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

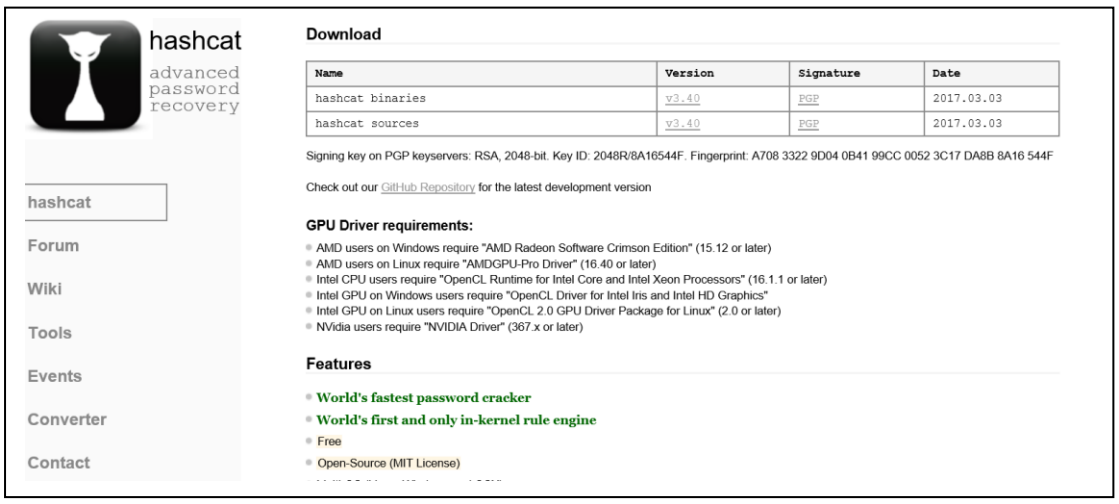
Overview of commands
Rather helpful overview of the options by BeanBagKing !!

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 and you will see the following web-page:



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

-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!