

# Cracking Windows Passwords with Hashcat

@mmar



**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**

**For this lecture, we are going to use it on Windows with all GPU drivers installed**





## CONCEPT

### Step-1

- Get the Hash from the SAM file with Kali Linux (Samdump2)

### Step-2

- Crack the hash with hashcat and RockYou dictionary on our PC



## Attack

### Scenario

- You have physical access to a system which is **password locked**. The tool can be used to quickly **crack** the password

You can copy the extracted hashes from the SAM file with Kali Linux in a USB drive and then in your own time (offline attack) crack the hashes at your home on your main machine with hashcat

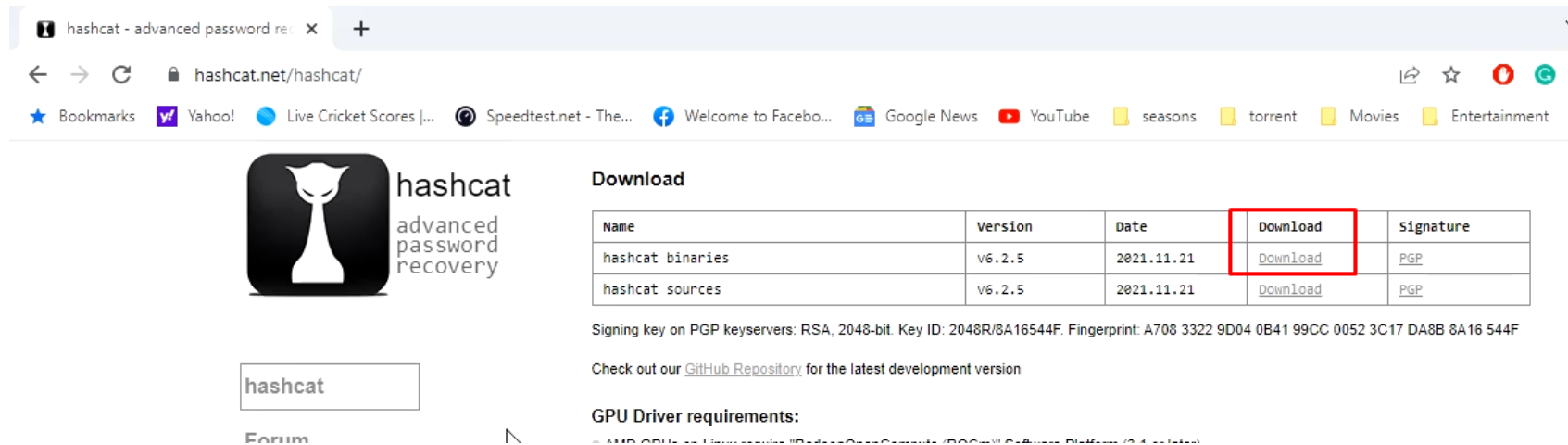


**We need to have Kali Live boot USB  
(Check the lecture “Kali Linux as a bootable USB  
Drive”)**

# Step- 1

❖ Install the Hashcat from official website in your main PC

<https://hashcat.net/hashcat/>



The screenshot shows the Hashcat website interface. On the left, there is a logo for 'hashcat advanced password recovery' and a 'hashcat Forum' button. The main content area features a 'Download' section with a table listing available binaries and sources. The 'Download' column in the table is highlighted with a red box. Below the table, there is a signing key and a link to the GitHub repository. The GPU driver requirements section is partially visible at the bottom.

Name	Version	Date	Download	Signature
hashcat binaries	v6.2.5	2021.11.21	<a href="#">Download</a>	<a href="#">PGP</a>
hashcat sources	v6.2.5	2021.11.21	<a href="#">Download</a>	<a href="#">PGP</a>

Signing key on PGP keyservers: RSA, 2048-bit. Key ID: 2048R/8A16544F. Fingerprint: A708 3322 9D04 0B41 99CC 0052 3C17 DA8B 8A16 544F

Check out our [GitHub Repository](#) for the latest development version

**GPU Driver requirements:**

– AMD GPUs on Linux require "RadeonOpenCompute" (ROCm) Software Platform (2.4 or later)

## Step- 2

- ❖ Download and extract the rockyou dictionary in hashcat folder

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

## Step- 3

- ❖ Boot from Kali Linux USB drive

Plug in USB to target PC and Boot from USB

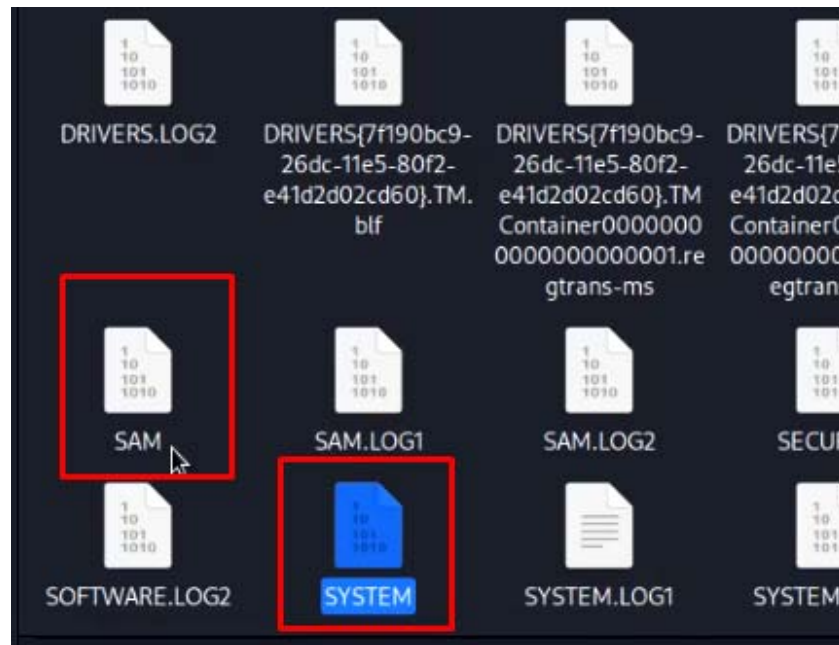




## Step- 4

- ❖ Navigate to windows/system32/config folder and copy these files to Kali Desktop

**SAM & SYSTEM**



## Step- 5

- ❖ Now open the terminal on the desktop and dump the hashes with following command

```
Samdump2 SYSTEM SAM >hash.txt
```

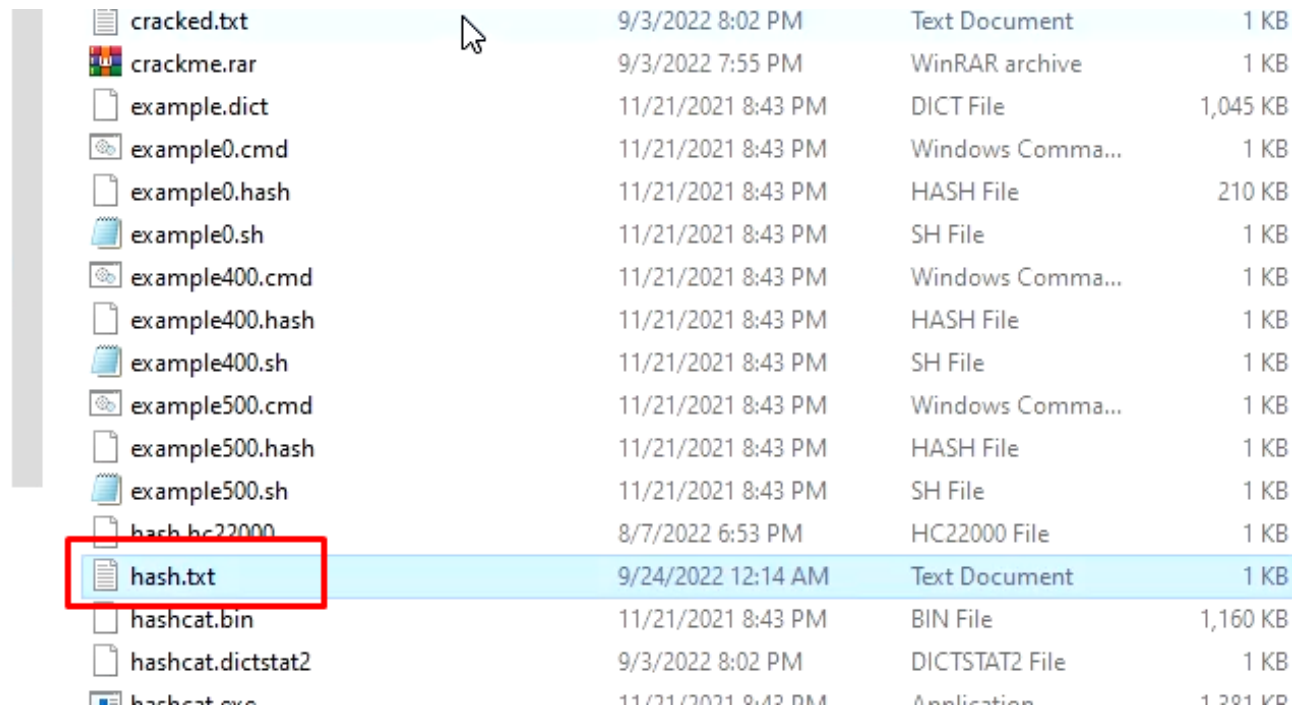
Here :

- Samdump2 is the tool we are using
- Hash.txt will contain all hashes that we are aiming to crack

```
(kali@kali)-[~/Desktop]  
└─$ samdump2 SYSTEM SAM >hash.txt
```

## Step- 6

- ❖ Now copy the hash.txt file to hashcat folder on your main PC (You can use a USB to copy the file)



cracked.txt	9/3/2022 8:02 PM	Text Document	1 KB
crackme.rar	9/3/2022 7:55 PM	WinRAR archive	1 KB
example.dict	11/21/2021 8:43 PM	DICT File	1,045 KB
example0.cmd	11/21/2021 8:43 PM	Windows Comma...	1 KB
example0.hash	11/21/2021 8:43 PM	HASH File	210 KB
example0.sh	11/21/2021 8:43 PM	SH File	1 KB
example400.cmd	11/21/2021 8:43 PM	Windows Comma...	1 KB
example400.hash	11/21/2021 8:43 PM	HASH File	1 KB
example400.sh	11/21/2021 8:43 PM	SH File	1 KB
example500.cmd	11/21/2021 8:43 PM	Windows Comma...	1 KB
example500.hash	11/21/2021 8:43 PM	HASH File	1 KB
example500.sh	11/21/2021 8:43 PM	SH File	1 KB
hash_hc22000	8/7/2022 6:53 PM	HC22000 File	1 KB
hash.txt	9/24/2022 12:14 AM	Text Document	1 KB
hashcat.bin	11/21/2021 8:43 PM	BIN File	1,160 KB
hashcat.dictstat2	9/3/2022 8:02 PM	DICTSTAT2 File	1 KB
hashcat.exe	11/21/2021 8:43 PM	Application	1,201 KB

## Step- 7

- ❖ Open the Power shell and then use the command to crack the passwords

```
.\Hashcat.exe -m 1000 -a 0 -o cracked.txt hash.txt rockyou.txt
```

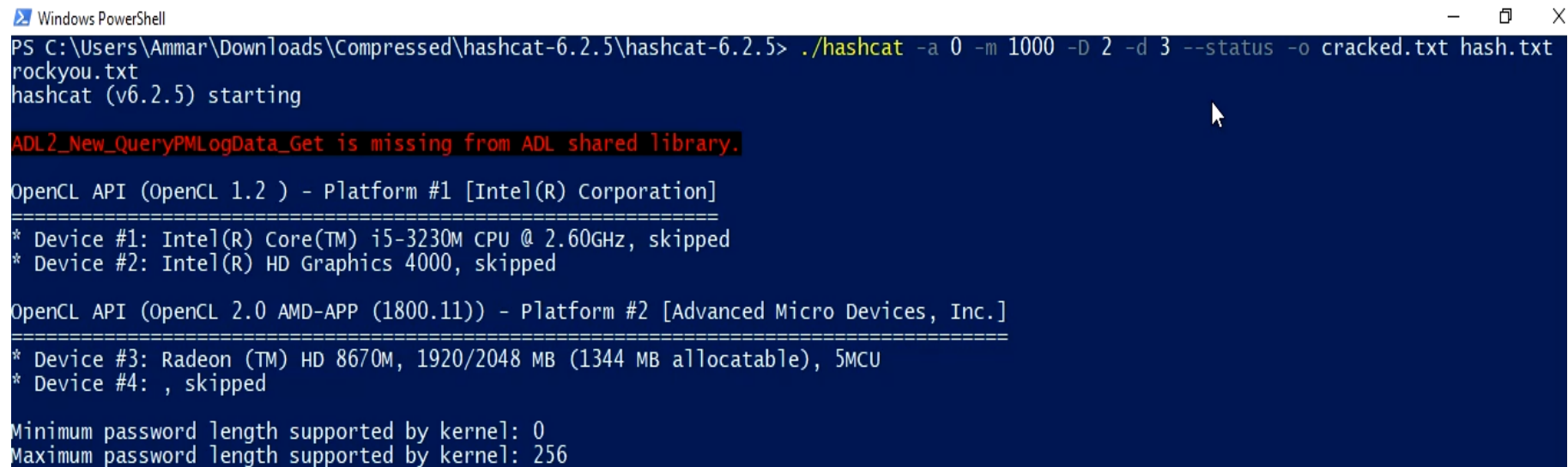
Here :

- 1000 tells the hashcat that its Windows password to be cracked
- Cracked.txt will store cracked passwords
- hash.txt is the source file
- Rockyou.txt is the dictionary file

## Step- 7

- ❖ Open the Power shell and then use the command to crack the passwords

```
.\Hashcat.exe -m 1000 -a 0 -o cracked.txt hash.txt rockyou.txt
```



```
Windows PowerShell
PS C:\Users\Ammar\Downloads\Compressed\hashcat-6.2.5\hashcat-6.2.5> ./hashcat -a 0 -m 1000 -D 2 -d 3 --status -o cracked.txt hash.txt
rockyou.txt
hashcat (v6.2.5) starting

ADL2_New_QueryPMLogData_Get is missing from ADL shared library.

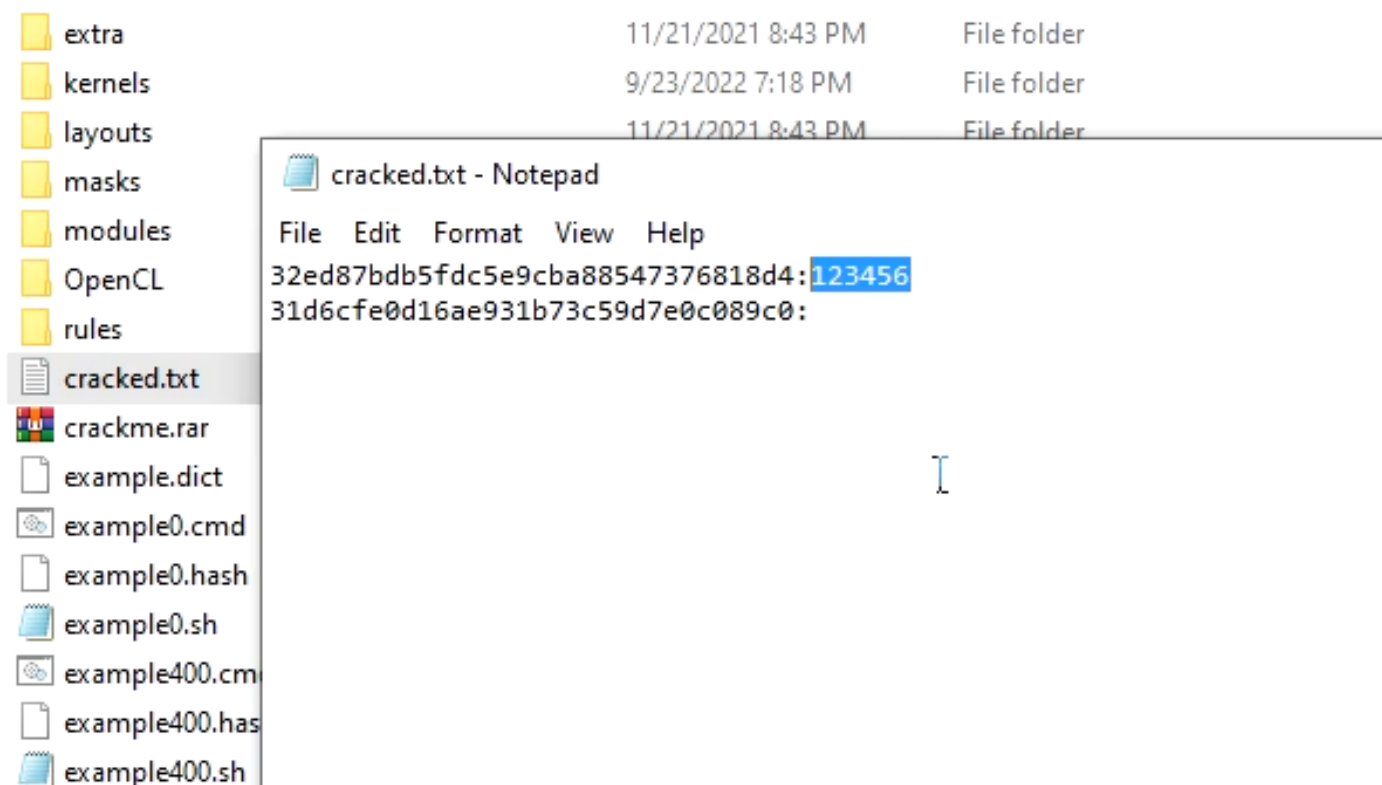
OpenCL API (OpenCL 1.2 ) - Platform #1 [Intel(R) Corporation]
=====
* Device #1: Intel(R) Core(TM) i5-3230M CPU @ 2.60GHz, skipped
* Device #2: Intel(R) HD Graphics 4000, skipped

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

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256
```

## Step- 8

- ❖ Open the cracked.txt file to view the cracked password





DEMO

## 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`



A photograph of a calm body of water with mountains in the background and a small structure on the right. The word 'THANKS' is overlaid in the center.

THANKS