MONTGOMERY COLLEGE

#MCCYBERLAB | CYBERLAB RAPTORS | HT230

OBJECTIVE

Password Cracking Basics with Hashcat

MATERIALS

Download and Use a virtual machine from www.offensive-security.com

Challenge: Which directory is the rockyou wordlist located in Kali? These wordlists usually come with Kali. What other wordlists can you find online and use? Be sure to record the website.

ACTIVITY

PASSWORD CRACKING 2 • FILE LOCATION •
MC Cyber Center Website > Dropbox MCC PW > passwordcracking2.txt

Our officers have obtained password dumps storing hacker passwords. After obtaining a few plaintext passwords, it appears that they overlap with the passwords from the rockyou breach.

6w0rG07UK$Kr3gUfqksMZy4Zc.OeuIQdqXXBN0ReooVQRJrCcIlGmjBhN/PFcdVdJt0S5OjGiJ/yjcL.ht5qx197h6N1qIK/
a11c8694ddaa49e036807888e4f739e0
4a2c8813df066aba95359d5cb99a7dac
6b12ba85cf7c36202bf75ba53cd75d7f
0b2db70c8a0ed91a6968fc95c21e2556
078767cdd05b7e91b7375a76cf66736f

Clue: Use the rockyou wordlist in Kali. Can you locate it? Can you figure out how to unzip the file? What is the type of hash you are solving for? Is the first hash different from the rest of the hashes? If you use a wordlist, what method will you use for -a?
What is the command line you need to use with hashcat to get the answer?

Record your answer in a notebook and save it so you can refer back to it later!

SUBMIT YOUR ANSWER

HASHCAT COMMAND LINE • NOTES • EXPLANATION

Submit your answers to *mccyberlab@gmail.com*, include your name, student email address, name of the activity/question solved, how you obtained your answer, and your answers