**COMPUTER SUBJECT:** SECURITY AND CRACKING

**TYPE:** GROUP WORK EXERCISE/DISCUSSION

**IDENTIFICATION:** HASHCAT/MC

**COPYRIGHT:** *Michael Claudius*

**LEVEL:** INTERMEDIATE

**DURATION:** 30 - 90 minutes

**SIZE:** 10 lines!!

**OBJECTIVE:** Cracking passwords using GPU

**REQUIREMENTS: Network Security Essentials**

**COMMANDS:**

IDENTIFICATION: HASHCAT/MICL

Prolog

You have by now investigated password cracking using word-dictionary and brutal force.

The Mission

You are to explore the most powerful cracking program in the world named Hashcat, which is utilizing the GPU (Graphical Processor Unit) on the computer.

Purpose

The purpose is to learn the possibilities provided by Hashcat as a cracking tool.

*Useful links*

[www.hashcat.net](http://www.hashcat.net) Also link to Videos

[How to crack passwords using hashcat](https://www.youtube.com/watch?v=KnkjBW3fMVo)

Fine fast introduction to hashcat

[Cracking using graphic processors video](https://www.youtube.com/watch?v=7U-RbOKanYs&feature=youtu.be)
A rather talkative and too long introduction. Just watch minutes: 0-1, 3-6

[Crack WPA2 network](https://www.youtube.com/watch?v=lja8PfPXtmk)

Tutorial on a PMKID hashcat Attack

[How to use hashcat youtube video](https://www.youtube.com/watch?v=8fxLH-pokAI)
Instructions on hashcat, rather primitive and long

Assignment 1: Download hashcat

Go to [www.hashcat.net](http://www.hashcat.net) and you will see the following web-page:



Download the little older version v5.0.0 zip file.

Either as:

Hashcat binaries, which is a standard set-up that must match the operating system. Recommended for Windows

Or as:

Hashcat sources, which will be compiled on your computer,

Recommended for Unix/Linux and maybe Window VM on MAC

Find an appropriate directory and unzip the file to hashcat-5.0.0.

Then rename hashcat32.exe (if you are on a 32-bit machine) or rename hashcat64.exe (if you are on a 64-bit machine) as hashcat.exe.

Furthermore, create an empty text-file output.txt and a sub-dictionary named wordlist.

Assignment 2: Explore hashcat

Watch the video [How to crack passwords using hashcat](https://www.youtube.com/watch?v=KnkjBW3fMVo)

Open a command prompt and change directory to the hashcat directory (e.g: cd C:\hashcat-5.0.0)

Type:

hashcat

Use help command

hashcat –-help

and the home page to investigate the possibilities

* Options
* Attack types
* Hashing modes
* Char set
* Workload performance

And more….

Assignment 3: Cracking

In example0.hash a list of hashed passwords using MD5 are given.

Open a command prompt and change directory to the hashcat directory (e.g: cd C:\hashcat-5.0.0)

First make a copy of the file:

copy example0.hash myexample0.hash

as the hashes might be removed when cracked.

Secondly, we shall use brute force (option –a 3) and MD5 (option –m 0) for the cracking of passwords 6 characters long (?a?a?a?a?a?a).

Type:

hashcat -a 3 -m 0 example0.hash ?a?a?a?a?a?a

Hopefully you will see something like:



If there are problems with openCL then add option “--force”

hashcat -a 3 -m 0 example0.hash ?a?a?a?a?a?a

this will slow down the cracking speed, but you will get the feeling of hashcat.

Alternatively try to append the option “-0” to the commandline.

The cracked passwords might also be collected in the file hashcat.potfile. Take a look at the file or just use the command “type”.

Investigate and enjoy other commands.

Assignment 4: Your own cracker

Try to run hashcat on the hashed passwords from the mandatory assignment.

*Line exceptions !!*

THINK!

*Not cracking !!*

THINK !!

