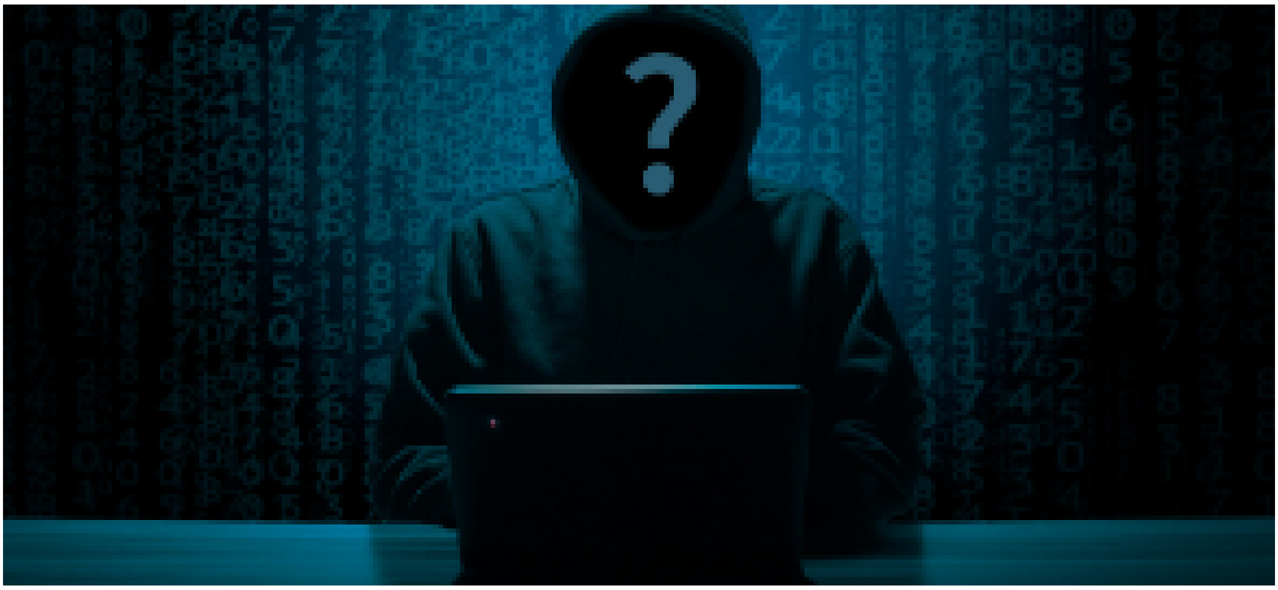
How to Brute Force a Password? (MD5 Hash)

infosecscout.com/how-to-brute-force-a-password

Patrick Fromaget



The idea of a brute force attack is to try any possibility, one by one, until finding the good password.
As the MD5 algorithm is really fast, is the perfect candidate for that kind of strategy.
In this article, we'll see the tools you can use to attempt a brute force attack on a MD5 hash.

**There are free tools like Hashcat and John the Ripper that can run brute force attack on MD5 hashes.
They encrypt thousands of words and compare the results with the MD5 hash to decrypt.**

In the following paragraph, I'll explain to you how the brute force is working exactly, which tools you can use and how to use them. I'll start by a quick reminder about the MD5 algorithm and the other strategies available.
This is important to understand all of this before going further.

By the way, if you are interested in how MD5 decryption really works, I highly encourage you to take a look at my e-book "The Secrets of MD5 Decryption"here. It explains everything you need to know, going directly to the point with practical examples you can test on your computer. You don't need any hardware to get started, just a few tips I give in this book.

Download now

Brute force attacks on MD5 hashes

Let's start with a bit of theory.

MD5 algorithm reminder

As a reminder, did you know how the MD5 algorithm works?

The MD5 algorithm takes any word or text in input and produce a 32 characters hexadecimal string.
Ex: "MD5Online" ⇒ "d49019c7a78cdaac54250ac56d0eda8a"

The MD5 encryption is very fast, you can see on our website that it takes a few seconds including the page load
On a powerful computer, it's even faster.

So, we'll use this encryption speed for the brute force attack.

Brute force process

The goal of a brute force, is not trying to decrypt the MD5 hash, but to encrypt thousands of words until we get the same string.

We can work with a dictionary of common passwords, but most of the time you'll need to start from 0 and try longer and longer password.
For example, encrypting "a" and compare with the MD5 hash, if not the same encrypt "b" and compare with the MD5 hash, etc …

This can take time if the encoded password was a long one.
That's why security advisors recommend taking a long password with special characters.
But you can reduce this time, by using a good CPU/GPU (see our resources page) or cloud computing.

Dictionary attack

Firstly, I recommend trying your MD5 hash in our MD5 decryption tool.
You'll save a lot of time if the MD5 hash is inside.
We have currently over 1,154 billion hashes decrypted and growing.
You'll need a lot of time to try all of this by brute force.
If you are trying to decrypt an SHA1 password (40 characters), click on the link to our other website to try it.

In a brute force software, you can also use your own dictionary.
If you have information about the password source, it can help you find the password faster (company name, family first names, birthdates, …).
By generating a massive dictionary with all this information compiled, you can also save a lot of time.

Brute force tools

Let's move to the practice part.
I'll show you two tools here, but there are other ones if you prefer.
The process is always the same.

HashCat

HashCat is currently considered as the fastest tool to brute force passwords.
It's free, and you can download it from the official website (click on the link).
It's available for any operating system, I'll show you how to use it on Windows and Linux.

Installation

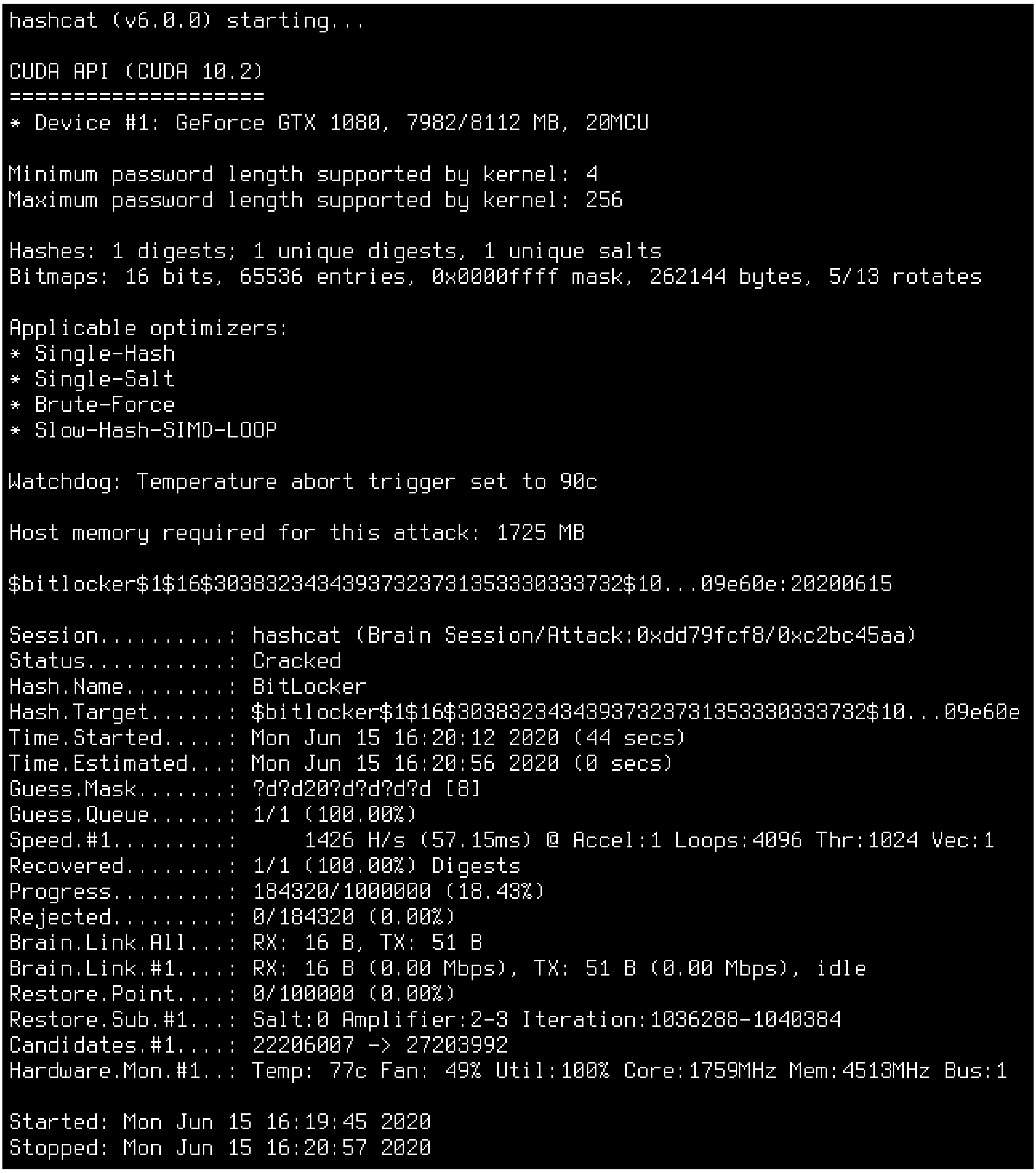
The installation for any operating system is almost the same on Windows and Linux.
Download the binaries archive from the official website (link above), and extract it somewhere.

Windows

To use it on Windows, follow this:

- **Create a new file with a hash to brute force inside**.
  I recommend starting by creating a file "hash.hash" in the hashcat folder.
  Then add this MD5 hash inside: 7f138a09169b250e9dcb378140907378
  It's an easy MD5 password, with 3 characters.
- Then **open a command prompt**.
  Start menu > start typing "command" and click to open the app.
- Then **move to the HashCat directory**.
  For example:
  ```
  cd C:\hashcat
  ```
  Or:
  ```
  cd C:\Users\<USERNAME>\Downloads\hashcat-x.x.x
  ```
- Finally, **use thehash cat command below** to brute force the hash file
  ```
  hashcat64.exe -a 3 -m 0 -w 4 hash.hash -i ?a?a?a --force
  ```

- Option details:
  - -a: The attack mode (3 = Brute force)
  - -m: The hash type on your file (0 = MD5)
  - -w: The workload profile (4 = Nightmare mode)
  - -i: Incremental mode with this mask (3 characters including lowercase/uppercase/number/special)
  - –force: I don't know if you'll need this, but on my laptop I have to use it to avoid an error
- Then check the hash.potfile to see what HashCat have found



```
hashcat (v6.0.0) starting...

CUDA API (CUDA 10.2)
====================
* Device #1: GeForce GTX 1080, 7982/8112 MB, 20MCU

Minimum password length supported by kernel: 4
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

Applicable optimizers:
* Single-Hash
* Single-Salt
* Brute-Force
* Slow-Hash-SIMD-LOOP

Watchdog: Temperature abort trigger set to 90c

Host memory required for this attack: 1725 MB

$bitlocker$1$16$30383234343937323731353330333732$10...09e60e:20200615

Session..........: hashcat (Brain Session/Attack:0xdd79fcf8/0xc2bc45aa)
Status...........: Cracked
Hash.Name........: BitLocker
Hash.Target......: $bitlocker$1$16$30383234343937323731353330333732$10...09e60e
Time.Started.....: Mon Jun 15 16:20:12 2020 (44 secs)
Time.Estimated...: Mon Jun 15 16:20:56 2020 (0 secs)
Guess.Mask.......: ?d?d20?d?d?d?d [8]
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:     1426 H/s (57.15ms) @ Accel:1 Loops:4096 Thr:1024 Vec:1
Recovered........: 1/1 (100.00%) Digests
Progress.........: 184320/1000000 (18.43%)
Rejected.........: 0/184320 (0.00%)
Brain.Link.All...: RX: 16 B, TX: 51 B
Brain.Link.#1....: RX: 16 B (0.00 Mbps), TX: 51 B (0.00 Mbps), idle
Restore.Point....: 0/100000 (0.00%)
Restore.Sub.#1...: Salt:0 Amplifier:2-3 Iteration:1036288-1040384
Candidates.#1....: 22206007 -> 27203992
Hardware.Mon.#1..: Temp: 77c Fan: 49% Util:100% Core:1759MHz Mem:4513MHz Bus:1

Started: Mon Jun 15 16:19:45 2020
Stopped: Mon Jun 15 16:20:57 2020
```

Did you find the password? 🙂

Linux

On Linux, it's almost the same thing, so please read the previous paragraph and adapt it.

The Command Prompt is often called "Terminal" on Linux, you should probably already know it better than Windows users 🙂
And the HashCat command is "./hashcat64.bin" instead of "hashcat64.exe".

If you have a specific device, you can also download the source archive, and compile it with "make".
It's quick, and you'll get an optimized binary for your system.

John The Ripper

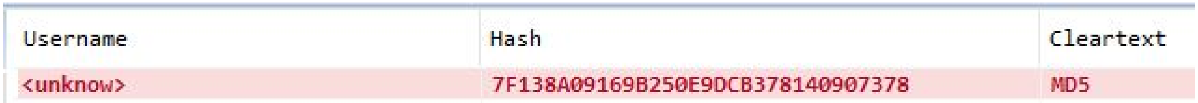
John the Ripper is another tool you can use for brute force.

Windows

John the Ripper is available for Windows, but their creators highly recommend to use HashSuite instead
You can find the software on this link.

Hide your IP address and location with a free VPN:
Try it for free now, with advanced security features.
2900+ servers in 65 countries. It's free. Forever.
There are several versions, but you can take the free one for this test.
You just need to know that there is a limit at 6 characters, but it's ok for now.

- Extract the downloaded archive and go in the extracted files.
- You'll see a "Hash_Suite_64.exe"
- Click on it, HashSuite opens
- In the top menu, click on the keys on the right
- Choose Import > From file
- Browse to the hash.hash file from the hashcat directory
  Or if you didn't install it previously, create a new file with one MD5 inside
  You can use "7f138a09169b250e9dcb378140907378" for example
- Then, on the Main submenu, click on "Start"
- After a few seconds, the MD5 is now decrypted:



Username	Hash	Cleartext
<unknow>	7F138A09169B250E9DCB378140907378	MD5

Linux

On Linux, you can download JohnTheRipper from GitHub.

- Clone the GitHub repository

```
cd /opt
git clone https://github.com/magnumripper/JohnTheRipper
```

- Then compile it as usual on Linux:
  ```
  cd JohnTheRipper/src
  ./configure && make
  ```
- If it ask you for any dependencies missing, install them with your current package manager (apt, yum, …)
- Finally, you can start your first brute force with:
  ```
  cd ../run ./john --format=raw-md5 /root/hash --fork=8
  ```
- Replace /root/hash with the filename containing your hashes
  Then update the fork value with the number of CPU cores you want to assign to this task
  It's not mandatory, on a weak device, you can remove it

You'll get the result in the same folder, but you can use the –show option to display it directly.

Related questions

What is the speed I can get in brute force mode? It highly depends on your hardware (CPU and GPU). With the best graphic card of the moment, searchers find that you can try 758kH/s. But I can't say a number, it will change every month, and doesn't really apply to your system, so try it 🙂

Can I brute-force anything? Same answer, it highly depends on your hardware, but you probably can't go over 8 characters passwords with a standard computer.

Conclusion

That's it, you know how to brute force passwords, with the theory and the practice with two different tools
Hope you'll try it soon and get the results you hope.

I just give you the basics here, feel free to check the official document from HashCat and JohnTheRipper to get all the options you can use with these commands.

Whenever you're ready for more security, here are things you should think about:

- **Break free from Gmail**: You should be able to choose what happens to your data. With Proton, only you can read your emails. Get private email.

- **Protect yourself online**: Use a high-speed Swiss VPN that safeguards your privacy. Open-source, no activity logs. Get Proton VPN risk-free.

- **Master Linux commands**: A sure method to learn (and remember) Linux commands. Useful ones only, one at a time, with clear explanations. Download the e-book.