OBJECTIVE

Password Cracking Basics with Hashcat

MATERIALS

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

Challenge: Do your own experiment and test. Which Windows operating systems are vulnerable to a SAM file dump? Have you tried Windows XP, Windows 7? What are the safeguards that are in place to prevent a user from obtaining the SAM file?

ACTIVITY

PASSWORD CRACKING 3 • FILE LOCATION•
MC Cyber Center Website > Dropbox MCC PW > passwordcracking3.txt

You have been locked out of your Windows XP machine but have been able to obtain the SAM dump password file. Can you crack the passwords and regain access to your machine?

```
B3919785373DA815AAD3B435B51404EE:E442EBE705AA9B36B719FDEFE573A6E8
A9598B0FA8F0685BAAD3B435B51404EE:129FA8BB2B780B124C5A9378A0D78BF5
5954DE905DF0EBDE4A3B108F3FA6CB6D:38F0AB0B3D1A01871CC2AE0230486A24
48C1987667531D5E4A3B108F3FA6CB6D:1BDC1CC085859563FC70D3FE5F0FC520
96C4705B18D466AFAAD3B435B51404EE:F575FBDCC88DCDEA79A90033ACF86B06
```

1. What is the format of the hash above?
2. Notice there is a colon. Which half is the LM hash? Which half is the NTLM hash?
3. What is the length of each of the hashes (separated by the colon)?
4. Is LM case sensitive? Is NTLM case sensitive?
5. What is the hash code for hashcat mode for LM?
6. What is the hash code for hashcat mode for NTLM?

Clue: Use the rockyou wordlist in Kali. Can you locate it? Can you figure out how to unzip the file? 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