Lab 10 – Security – Password Cracking with Hashcat

By

Lukas Fuller

IAE-201-D02

IA-201: Introduction to Information Assurance

**Abstract**

The objective of this lab is to introduce students to password cracking and the Hashcat program. The students will understand the differences between password types and how to secure passwords. The student will be able to use Hashcat to crack simple passwords.

**Materials**

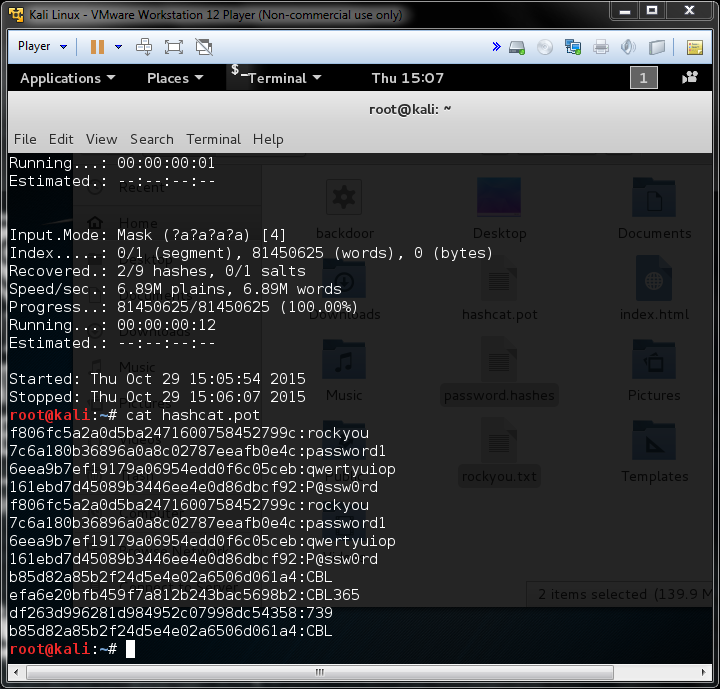
1. Kali Linux Virtual Machine
2. plaintext.txt file
3. password.hashes file

**Conclusion**

I somewhat understand how password-cracking works with hashcat, and I do feel comfortable with using it. However, I’m not too certain on what makes up the different rules for cracking passwords, as indicated by the last two questions unanswered. I searched online, but I’m not entirely sure what is meant by it. Regardless, besides that area, I feel like I have learned more about the importance of having different passwords for each account, and making sure that I have a password over probably 10 characters if possible (because 6 didn’t take too long to crack). Overall I feel like I understand how to use hashcat, just that one area is a little fuzzy to me.

**Screenshots**

1. Screenshot of the hashcat.pot file with 6 passwords cracked.



**Questions:**

1. What is Hashcat? **A password cracking program**
2. What is a hash? **The character used as a placeholder for a certain amount of data**
3. What is a password dictionary? **A list of known weaknesses or leaked passwords**
4. What is the most secure of the following: MD5, SHA-1, SHA-256, or SHA-512? **SHA-512**
5. Why is it important to pick a complex password? Answer with respect to what we have learned in this lab. **To prevent easy password cracking, longer password means more security**
6. Why is it important to not reuse passwords? Answer with respect to what we have learned in this lab. **If you have account hacked and you use that password on multiple accounts, the attacker won’t have to crack any more of your passwords and can use it for all of your accounts with that password**
7. What is a dictionary attack? **An attack that goes through known leaded or weak passwords**
8. What is a combinational attack? **It will combine two dictionaries and every possible combination between the two**
9. What is a brute force attack? **Using a pattern and every possible form of that pattern**
10. Form a Hashcat rule for the following password: Inf0S3c
11. Form a Hashcat rule for the following password: $up3r$3cur3