Lab - Challenge Passwords with Kali Tools

1. Objectives

In this lab, you will explore tools that are available in the Kali VM to challenge passwords.

Part 1: Using Hashcat to Challenge Passwords

Part 2: Investigating Other Password Challenging Tools on Kali Linux

1. Background / Scenario

There are numerous Kali tools used to challenge passwords. It is very likely you have already seen and/or used John the Ripper (john). John is a very powerful tool, but there are other tools that might be more appropriate to use depending on the situation. It is very important to be aware of as many tools as possible so you can select the most appropriate tool for the task at hand.

Hashcat is a very powerful password challenging tool that offers different features and has other advantages in comparison to John the Ripper that you might find helpful to know how to use. Hashcat is an offline password cracking tool that is claimed to be the world’s fastest CPU-based password recovery tool. It offers various attack modes including dictionary, brute force, and combination attack. For the purposes of this lab, we will use the combination attack based on the available information. We will be using a combination attack to recover the password for a serious golf fan.

1. Required Resources

* PC with IoTSec Kali VM installed
* Internet connection

1. Using Hashcat to Challenge Passwords
   * 1. Set up the environment and open a terminal window.
        1. Start the IoT Security lab topology with Kali VM. Log into Kali VM with the username **root** and password **toor**.
        2. Open a terminal on the Kali VM.
        3. Create a directory called passwordlab:

root@kali:~# **mkdir passwordlab**

* + - 1. Move into this directory:

root@kali:~# **cd passwordlab**

* + 1. Create the necessary dictionary files and MD5 hash file.

A MD5 hash value has been recovered for a user, and it is your job to crack this value. Rather than using a brute force method that could take a long time, you will be using known information to crack this value much quicker. The user is a golf fan and has specifically talked about Tiger Woods. In addition, it was discovered from one of his social media public profiles that he graduated in 2002.

It is very typical for users to create passwords using words from their special interests or hobbies. When their special interests are known, wordlists can be very helpful in recovering passwords or cracking hashes. There are numerous sites out that provide wordlists for a wide variety of interests. For example:

<https://packetstormsecurity.com/Crackers/wordlists/>

This site provides a golfers.gz file that contains a list of golf names/words that can be used for a wordlist. It is also known that users will usually take a name and make the password more complicated by either repeating the name or word and/or adding numbers or special characters to it.

The following MD5 hash value was provided to you by a known golf fan, and it is your job to crack it:

22bb33653af9cc8f21d71fa0e55751b4

MD5 hash values are hexadecimal characters. Hexadecimal characters are alphanumeric from a to f and numeric values from 0 through 9.

For the purposes of this lab, and time constraint issues, we will create our own dictionaries and use just a few words per dictionary.

* + - 1. Create a dictionary file using multiple combinations of “tiger woods”:

root@kali:~/passwordlab# **echo “tiger woods” > dict1.txt**

root@kali:~/passwordlab# **echo “tiger” >> dict1.txt**

root@kali:~/passwordlab# **echo “woods” >> dict1.txt**

root@kali:~/passwordlab# **echo “golf” >> dict1.txt**

root@kali:~/passwordlab# **more dict1.txt**

**Text

Description automatically generated**

* + - 1. The second dictionary file we will create will be the file that Hashcat will run the various combinations with. It is very common for users to combine numbers with their passwords in order to make them longer and minimum length requirements.

root@kali:~/passwordlab# **echo “0” > dict2.txt**

root@kali:~/passwordlab# **echo “1” >> dict2.txt**

root@kali:~/passwordlab# **echo “2” >> dict2.txt**

root@kali:~/passwordlab# **echo “2002” >> dict2.txt**

root@kali:~/passwordlab# **echo “02” >> dict2.txt**

root@kali:~/passwordlab# **more dict2.txt**

**Text

Description automatically generated**

* + - 1. Save the md5 hash value into a text file called hash.txt:

root@kali:~/passwordlab# **echo "22bb33653af9cc8f21d71fa0e55751b4" > hash.txt**

**A picture containing text

Description automatically generated**

* + - 1. If there are any typos with the hash when entering it, the lab will not work.

What command did you use to view the content in the file **hash.txt**? more hash.txt

* + 1. Crack a known MD5 hash value using Hashcat.
       1. Use the man pages for hashcat to answer the following questions:

root@kali:~/passwordlab# **man hashcat**

What command should be used for an MD5 hash? hashcat -m 0

What command should be used for the attack mode of combination? hashcat -a 1

* + - 1. The --force option below is required because you are running this on a virtual image.

root@kali:~/passwordlab# h**ashcat –m 0 –a 1 –-force hash.txt dict1.txt dict2.txt**

**Note**: If you want to run this again with the same hash value, use the **--potfile-disable** option:

root@kali:~/passwordlab# **hashcat –m 0 –a 1 –-force hash.txt dict1.txt dict2.txt --potfile-disable**

Text

Description automatically generated

* + - 1. Review the output from this command .
      2. To view the saved passwords from the hash.txt file use the following command:

root@kali:~/passwordlab# **hashcat –-show hash.txt**

Text

Description automatically generated

1. Investigating Other Password Challenging Tools on Kali Linux

In the previous part, you have learned to use a very powerful password cracking tool. There are a wide variety of other tools that could be useful in addition to John the Ripper (john) and Hashcat.

Perform a web search to research the answers to the following questions.

* 1. In the previous part, you were provided a hash value to crack. You were told that it was an MD5 hash value and when you entered the command **hashcat**, you used the value of **-m 0** to indicate that it was an MD5 value. What if you did not know whether it was an MD5 or SHA1 value?

What tool can be used to determine what type of hash a particular hash value is?

hash-identifier

* 1. One of the commands that can identify the hash type is **hash-identifier**. Enter the command at the prompt:

root@kali:~# **hash-identifier**

When prompted, enter the MD5 hash value from the previous part: **22bb33653af9cc8f21d71fa0e55751b4**

What was the possible hash value that was identified through the hash-identifier tool? MD5

* 1. What Kali Linux password cracking tool can be used to crack Windows passwords using rainbow tables?

Ophcrack

* 1. What Kali Linux password cracking tool can be used to retrieve the syskey and extract Windows password hashes from Windows?

samdump2