

Forum:[Hack Forums](#)

Thread: [\[Tutorial\] How to crack hashes & .cap files \(WPA/WPA2\) using Hashcat GUI](#)

LSDoom - September 13, 2015, 3:28 pm

What will you learn in this tutorial?

You will learn how to crack different types of hashes using one of the best tools available, which also happens to be free.

You will also learn the basics on how to identify the most commonly used hashing algorithms.

Tables of content: Choosing the correct version of Hashcat (CPU vs GPU & AMD vs Nvidia)

GUI vs Command Line

Installing the GUI (Skip this part if you want to stick to the command line version)

A brief overview of the GUI

Hash Types

Attack Modes

Cracking your first hashes

1. Choosing the correct version of Hashcat:

Hashcat has a few different versions available, so this is where you decide what to use.

First you need to decide if you want the CPU or GPU cracker. I HIGHLY recommend the GPU cracker. You will get much better cracking speed with GPUs, but if you for some reason don't have a dedicated GPU you will need to use the CPU cracker instead.

This can be the case with some laptops, so check what GPU you have before proceeding any further.

Now you need to choose the AMD or Nvidia version of Hashcat. This is pretty straight forward, if you have an AMD card you choose the AMD version of Hashcat and if you have an Nvidia card you choose the Nvidia version.

Download links can be found here:

[AMD or Nvidia Version](#)

[CPU Version](#)

2. GUI vs Command Line:

Now comes the big question, do you use the Graphical User Interface or the command line?

Personally I use the GUI on my Windows machine and the command line on my Linux machine.

There are pros and cons for both, but it all comes down to personal preference.

I think the GUI is more efficient, but this guide is only going to cover the GUI.

(I might make a guide on how to use the command line for you Linux guys later)

NOTE:

I have had some issues using the GUI on Linux, so this guide does not include the setup on any Linux operating system.

Download link can be found here:

[Hashcat GUI](#)

3. Installing the GUI:

Create a new folder in your C: Drive called "Hashcat GUI"

Extract the Hashcat GUI .zip folder you just downloaded into this directory.

The final step is to take the AMD/Nvidia Hashcat and put that folder into the folder you just created.

It should look something like this: (Keep in mind that your folder will be called something different if you are using the AMD version of Hashcat.)

Now you need to run the program called "App.HashcatGUI".

You will be prompted with something like this:

Located the "oclHashcat" tab and find your binary inside the downloaded AMD/Nvidia folder.

Make sure you select "Applications" and either 32 or 64bit depending on your OS. When you are all done, hit "Open".

You are now done setting up your Hashcat GUI.

4. A brief overview of the GUI:

This is going to be a brief overview of the GUI,

so feel free to look back at this later if you are uncertain of where certain settings are changed.

1. This is where you located the file of saved hashes you wish to crack. Choose your .cap file here if that is what you are trying to crack.

2. Here you change attack modes

3. You select the hash types to crack here.

4. This is where you can apply rules to your attacks.

5. Hash types

The first thing you do when you are going to attempt to crack a hash is identify the hashing algorithm.

This is one of the trickiest parts of hash cracking.
Sometimes it can be very difficult to recognize the algorithm used.

There are some hash types that are a lot more common than others, for example MD5 or SHA1, but if you are uncertain you can use the site below to compare and analyze.

[This is a page containing all the different hash algorithms that are crack-able in Hashcat](#)

I use that page all the time when I am uncertain about what hashing algorithm I am working against. You can also use tools to identify hash types, but these are very often inaccurate or don't even work at all. I try to avoid them because of how unreliable they are.

The first things you should look at when presented with a new hash is the length, what type of characters (numbers, special characters, uppercase/lowercase letter etc.) and lastly you should check if there is a salt.

The salt is displayed at the end of the hash with a ":" separator.

Unsalted MD5:

8743b52063cd84097a65d1633f5c74f5

Salted MD5:

01dfae6e5d4d90d9892622325959afbe:7050461

In Hashcat there are different modes for a salted MD5 and an unsalted MD5, so make sure you choose the correct one.
When you think you have identified your hash please proceed to the next step.

6. Attack Modes

After figuring out what hash you are working with, the next step would be to start attacking it. Understand how the different attack modes work can be a little confusing. I will try to explain the most used ones in the order I would use them.

1. Straight Attack

This tries the hash against all the words in your dictionary from top to bottom WITHOUT altering them in any way.

This is often the fastest attack and this will crack the most common passwords.

2. Straight Attack W/ Rules

Now this is where things start getting a little more complicated.

This does almost the same as a regular straight attack, but with one exception.

Depending on what rule you use, the rules modify the words in the dictionary, removing digits, adding digits, swapping words around etc.

Rule attacks can be pretty fast, but they can also be extremely slow depending on how extensive the rule is.

I suggest trying some light rules first and then moving on to more heavy rules later.

3. Mask Attack

Mask attacks are similar to Brute Forcing. You basically try all combinations within a keyspace.

Masks work like this:

?l = abcdefghijklmnopqrstuvwxyz
?u = ABCDEFGHIJKLMNOPQRSTUVWXYZ
?d = 0123456789
?s = «space»!"#\$%&'()*+,-./:;<=>?@[\\]^_`{|}~
?a = ?l?u?d?s
?b = 0x00 - 0xff

So if I want to crack a password like "Hashcat1990" I would use a mask like this:

?u ?l ?l ?l ?l ?l ?l ?d ?d ?d ?d

[More information about mask attacks if you feel like you need it](#)

7. Cracking your first hash

The only thing you need now is a dictionary. For the sake of this tutorial we will make our own dictionary just for the simplicity.

Create a new text file called dictionary.txt and enter this:

Code password123

password

qwerty

changeme

root

123456

helloworld

hackforums123This will be your dictionary for the sake of this tutorial.

Next you need some hashes. The hashes below as unsalted MD5. Create another text file called hashes.txt and enter this:

Code 482c811da5d5b4bc6d497ffa98491e38

d8578edf8458ce06fbc5bb76a58c5ca4

f62b5748f2802393b6d7a9748b4e6a0e

Now to import the dictionary you find the "Wordlists & Markov" tab and click "Add Wordlists". Brows for the file you just created under the name dictionary.txt and add it.

Now head back to the "oclHashcat" tab and brows for your hashes.txt file.

Set the hash type to "MD5" and hit "Seek and Destroy". (The button might have a different name, it changes all the time.)

The recovered hashes are saved in a .pot file located in your AMD/Nvidia hashcat folder.

You can open this file with any text editor to see whats inside.

It should display this:

Code 482c811da5d5b4bc6d497ffa98491e38:password123

d8578edf8458ce06fbc5bb76a58c5ca4:qwerty

f62b5748f2802393b6d7a9748b4e6a0e:hackforums123

Congrats on cracking your first hashes!

Feel free to post here or PM me if you have any questions or encounter any problems.

Seizure - September 13, 2015, 3:54 pm

Nice tutorial, it's HQ as hell. Whoever needs this won't have a problem reading and understanding.

CubicMuffin - September 13, 2015, 5:44 pm

Very nice OP! I'm sure this will help many people understand (if they actually try and read it all and not just look for the word "automatic") the basics.

LSDoom - September 14, 2015, 1:02 pm

(Sep 13, 2015 05:44 PM)CubicMuffin Wrote: [\[CITE\]](#) Very nice OP! I'm sure this will help many people understand (if they actually try and read it all and not just look for the word "automatic") the basics. Hopefully this will teach people who are interested how they can crack some hashes :)

Stixx - September 14, 2015, 2:14 pm

Thanks for the tutorial man. Will help some people who are maybe confused about this, I know I was.

_Crack - October 23, 2015, 5:18 am

I think I should give Hashcat another go.

Tried the GUI but the command lines it gave me were always non functional.

Nonetheless, it's a great tutorial and would definitely help beginners :)

LSDoom - October 23, 2015, 5:25 am

(Oct 23, 2015 05:18 AM)_Crack Wrote: [\[CITE\]](#) I think I should give Hashcat another go.

Tried the GUI but the command lines it gave me were always non functional.

Nonetheless, it's a great tutorial and would definitely help beginners :)

I can help you setup the GUI and get you started if you want. PM me your skype if you are interested :)

CubicMuffin - October 23, 2015, 7:17 am

(Oct 23, 2015 05:18 AM)_Crack Wrote: [\[CITE\]](#) I think I should give Hashcat another go.

Tried the GUI but the command lines it gave me were always non functional.

Nonetheless, it's a great tutorial and would definitely help beginners :)

Yeah I also found the GUI sometimes a bit tricky. However, setting up a little batch script that takes just a few inputs like hashtype and location of hashes saved me a lot of bother

tux1 - October 23, 2015, 7:23 am

Nice tutorial thanks for sharing.

_Crack - October 24, 2015, 4:05 am

Well, I just downloaded the HashcatGUI & stuff again.

Hope I can make it work this time ;p

Mi2414 - March 20, 2017, 9:50 pm

Really clean tutorial still works, helped me learn a little more. Thanks a bunch man!