How To Crack WPA/WPA2 Hash Using HashCat

How To Crack WPA/WPA2 With HashCat

The tutorial will illustrate how to install and configure HashCat on a Windows client and crack the captured PMKID or .hccap files using a wordlist dictionary attack.

“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. Versions are available for Linux, OS X, and Windows and can come in CPU-based or GPU-based variants.”

The WPA2 handshake can be captured on a Linux compatible client like Kali Linux with a supported WiFi card running on VirtualBox. Then converted to the right format depending on the captured method and moved over to the Windows client to be cracked.

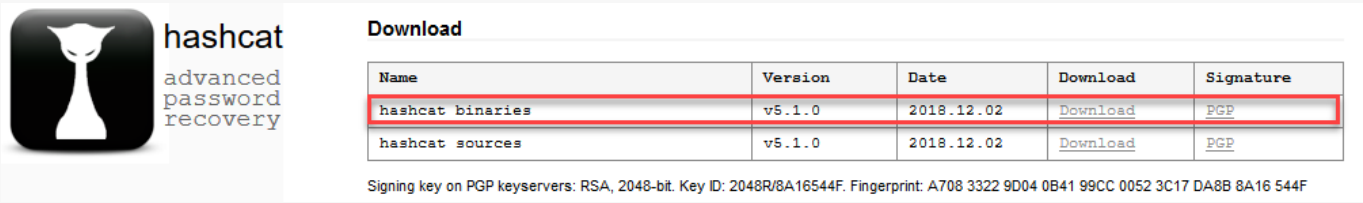
Use the guides Capturing WPA2 and Capturing WPA2 PMKID to capture the WPA2 handshake. For this test we will use the famous “Rockyou” wordlist.

DISCLAIMER: This software/tutorial is for educational purposes only. It should not be used for illegal activity. The author is not responsible for its use or the users action.

Step 1: Download HashCat

Hashcat do not require any installation, it is a portable program it requires you to unpack the downloaded archive.

1. First you need to download Hashcat binaries from https://hashcat.net/hashcat/
2. Navigate to the location where you saved the downloaded file, and unzip the file



Step 2: Download Wordlist

They are numerous wordlists out on the web, for this test we are going to use the famous “rockyou”.

1. Open the hashcat folder on your hard drive and create a new folder called “wordlist”
2. Download the rockyou.txt wordlist from this Link.
3. Save the downloaded file in the new folder “wordlist”

Step 3: Prepare Your Captured WPA2 Handshake

Depending on the method you used to capture the handshake you either must format the cap file to 2500 hash-mode or the PMKID file to hashcat 16800 hash-mode .

For how to format the files please see the guides Capturing WPA2 and Capturing WPA2 PMKID.

In this lab we are using a captured PMKID and a pcpa handshake formatted to hashcat readable format. “HonnyP01.hccapx ” and ” HonnyP02.16800″.

I’m using two different home routers from D-Link and Technicolor for this experiment, both WiFi routers are owed by me.

- The “HonnyP01.hccapx” file is captured from the D-Link router.
- The ” HonnyP02.16800″ file is captured from the Technicolor router.

Step 4: Start Hashcat

You need to run hashcat in CMD or PowerShell. In this example we will use CMD to execute our commands and crack the handshake.

Open CMD and navigate to the hashcat folder.

```
C:\>cd hashcat-5.1.0
C:\hashcat-5.1.0>
```

Type hashcat64 -h to display all options

```
C:\hashcat-5.1.0>hashcat64 -h
```

```
 ===+=============
  1 | CPU
  2 | GPU
  3 | FPGA, DSP, Co-Processor

- [ Workload Profiles ] -

  # | Performance | Runtime | Power Consumption | Desktop Impact
 ===+=============+=========+===================+================
  1 | Low         |   2 ms  | Low               | Minimal
  2 | Default     |  12 ms  | Economic          | Noticeable
  3 | High        |  96 ms  | High              | Unresponsive
  4 | Nightmare   | 480 ms  | Insane            | Headless

- [ Basic Examples ] -

  Attack-          | Hash- |
  Mode             | Type  | Example command
==================+=======+=================================================================
==========
  Wordlist         | $P$   | hashcat -a 0 -m 400 example400.hash example.dict
  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

If you still have no idea what just happened, try the following pages:

* https://hashcat.net/wiki/#howtos_videos_papers_articles_etc_in_the_wild
* https://hashcat.net/faq/

C:\hashcat-5.1.0>
```

Step 5: Crack WPA2

In the First example we will illustrate how to get the password from a converted pcap file “.hccapx”.

Copy your converted file to the hashcat folder, in this example i am copying the file HonnyP01.hccapx to my hashcat folder.

Next we will start hashcat and use the wordlist rockyou, type in the parameters below in CMD.

```
C:\hashcat-5.1.0>hashcat64 -m 2500 -w3 HonnyP01.hccapx "wordlist\rockyou.txt"
```

- hashcat64 the binary
- -m 2500 the format type
- -w 3 workload-profile 3
- HonnyP01.hccapx the formatted file
- “wordlist\rockyou.txt” the path to the wordlist

Hashcat will start processing the file, if you are successful the terminal will display the hash and the password.

```
Watchdog: Temperature abort trigger set to 90c

Dictionary cache hit:
* Filename..: wordlist\rockyou.txt
* Passwords.: 14344384
* Bytes.....: 139921497
* Keyspace..: 14344384

7005312a9933d3a57065450f0749f210:84c9b26a9e90:f4bf80c7ec46:HonnyP01:password
2fed89e93e2cd63175f435db16ca75f0:84c9b26a9e90:f4bf80c7ec46:HonnyP01:password
```

Here we can see that hashcat was able to match the hash to a password in the wordlist, in this lab the password to the D-Link WiFi is “password”. You can chose to let the application run trough the wordlist or press “q” to quit.

```
Approaching final keyspace - workload adjusted.


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

```
Status...........: Cracked
Hash.Type........: WPA-EAPOL-PBKDF2
Hash.Target......: HonnyP01.hccapx
Time.Started.....: Fri Jan 18 20:13:27 2019 (42 secs)
Time.Estimated...: Fri Jan 18 20:14:09 2019 (0 secs)
Guess.Base.......: File (wordlist\rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:   230.7 kH/s (46.06ms) @ Accel:512 Loops:128 Thr:64 Vec:1
Recovered........: 18/25 (72.00%) Digests, 0/1 (0.00%) Salts
Progress.........: 14344384/14344384 (100.00%)
Rejected.........: 4734913/14344384 (33.01%)
Restore.Point....: 14344384/14344384 (100.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:24-49
Candidates.#1....: $HEX[303531313037353434] -> $HEX[042a0337c2a156616d6f732103]
Hardware.Mon.#1..: Temp: 66c Fan: 44% Util: 97% Core:1949MHz Mem:4006MHz Bus:16

Started: Fri Jan 18 20:13:12 2019
Stopped: Fri Jan 18 20:14:10 2019

C:\hashcat-5.1.0>
```

You can display the cracked password with the “show” command or by running the same command again, all cracked hashes will be stored in the “hashcat.potfile” in the hashcat folder.

To display the cracked password in CDM type the command bellow.

```
C:\hashcat-5.1.0>hashcat64 -m 2500 -w3 HonnyP01.hccapx "wordlist\rockyou.txt" --
show
```

```
C:\hashcat-5.1.0>hashcat64 -m 2500 -w3 HonnyP01.hccapx "wordlist\rockyou.txt" --
show
7005312a9933d3a57065450f0749f210:84c9b26a9e90:f4bf80c7ec46:HonnyP01:password
2fed89e93e2cd63175f435db16ca75f0:84c9b26a9e90:f4bf80c7ec46:HonnyP01:password
fcaf4223879e125e10a272f9234256fe:84c9b26a9e90:f4bf80c7ec46:HonnyP01:password
7617ef601966436708eae3ad2c02d295:84c9b26a9e90:f4bf80c7ec46:HonnyP01:password
```

```
8b5ddfc6bade402e38e2ce023449bf07:84c9b26a9e90:f4bf80c7ec46:HonnyP01:password
C:\hashcat-5.1.0>
```

In the next example we will run the same command except now we use the 16800 mode to run the dictionary attack against formatted PMKID file captured from the Technicolor router.

```
C:\hashcat-5.1.0>hashcat64 -m 16800 -w 3 HonnyP02.16800 "wordlist\rockyou.txt"
```

- hashcat64 the binary
- -m 16800 the format type
- -w 3 workload-profile 3
- HonnyP02.16800 the formatted file
- “wordlist\rockyou.txt” the path to the wordlist

```
17a40e5b92e3815f6111554b1c80f4d9*c4ea1d1f7d93*c498808d7d5f*4c656f6e20322e342047487a
:adsladsl

Session..........: hashcat
Status...........: Cracked
Hash.Type........: WPA-PMKID-PBKDF2
Hash.Target......: 17a40e5b92e3815f6111554b1c80f4d9*c4ea1d1f7d93*c4988...47487a
Time.Started.....: Fri Jan 18 23:12:55 2019 (27 secs)
Time.Estimated...: Fri Jan 18 23:13:22 2019 (0 secs)
Guess.Base.......: File (wordlist\rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:   268.6 kH/s (51.75ms) @ Accel:512 Loops:128 Thr:64 Vec:1
Recovered........: 1/1 (100.00%) Digests, 1/1 (100.00%) Salts
Progress.........: 11008839/14344384 (76.75%)
Rejected.........: 3636039/11008839 (33.03%)
Restore.Point....: 10261572/14344384 (71.54%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidates.#1....: aldohizo123 -> Juelle98
Hardware.Mon.#1..: Temp: 68c Fan: 43% Util: 95% Core:1847MHz Mem:4006MHz Bus:16

Started: Fri Jan 18 23:12:48 2019
Stopped: Fri Jan 18 23:13:24 2019
```

```
C:\hashcat-5.1.0>
```

Here we can see that the cracked password is “adsladsl” for the Technicolor router.

```
C:\hashcat-5.1.0>hashcat64 -m 16800 -w 3 HonnyP02.16800 "wordlist\rockyou.txt" --
show
17a40e5b92e3815f6111554b1c80f4d9*c4ea1d1f7d93*c498808d7d5f*4c656f6e20322e342047487a
:adsladsl

C:\hashcat-5.1.0>
```

Extra: Brute Force Attack And Rule based attack

You can let hashcat brute force the file with the command bellow.

```
C:\hashcat-5.1.0>hashcat64 -m 16800 -w 3 HonnyP02.16800 ?l?l?l?l?l?l?l?l
```

Or use ruled base attack.

```
C:\hashcat-5.1.0>hashcat64 -m 16800 -w 3 -r rules\best64.rule
"wordlist\rockyou.txt"
```

Conclusion

Your home or office WiFi can be hacked if you are using a weak password, as always a strong and complex password is still the best defense against an attacker.

DISCLAIMER: This software/tutorial is for educational purposes only. It should not be used for illegal activity. The author is not responsible for its use or the users action.