# Password Cracking with Hashcat Lab

## Introduction

In this lab, you will learn how to use Hashcat, a powerful password recovery tool, to crack password hashes. Hashcat supports many hash types and comes with various attack modes. This exercise will give you practical experience with password cracking techniques in a controlled environment.

## Objectives

* Understand how to use Hashcat to crack password hashes.
* Learn about different hash types and Hashcat attack modes.

## Prerequisites

* Basic knowledge of command line interface (CLI) usage.
* Access to a computer with Kali Linux installed.

## Required Tools

* Kali Linux
* Hashcat (pre-installed on Kali Linux)

## Lab Setup

1. **Start your Kali Linux environment.** Ensure that you have administrative access.
2. **Open your terminal.** You will perform most of the tasks in this terminal.

## Lab Tasks

### Task 1: Identifying the Hash Type

Before you can begin cracking a hash, you need to identify what type of hash it is. Use the hash-identifier tool that comes with Kali Linux or refer to online resources to identify your hash type.

**Example Command:**

hash-identifier 5f4dcc3b5aa765d61d8327deb882cf99

### Task 2: Prepare a Password List

For successful password cracking with Hashcat, you will need a list of potential passwords, commonly referred to as a “wordlist.” Kali Linux comes equipped with several wordlists, including the widely used rockyou.txt.

**Steps to prepare your password list:**

1. **Locate the Wordlist:** Kali Linux stores its wordlists in the /usr/share/wordlists/ directory. For this task, we will use rockyou.txt, which is a comprehensive list of commonly used passwords.

* **Command to locate rockyou.txt:**
* ls /usr/share/wordlists/

1. Is the file there? You should see something like this:

* ┌──(kali㉿kali)-[~]  
  └─$ ls /usr/share/wordlists -lh  
  total 51M  
  lrwxrwxrwx 1 root root 26 Mar 25 10:18 amass -> /usr/share/amass/wordlists  
  lrwxrwxrwx 1 root root 25 Mar 25 10:18 dirb -> /usr/share/dirb/wordlists  
  lrwxrwxrwx 1 root root 30 Mar 25 10:18 dirbuster -> /usr/share/dirbuster/wordlists  
  lrwxrwxrwx 1 root root 35 Mar 25 10:18 dnsmap.txt -> /usr/share/dnsmap/wordlist\_TLAs.txt  
  lrwxrwxrwx 1 root root 41 Mar 25 10:18 fasttrack.txt -> /usr/share/set/src/fasttrack/wordlist.txt  
  lrwxrwxrwx 1 root root 45 Mar 25 10:18 fern-wifi -> /usr/share/fern-wifi-cracker/extras/wordlists  
  lrwxrwxrwx 1 root root 28 Mar 25 10:18 john.lst -> /usr/share/john/password.lst  
  lrwxrwxrwx 1 root root 27 Mar 25 10:18 legion -> /usr/share/legion/wordlists  
  lrwxrwxrwx 1 root root 46 Mar 25 10:18 metasploit -> /usr/share/metasploit-framework/data/wordlists  
  lrwxrwxrwx 1 root root 41 Mar 25 10:18 nmap.lst -> /usr/share/nmap/nselib/data/passwords.lst  
  -rw-r--r-- 1 root root 51M May 12 2023 rockyou.txt.gz  
  lrwxrwxrwx 1 root root 39 Mar 25 10:18 sqlmap.txt -> /usr/share/sqlmap/data/txt/wordlist.txt  
  lrwxrwxrwx 1 root root 25 Mar 25 10:18 wfuzz -> /usr/share/wfuzz/wordlist  
  lrwxrwxrwx 1 root root 37 Mar 25 10:18 wifite.txt -> /usr/share/dict/wordlist-probable.txt

1. You need to decompress it:

* sudo gzip -d /usr/share/wordlists/rockyou.txt.gz  
   ```  
    
  Note: If the file is already decompressed, this step can be skipped. You can check if it exists in uncompressed form by using the ls command.  
  After decompressing the file, ensure it is ready for use by checking its content.  
  ```bash  
  head /usr/share/wordlists/rockyou.txt

### Task 3: Cracking the Hash

Now that you have identified the type of hash and prepared a wordlist, you’re ready to use Hashcat to attempt to crack the hash. Follow the steps below to properly configure and execute Hashcat.

#### Step 1: Prepare the Hash File

To begin, you’ll need to place the hash you want to crack into a text file. Make sure the hash format is compatible with the hash type you identified in Task 1.

**Example Command to Create a Hash File:**

echo "5f4dcc3b5aa765d61d8327deb882cf99" > hash.txt

### Step 2: Choose the Right Hashcat Mode

Identifying the correct mode is crucial for effectively using Hashcat to crack a hash. Hashcat modes are specific to the type of hash you are dealing with. The mode tells Hashcat how to properly interpret the hash and what algorithm to use for cracking it.

**How to Choose the Mode:**

1. **Refer to Hashcat’s Mode List:** Hashcat documentation provides a complete list of modes for va
2. \*\*Identify your hash type Recall the hash type you identified in Task 1. Use this information to find the corresponding mode in the Hashcat list.

hashcat --help | grep -i md5

The output will show the mode number for MD5 hashes, typically 0. This mode number is what you will use in the Hashcat command to crack the MD5 hash. Once you have identified the correct mode number from the list, note it down as you will need to specify this mode in your Hashcat command line to ensure that Hashcat processes the hash correctly.

#### Crack it!

If you are cracking an MD5 has, you should use mode 0. Your hashcat command will look like this:

hashcat -m 0 hash.txt /usr/share/wordlists/rockyou.txt