‹ Dashboard

BASICS
Hashes

Password hashing is the process of passing a plaintext password to a one-way function (hash function) that generates a hexadecimal string of a fixed length called a password hash. This function is chosen in such a manner that getting a hash from a plaintext password is very efficient while recovering the plaintext password from the hash is very difficult. Hence, the name “one-way function”. Password hashing serves as the last defense against the attacker because, even after getting his hands on the username and password hashes, the attacker still has to recover the plaintext passwords in order to use the credentials. In these labs, various types of hashes are provided along with the Hashcat tool. The user has to crack the given hash and recover the plaintext password.

What will you learn?

- Cracking hashes with Hashcat using a dictionary and mask-based brute-force attacks.

References:

1. Hashcat (https://hashcat.net/hashcat/)

Labs Covered:

- Cracking MD5 Hashes
  Crack MD5 hashes by launching a mask-based brute-force attack with Hashcat.

- Cracking Salted MD5 Hashes
  Crack salted MD5 hashes by launching a dictionary attack with Hashcat.

- Cracking HMAC-SHA1 key
  Crack the key for HMAC-SHA1 digest by launching a dictionary attack with Hashcat.

- Cracking CRC32s
  Crack CRC32 hashes by launching a dictionary attack with Hashcat.

- Cracking SHA-1 Hashes
  Crack SHA-3 hashes by launching a dictionary attack with Hashcat.

- Cracking SHA-2 Digests
  Crack SHA-2 hashes by launching a mask-based brute-force attack with Hashcat.

- Cracking SHA-3 Digests
  Crack SHA-3 hashes by launching a dictionary attack with Hashcat.

- Cracking NTLM Hashes
  Crack NTLM hashes by launching a mask-based brute-force attack with Hashcat.

Cracking MD5 Hashes

Start

Cracking Salted MD5 Hashes

Start

Cracking HMAC-SHA1 key

Start

Cracking CRC32s

Start

Cracking SHA-1 Hashes

Start

Cracking SHA-2 Digests

Start

Cracking SHA-3 Digests

Start

Cracking NTLM Hashes

Start