

---

**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)

### Overview of commands

Rather helpful overview of the options by BeanBagKing !!

### Cracking using graphic processors video

A rather talkative and too long introduction. Just watch minutes: 0-1, 3-6

### How to use hashcat youtube video

Instructions on hashcat, rather primitive

### Assignment 1: Download hashcat

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

The screenshot shows the hashcat website interface. On the left is a navigation menu with links for hashcat, Forum, Wiki, Tools, Events, Converter, and Contact. The main content area features a 'Download' section with a table of binaries and sources, both at version v3.40 and signed with PGP. Below the table is a PGP signing key and a link to the GitHub repository. A 'GPU Driver requirements' section lists specific hardware and software needs for Windows and Linux users. A 'Features' section highlights that it is the world's fastest password cracker, has a unique in-kernel rule engine, is free, and is open-source under the MIT license.

Name	Version	Signature	Date
hashcat binaries	v3.40	PGP	2017.03.03
hashcat sources	v3.40	PGP	2017.03.03

Signing key on PGP keyserver: 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 users on Windows require "AMD Radeon Software Crimson Edition" (15.12 or later)
- AMD users on Linux require "AMDGPU-Pro Driver" (16.40 or later)
- Intel CPU users require "OpenCL Runtime for Intel Core and Intel Xeon Processors" (16.1.1 or later)
- Intel GPU on Windows users require "OpenCL Driver for Intel Iris and Intel HD Graphics"
- Intel GPU on Linux users require "OpenCL 2.0 GPU Driver Package for Linux" (2.0 or later)
- Nvidia users require "NVIDIA Driver" (367.x or later)

**Features**

- World's fastest password cracker
- World's first and only in-kernel rule engine
- Free
- Open-Source (MIT License)

Download the v6.2.6 zip file or newer version or an older version 5.x.x

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 and choose appropriate directory and unzip the file to hashcat-6.2.2.

If you see files hashcat32.exe or hashcat64.exe 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

Open a command prompt and change to the hashcat directory (e.g: cd C:\hashcat-6.2.6)

Type:

```
hashcat
```

Use help to investigate the possibilities

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

And more....

Notice the many versions of SHA from SHA1 to SHA512 with and without salt.

Also notice MD5 and Kerberos.

### Assignment 3: Cracking

Open a command prompt and change to the hashcat directory (e.g: cd C:\hashcat-6.2.6)

Type:

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

-a 3 is the bruteforce attack mode

-m 0 is the hash algorithm MD5 to be used

Investigate and enjoy some other commands.

### Assignment 4: Your own cracker

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

*Line exceptions !!*

THINK!