

Laboratory_04: Hashcat

This laboratory covers how to use Hashcat to crack MD5 hashes efficiently.

Installation

- `sudo apt update`
- `sudo apt install hashcat`
- Clone a dictionary git clone [dw0rsec/rockyou.txt](https://github.com/dw0rsec/rockyou.txt): `rockyou.txt wordlist`

Basic Hashcat Usage for MD5

1. The basic syntax for cracking MD5 hashes with Hashcat is:
 - a. `hashcat -m 0 -a [attack_mode] [hash_file] [wordlist/mask]`
 1. e.g.: `hashcat -m 0 -a 0 target_hash.txt rockyou.txt/rockyou.txt --force`

Where:

1. `-m 0` specifies MD5 hash type
2. `-a [attack_mode]` specifies the attack type (0 = dictionary, 3 = brute force/mask, etc.)
3. `[hash_file]` is a file containing hashes to crack (one per line)
4. `[wordlist/mask]` is either a wordlist file or a pattern mask

Dictionary Attack

1. Dictionary attacks try passwords from a wordlist file:
 - a. MD5
 - i. `echo "5f4dcc3b5aa765d61d8327deb882cf99" > target_hash.txt`
 - ii. `hashcat -m 0 -a 0 target_hash.txt /path/to/wordlist.txt`
 - b. SHA-1
 - i. `echo "b2e98ad6f6eb8508dd6a14cfa704bad7f05f6fb1" > target_hash.txt`
 - ii. `hashcat -m 100 -a 0 target_hash.txt rockyou.txt/rockyou.txt --force`

Brute Force (Mask Attack)

1. For short passwords or when the pattern is known:

a. MD5

i. `hashcat -m 0 -a 3 target_hash.txt ?l?l?l?l?l --force -show`

b. SHA-1

i. `hashcat -m 100 -a 3 target_hash.txt ?l?l?l?l?l --force -show`

Common mask placeholders:

- `?l` = lowercase (a-z)
- `?u` = uppercase (A-Z)
- `?d` = digits (0-9)
- `?s` = special characters (!@#\$...)
- `?a` = all characters