.dict

┌──(kali㉿kali)-[~]

└─$

┌──(kali㉿kali)-[~]

└─$ hashcat -m 0 -a 0 -o cracked.txt hashes.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 18.1.8, SLEEF, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]

==========

* Device #1: cpu-sandybridge-12th Gen Intel(R) Core(TM) i5-1235U, 6750/13564 MB (2048 MB allocatable), 4MCU

Minimum password length supported by kernel: 0

Maximum password length supported by kernel: 256

Hashfile 'hashes.txt' on line 1 (482c811da5d5b4bc6d497ffa98491e38 -): Token length exception

* Token length exception: 1/1 hashes
  This error happens if the wrong hash type is specified, if the hashes are
  malformed, or if input is otherwise not as expected (for example, if the
  --username option is used but no username is present)

No hashes loaded.

Started: Wed Apr 23 04:44:37 2025
Stopped: Wed Apr 23 04:44:40 2025

┌──(kali㉿kali)-[~]
└─$ cat cracked.txt

cat: cracked.txt: No such file or directory

┌──(kali㉿kali)-[~]
└─$ cat hashes.txt | awk '{print $1}' > clean_hashes.txt

┌──(kali㉿kali)-[~]
└─$ wget https://github.com/brannondorsey/naive-hashcat/releases/download/data/rockyou.txt

--2025-04-23 04:45:54-- https://github.com/brannondorsey/naive-hashcat/releases/download/data/rockyou.txt

Resolving github.com (github.com)... 20.207.73.82

Connecting to github.com (github.com)|20.207.73.82|:443... connected.

HTTP request sent, awaiting response... 302 Found

Location: https://objects.githubusercontent.com/github-production-release-asset-2e65be/97553311/d4f580f8-6b49-11e7-8f70-7f460f85ab3a?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=releaseassetproduction%2F20250423%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Date=20250423T084543Z&X-Amz-Expires=300&X-Amz-Signature=f76e06aabb9117c242baf84b25069005850faae37cdc1f2acb2e650fa2d46239&X-Amz-SignedHeaders=host&response-content-disposition=attachment%3B%20filename%3Drockyou.txt&response-content-type=application%2Foctet-stream [following]

--2025-04-23 04:45:55-- https://objects.githubusercontent.com/github-production-release-asset-2e65be/97553311/d4f580f8-6b49-11e7-8f70-7f460f85ab3a?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=releaseassetproduction%2F20250423%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Date=20250423T084543Z&X-Amz-Expires=300&X-Amz-Signature=f76e06aabb9117c242baf84b25069005850faae37cdc1f2acb2e650fa2d46239&X-Amz-SignedHeaders=host&response-content-disposition=attachment%3B%20filename%3Drockyou.txt&response-content-type=application%2Foctet-stream

Resolving objects.githubusercontent.com (objects.githubusercontent.com)... 185.199.108.133, 185.199.109.133, 185.199.110.133, ...

Connecting to objects.githubusercontent.com (objects.githubusercontent.com)|185.199.108.133|:443... connected.

HTTP request sent, awaiting response... 200 OK

Length: 139921497 (133M) [application/octet-stream]

Saving to: ‘rockyou.txt’

rockyou.txt
100%[==
===============>] 133.44M 2.35MB/s   in 77s

2025-04-23 04:47:13 (1.74 MB/s) - ‘rockyou.txt’ saved [139921497/139921497]

┌──(kali㉿kali)-[~]

└─$ hashcat -m 0 -a 0 -o cracked.txt clean_hashes.txt rockyou.txt

hashcat (v6.2.6) starting

OpenCL API (OpenCL 3.0 PoCL 6.0+debian Linux, None+Asserts, RELOC, LLVM 18.1.8, SLEEF, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]

==========
* Device #1: cpu-sandybridge-12th Gen Intel(R) Core(TM) i5-1235U, 6750/13564 MB (2048 MB allocatable), 4MCU

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: 1 MB

Dictionary cache built:

* Filename..: rockyou.txt
* Passwords.: 14344391
* Bytes.....: 139921497
* Keyspace..: 14344384
* Runtime...: 2 secs

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

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

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

Hash.Target......: 482c811da5d5b4bc6d497ffa98491e38

Time.Started.....: Wed Apr 23 04:48:37 2025 (1 sec)

Time.Estimated...: Wed Apr 23 04:48:38 2025 (0 secs)

Kernel.Feature...: Pure Kernel

Guess.Base.......: File (rockyou.txt)

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

Speed.#1.........:   15271 H/s (0.64ms) @ Accel:1024 Loops:1 Thr:1 Vec:8

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

Progress.........: 4096/14344384 (0.03%)

Rejected.........: 0/4096 (0.00%)

Restore.Point....: 0/14344384 (0.00%)

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

Candidate.Engine.: Device Generator

Candidates.#1....: 123456 -> oooooo

Hardware.Mon.#1..: Util: 28%

Started: Wed Apr 23 04:47:32 2025

Stopped: Wed Apr 23 04:48:39 2025

┌──(kali㉿kali)-[~]

└─$ hashcat -m 0 -a 0 --show clean_hashes.txt rockyou.txt --debug-mode 2

Use of --debug-mode requires -r/--rules-file or -g/--rules-generate.

```
┌──(kali㉿kali)-[~]
└─$ cat cracked.txt

482c811da5d5b4bc6d497ffa98491e38:password123

┌──(kali㉿kali)-[~]
└─$
```