findmyhash Package Description

Accepted algorithms are:

- MD4 – RFC 1320

- MD5 – RFC 1321

- SHA1 – RFC 3174 (FIPS 180-3)

- SHA224 – RFC 3874 (FIPS 180-3)

- SHA256 – FIPS 180-3

- SHA384 – FIPS 180-3

- SHA512 – FIPS 180-3

- RMD160 – RFC 2857

- GOST – RFC 583

- WHIRLPOOL – ISO/IEC 10118-3:2004

- LM – Microsoft Windows hash NTLM – Microsoft Windows hash

- MYSQL – MySQL 3, 4, 5 hash

- CISCO7 – Cisco IOS type 7 encrypted passwords

- JUNIPER – Juniper Networks 9 encrypted passwords

- LDAP_MD5 – MD5 Base64 encoded

- LDAP_SHA1 – SHA1 Base64 encoded

Source: https://code.google.com/p/findmyhash/
findmyhash Homepage | Kali findmyhash Repo

- Author: JulGor

- License: GPLv3

Tools included in the findmyhash package

findmyhash – Crack hashes with online services

root@kali:~# findmyhash
/usr/bin/findmyhash 1.1.2 (http://code.google.com/p/findmyhash/)

Usage:

------

python /usr/bin/findmyhash <algorithm> OPTIONS

Accepted algorithms are:

  MD4   - RFC 1320
  MD5   - RFC 1321
  SHA1   - RFC 3174 (FIPS 180-3)
  SHA224   - RFC 3874 (FIPS 180-3)
  SHA256   - FIPS 180-3
  SHA384   - FIPS 180-3
  SHA512   - FIPS 180-3
  RMD160   - RFC 2857
  GOST   - RFC 5831
  WHIRLPOOL - ISO/IEC 10118-3:2004
  LM   - Microsoft Windows hash
  NTLM   - Microsoft Windows hash
  MYSQL   - MySQL 3, 4, 5 hash
  CISCO7   - Cisco IOS type 7 encrypted passwords
  JUNIPER   - Juniper Networks 9 encrypted passwords
  LDAP_MD5 - MD5 Base64 encoded
  LDAP_SHA1 - SHA1 Base64 encoded

  NOTE: for LM / NTLM it is recommended to introduce both values with this format:
      python /usr/bin/findmyhash LM   -h 9a5760252b7455deaad3b435b51404ee:0d7f1f2bdeac6e574d6e18ca85fb58a7
      python /usr/bin/findmyhash NTLM -h 9a5760252b7455deaad3b435b51404ee:0d7f1f2bdeac6e574d6e18ca85fb58a7

Valid OPTIONS are:

 -h <hash_value> If you only want to crack one hash, specify its value with this option.

 -f <file>   If you have several hashes, you can specify a file with one hash per line.
          NOTE: All of them have to be the same type.

 -g   If your hash cannot be cracked, search it in Google and show all the results.
          NOTE: This option ONLY works with -h (one hash input) option.

Examples:

  -> Try to crack only one hash.
     python /usr/bin/findmyhash MD5 -h 098f6bcd4621d373cade4e832627b4f6

  -> Try to crack a JUNIPER encrypted password escaping special characters.
     python /usr/bin/findmyhash JUNIPER -h "\$9\$LbHX-wg4Z"

  -> If the hash cannot be cracked, it will be searched in Google.
     python /usr/bin/findmyhash LDAP_SHA1 -h "{SHA}cRDtpNCeBiql5KOQsKVyrA0sAiA=" -g

  -> Try to crack multiple hashes using a file (one hash per line).
     python /usr/bin/findmyhash MYSQL -f mysqlhashesfile.txt

Contact:

[Web]   http://laxmarcaellugar.blogspot.com/
[Mail/Google+] bloglaxmarcaellugar@gmail.com
[twitter]   @laXmarcaellugar

findmyhash Usage Example

Specifying the hash algorithm *(MD5)*, attempt to crack the given hash *(-h 098f6bcd4621d373cade4e832627b4f6)*:

root@kali:~# findmyhash MD5 -h 098f6bcd4621d373cade4e832627b4f6

Cracking hash: 098f6bcd4621d373cade4e832627b4f6

Analyzing with md5online (http://md5online.net)...

***** HASH CRACKED!! *****
The original string is: test

The following hashes were cracked:

  098f6bcd4621d373cade4e832627b4f6 -> test

Become a Certified Penetration Tester

Enroll in Penetration Testing with Kali Linux, the course required to become an Offensive Security Certified Professional (OSCP)