Hacking WPA/WPA2 Wi-fi with Hashcat Full Tutorial 2019 9 min read

on June 13, 2019

Facebook 22 Twitter LinkedIn WhatsApp Pinterest

For the most part, aircrack-ng is ubiquitous for wifi and network hacking. But in this article, we will dive in in another tool – Hashcat, is the self-proclaimed world's fastest password recovery tool. It had a proprietary code base until 2015, but is now released as free software and also open source. Versions are available for Linux, OS X, and Windows and can come in CPU-based or GPU-based variants.

WHAT IS DIFFERENT BETWEEN AIRCRACK-NG AND HASHCAT?

Basically, **Hashcat** is a technique that uses the graphics card to brute force a password hash instead of using your CPU, it is fast and extremely flexible- to writer made it in such a way that allows distributed cracking. **aircrack-ng** can only work with a dictionary, which severely limits its functionality, while oclHashcat also has a rule-based engine.

Before we go through I just want to mention that you in some cases you need to use a **wordlist**, **which** is a text file containing a collection of words for use in a dictionary attack. And, also you need to install or update your GPU driver on your machine before move on.

SETUP ENVIRONMENT

Suppose this process is being proceeded in Windows. First, to perform a GPU based brute force on a windows machine you'll need:

- Hashcat binaries
- HashcatGUI

Then:

Search

CATEGORIES

Select Category ▾

ARCHIVES

Select Month ▾

RECENT POSTS

Basic Syntax in Java Programming

Java Environment Setup step-by-step

Learning How to Learn: Powerful mental tools to help you master tough subjects

Introduction to Java Programming

The Algorithm Design Manual – 2nd Edition (free download)

- You need to go to the home page of Hashcat to download it at: https://hashcat.net/hashcat/
- Then, navigate the location where you downloaded it. Then unzip it, on Windows or Linux machine you can use 7Zip, for OS X you should use Unarchiever.
- Open up your Command Prompt/Terminal and navigate your location to the folder that you unzipped. If you haven’t familiar with command prompt yet, check out this article.
- Run the executable file by typing `hashcat32.exe` or `hashcat64.exe` which depends on whether your computer is 32 or 64 bit (type `make` if you are using macOS).

WPA2 dictionary attack using Hashcat

Open cmd and direct it to Hashcat directory, copy .hccapx file and wordlists and simply type in cmd

```
cudaHashcat64.exe -m 2500 rootsh3ll-01.hccapx  wordlist.txt wordlist2.t
```

Here I have NVidia’s graphics card so I use CudaHashcat command followed by 64, as I am using Windows 10 64-bit version. yours will depend on graphics card you are using and Windows version(32/64).

cudaHashcat64.exe – The program, In the same folder theres a cudaHashcat32.exe for 32 bit OS and cudaHashcat32.bin / cudaHashcat64.bin for Linux. *oclHashcat*.exe* for AMD graphics card.

-m 2500 = The specific hashtype. 2500 means WPA/WPA2.

> In case you forget the WPA2 code for Hashcat.
>
> Windows CMD: **`cudaHashcat64.exe –help | find “WPA”`**
>
> Linux Terminal: **`cudaHashcat64.bin –help | grep “WPA”`**
>
> It will show you the line containing “WPA” and corresponding code.

`Handshake-01.hccap` = The converted `*.cap` file.

`wordlist.txt wordlist2.txt`= The wordlists, you can add as many wordlists as you want. To simplify it a bit, every wordlist you make should be saved in the CudaHashcat folder.

After executing the command you should see a similar output:

Wait for Hashcat to finish the task. You can pass multiple wordlists at once so that Hashcat will keep on testing next wordlist until the password is matched.

WPA2 Mask attack using Hashcat

As told earlier, Mask attack is a replacement of the traditional Brute-force attack in Hashcat for better and faster results.

let’s have a look at what Mask attack really is.

In Terminal/cmd type:

```
cudaHashcat64.exe -m 2500 <rootsh3ll-01.hccapx> -a 3 ?d?l?u?d?d?d?u?d?s?a
```

`-a 3` is the Attack mode, custom-character set (Mask attack)

`?d?l?u?d?d?d?u?d?s?a` is the character-set we passed to Hashcat. Let's understand it in a bit of detail that

- What is a character set in Hashcat ?
- Why it is useful ?

What is a character set in Hashcat ?

`?d ?l ?u ?d ?d ?d ?u ?d ?s ?a` = 10 letters and digits long WPA key. Can be 8-63 char long.

The above text string is called the "Mask". Every pair we used in the above examples will translate into the corresponding character that can be an Alphabet/Digit/Special character.

For remembering, just see the character used to describe the charset

?d: For digits

?s: For Special characters

?u: For Uppercase alphabets

?l: For Lowercase alphabets

?a: all of the above.

Simple! isn’t it ?

Here is the actual character set which tells exactly about what characters are included in the list:

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

Here are a few examples of how the PSK would look like when passed a specific Mask.

PSK = `?d?l?u?d?d?d?u?d?s?a`

```
0aC575G2/@
9zG432H0*K
8sA111W1$4
3wD001Q5+z
```

So now you should have a good understanding of the mask attack, right ?

Let’s dig a bit deeper now.

Mixing Mask attack with Custom characters.

Let’s say, we somehow came to know a part of the password. So, it would be better if we put that part in the attack and randomize the remaining part in Hashcat, isn’t it ?

Sure! it is very simple. Just put the desired characters in the place and rest with the Mask.

Here?d ?l **123** ?d ?d ?u ?d **C** is the custom Mask attack we have used. Here assuming that I know the first 2 characters of the original password then setting the 2nd and third character as digit and lowercase letter followed by “123” and then “?d ?d ?u ?d” and finally ending with “C” as I knew already.

What we have actually done is that we have simply placed the characters in the exact position we knew and Masked the unknown characters, hence leaving it on to Hashcat to test further.

Here is one more example for the same:

Let’s say password is “Hi123World” and I just know the “Hi123” part of the password, and remaining are lowercase letters. Assuming length of password to be 10.

So I would simply use the command below

```
cudaHashcat64.exe -m 2500 <handshake.hccap> -a 3 Hi123?u?u?u?u?u
```

Where `?u` will be replaced by uppercase letters, one by one till the password is matched or the possibilities are exhausted.

Moving on even further with Mask attack i.r the Hybrid attack.

In hybrid attack what we actually do is we don’t pass any specific string to hashcat manually, but automate it by passing a wordlist to Hashcat.

Hashcat picks up words one by one and test them to the every password possible by the Mask defined.

Example:

- `cudaHashcat64.exe -m 2500 handshake.hccapx -a 1 password.txt ?d?l?d?l`

-a 1 : The hybrid attack
password.txt : wordlist
?d?l?d?l = Mask (4 letters and numbers)

The wordlist contains 4 words.

```
carlos
bigfoot
guest
onion
```

Now it will use the words and combine it with the defined Mask and output should be this:

```
carlos2e1c
bigfoot0h1d
guest5p4a
onion1h1h
```

It is cool that you can even reverse the order of the mask, means you can simply put the mask before the text file. Hashcat will bruteforce the passwords like this:

```
7a2ecarlos
8j3abigfoot
0t3wguest
6a5jonion
```

You getting the idea now, right ?

Using so many dictionary at one, using long Masks or Hybrid+Masks takes a long time for the task to complete. It is not possible for everyone every time to keep the system on and not use for personal work and the Hashcat developers understands this problem very well. So, they came up with a brilliant solution which no other password recovery tool offers built-in at this moment. That is the Pause/Resume feature

WPA2 Cracking Pause/resume in Hashcat (One of the best features)

This feature can be used anywhere in Hashcat. It isn't just limited to WPA2 cracking. Even if you are cracking md5, SHA1, OSX, wordpress hashes. As soon as the process is in running state you can pause/resume the process at any moment.

Just press [**p**] to pause the execution and continue your work.

To resume press [**r**]. All the commands are just at the end of the output while task execution. See image below

You might sometimes feel this feature as a limitation as you still have to keep the system awake, so that the process doesn't gets cleared away from the memory.

And we have a solution for that too. Create session!

WPA2 Cracking save Sessions and Restore.

Creating and restoring sessions with hashcat is Extremely Easy.

Just add –session at the end of the command you want to run followed by the session name.

Example:

```
cudaHashcat64.exe -m 2500 rootsh3ll-01.hccapx -a 3 Hello?d?l?d?u123?l?l
```

Here I named the session “blabla”. You can see in the image below that Hashcat has saved the session with the same name i.e blabla and running.

Now you can simply press [**q**] close cmd, ShutDown System, comeback after a holiday and turn on the system and resume the session. That easy!

> NOTE: Once execution is completed session will be deleted.

How to restore ?

Above command – “**–restore**”. Here it goes:

```
cudaHashcat64.exe -m 2500 rootsh3ll-01.hccapx -a 3 Hello?d?l?d?u123?l?l
```

Hashcat will now check in its working directory for any session previously created and simply resume the Cracking process.

Simple enough ? Yes it is.

This is all for Hashcat. Hope you understand it well and performed it along. No need to be sad if you don’t have enough money to purchase those expensive Graphics cards for this purpose you can still try cracking the passwords at high speeds using the clouds. You just have to pay accordingly.

To specify device use the -d argument and the number of your GPU.
The command should look like this in end:

```
hashcat64.exe -m 2500 -d 3 [handshake_file] example: Handshake.hccapx"
```

Example:

```
hashcat64.exe -m 2500 -d 3 Handshake.hccapx eightdigit.txt
```

Where Handshake.hccapx is my handshake file, and eithdigit.txt is my wordlist, you need to convert cap file to hccapx using https://hashcat.net/cap2hccapx/

This article is referred from **rootsh3ll.com**.

5.0 06 ★★★★★

Facebook Comments

0 Comments Sort by **Oldest**

Add a comment...

Facebook Comments Plugin

PREVIOUS ARTICLE

How to Get Kids involved in Computer Science & Coding

NEXT ARTICLE

Learn Python and Ethical Hacking from Scratch FULL free download [Updated]

Leave a Reply

Start the discussion...

✉ Subscribe ▾