Cracking Handshakes with Hashcat

CAPTURED HANDSHAKES

Hcxdumptool

- .pcapng file

Aircrack-ng

- .pcap file

hash.hc22000 file (for Hashcat)

Hashcat is a GPU based tool, so you need to have it running on a machine with a powerful graphics card with all drivers. It can be your windows machine, Ubuntu/ Kali machine or you can do it in the cloud

Cracking in the Cloud

- Google, Azure and Linode are a few cloud service providers that offer GPU based VPS servers on rent
- There is anther way to run hashcat on powerful cloud servers by running it through Jupyter-based notebooks(mostly used for machine learning)
  - ✓ Google Collab
  - ✓ Gradient

Cracking on cloud based servers is very fast

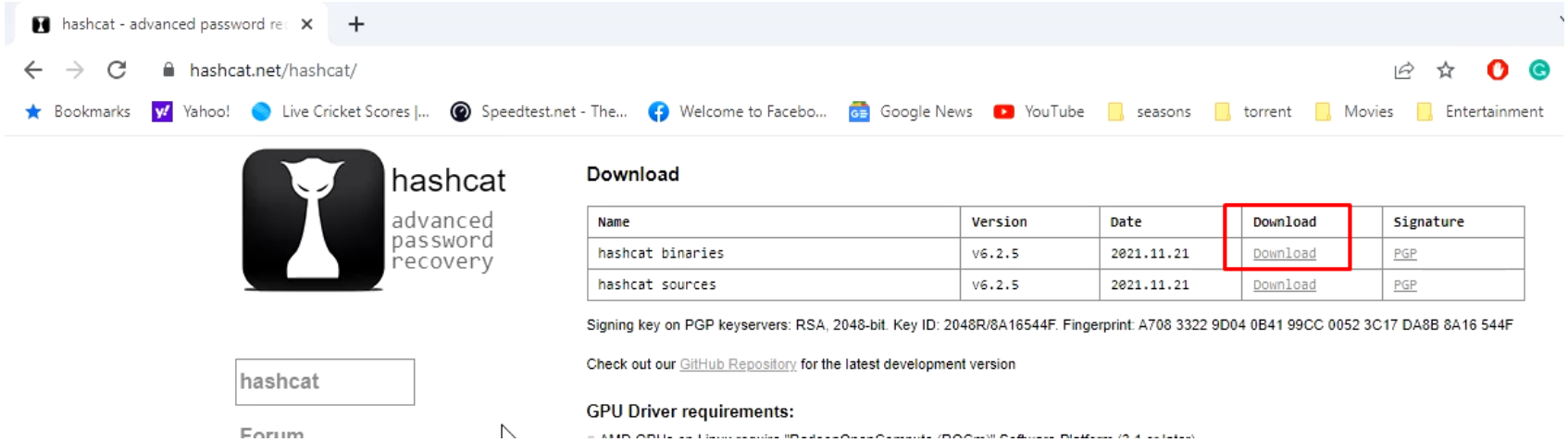
Method -1

Cracking handshakes on Windows with Powerful graphics Card

Step- 1

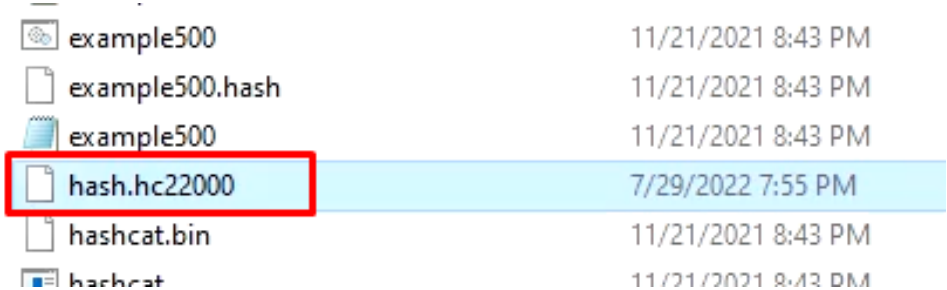
- Install the Hashcat from official website

https://hashcat.net/hashcat/



Step- 2

- Copy the handshake file to hashcat directory



Step- 3

- Download and extract the rockyou dictionary in hashcat folder

https://github.com/brannondorsey/naive-hashcat/releases/download/data/rockyou.txt

Step- 4

- Open the Power shell and then use the command to crack the handshake

```
.\Hashcat.exe -m 22000 -a 0 -o cracked.txt hash.hc22000 rockyou.txt
```

Here :

- 22000 tells the hashcat that its wifi password to be cracked
- Cracked.txt will store cracked passwords
- Hash.hc22000 is the source file
- Rockyou.txt is the dictionary file

Step- 4 (Optional)

To select a particular device. Just select the device with category flag.

```
OpenCL API (OpenCL 1.2 ) - Platform #1 [Intel(R) Corporation]
============================================================
* Device #1: Intel(R) Core(TM) i5-3230M CPU @ 2.60GHz, skipped
* Device #2: Intel(R) HD Graphics 4000, skipped

OpenCL API (OpenCL 2.0 AMD-APP (1800.11)) - Platform #2 [Advanced Micro Devices, Inc.]
================================================================================
* Device #3: Radeon (TM) HD 8670M, 1920/2048 MB (1344 MB allocatable), 5MCU
* Device #4: , skipped
```

To select Device 3 only, use –D 2 –d 3

Method -2

Cracking handshakes in cloud with Google collab

Google Collab

- Google Collab is a free service offered by google to students to train their ML models.
- There are a few jupyter notebooks already created by experts which can be utilized to crack the password
- Do not abuse the service as its use may be restricted on abuse

Step- 1

- Open any of the following links while signed in with your Google account (Separate account is preferred)

- ✓ https://colab.research.google.com/github/mxrch/penglab/blob/master/penglab.ipynb
- ✓ https://colab.research.google.com/github/someshkar/colabcat/blob/master/colabcat.ipynb
- ✓ https://colab.research.google.com/github/ShutdownRepo/google-colab-hashcat/blob/main/google_colab_hashcat.ipynb

Step- 2

- Install hashcat and required dictionaries while following instructions)

Step- 3

- Upload your hash file to an online file hosting provider like filebin.com or catbox.moe and then import it in your notebook with the following command in a new block

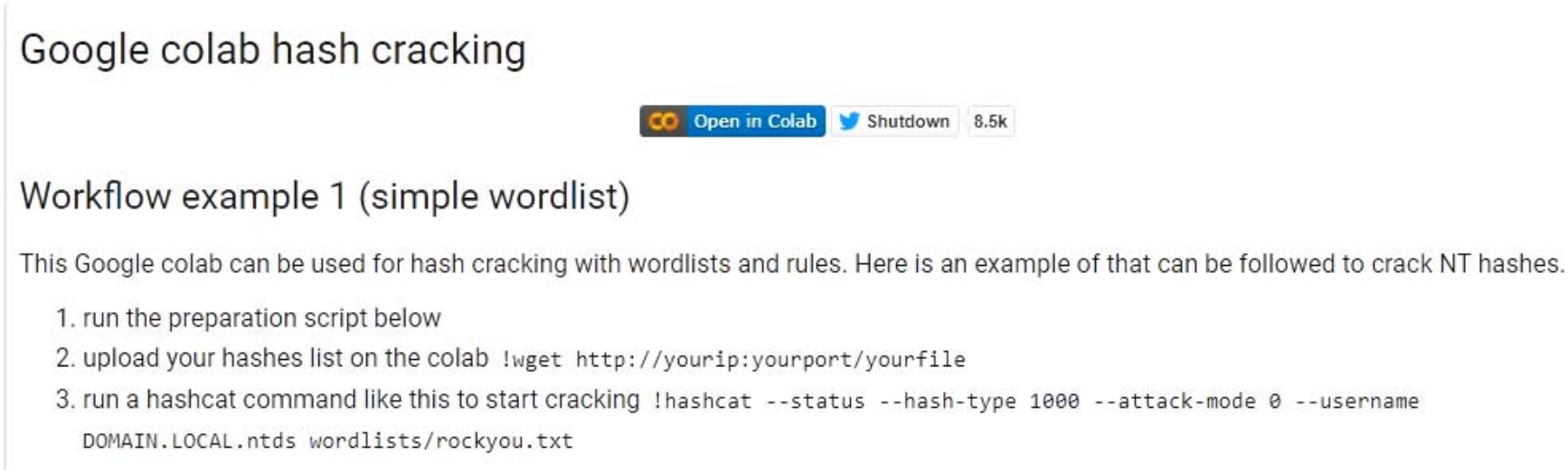
```
>wget http://filebin.com/filename
```

Do not worry with the detail we are going to see details in practical demonstration

Step- 4

- Crack the handshake with following command

```
>!hashcat --status -m 22000 -a 0 -o cracked.txt hash.hc22000 /content/wordlists/rockyou.txt
```



Google colab hash cracking

Open in Colab | Shutdown | 8.5k

Workflow example 1 (simple wordlist)

This Google colab can be used for hash cracking with wordlists and rules. Here is an example of that can be followed to crack NT hashes.

1. run the preparation script below
2. upload your hashes list on the colab `!wget http://yourip:yourport/yourfile`
3. run a hashcat command like this to start cracking `!hashcat --status --hash-type 1000 --attack-mode 0 --username DOMAIN.LOCAL.ntds wordlists/rockyou.txt`

Method -3
Cracking handshakes in cloud with Gradient

Step- 1

- Sign up for a gradient account

https://gradient.run/

Step- 2

- Copy Block by Block, the code from following repo to a new notebook

  - ✓ https://colab.research.google.com/github/ShutdownRepo/google-colab-hashcat/blob/main/google_colab_hashcat.ipynb

Step- 3

- Use the same commands to crack the handshake as we used in google collab

```
>wget http://filebin.com/filename
```

```
>!hashcat --status -m 22000 -a 0 -o cracked.txt hash.hc22000 /content/wordlists/rockyou.txt
```

Step- 3

- Use the same commands to crack the handshake as we used in google collab

```
!hashcat -m 22000 -a 0 -o cracked.txt hash.hc22000 wordlists/rockyou.txt
```

```
hashcat (v6.2.5-634-g5fa08a798) starting

clGetPlatformIDs(): CL_PLATFORM_NOT_FOUND_KHR

CUDA API (CUDA 11.2)
====================
* Device #1: Quadro M4000, 8068/8126 MB, 13MCU
```

DEMO

THANKS