Password Cracking

Hash 100

Ihre Aufgabe besteht darin, die folgenden Hashwerte zu knacken. Als Hashfunktion wird MD5 eingesetzt.

- Für das Cracken von einfachen Passwörtern verwendet man Hashcat mit den Startoptionen:
  1. -a 3 (Bruteforce Attack)
  2. -m 0 (MD5 Hashes)
  3. -o ./found100.txt (Output File)
  4. ./hash100.txt (Hash File)

    - hashcat -a 3 -m 0 -o ./found100.txt ./hash100.txt --force

MD5 Hashwert	Passwort
a4757d7419ff3b48e92e90596f0e7548	god
5ebe2294ecd0e0f08eab7690d2a6ee69	secret
b5c0b187fe309af0f4d35982fd961d7e	love
3c3662bcb661d6de679c636744c66b62	sex

Hash 200

Ihre Aufgabe besteht darin, die folgenden Hashwerte zu knacken. Als Hashfunktion wird MD5 eingesetzt. Salt wird nicht verwendet. Benutzen Sie dafür die Wortliste rockyou.txt. Bei Kali wird diese komprimiert mitgeliefert und kann mit folgendem Befehl in das HOME-Verzeichnis entpackt werden:

- zcat /usr/share/wordlists/rockyou.txt.gz > ~/rockyou.txt

- Für das Cracken von umfangreicheren Passwörtern verwendet man die Parameter:
  1. -a 0 (Dictionary Attack)
  2. -m 0 (MD5 Hashes)
  3. -o ./found200.txt (Output File)
  4. ./hash200.txt (Hash File)
  5. ./rockyou.txt (Dictionary File)

    - hashcat -a 0 -m 0 -o ./found200.txt ./hash200.txt ./rockyou.txt --force

MD5 Hashwert	Passwort
a5d36c7f6054f02e44f2c2d8da648f45	rangers280271
3b1040e285e367908c5589efe259456a	6plutonium9
28c1050a9208e13a6d72b7fa214203de	julzrulz01
05e33c4824b0ab78734c50f4d0d14f6c	liverpoolrulez

Hash 300

Ihre Aufgabe besteht darin, die folgenden Hashwerte zu knacken. Als Hashfunktion wird MD5 eingesetzt. Salt wird nicht verwendet. Die Passwörter bestehen aus jeweils 6 Zeichen, welche Kleinbuchstaben oder Ziffern sein können.

- Für Passwörtern mit bekanntem, einfachem Muster verwendet man die Startparameter:
  1. -a 3 (Bruteforce Attack)
  2. -m 0 (MD5 Hashes)
  3. -o ./found300.txt (Output File)
  4. ./hash300.txt (Hash File)
  5. ?h?h?h?h?h?h (Mask: h = lowercase + digits)

    - hashcat -a 3 -m 0 -o ./found300.txt ./hash300.txt ?h?h?h?h?h?h --force

MD5 Hashwert	Passwort
a5d36c7f6054f02e44f2c2d8da648f45	uudem5
3b1040e285e367908c5589efe259456a	au9dee
28c1050a9208e13a6d72b7fa214203de	aimee5
05e33c4824b0ab78734c50f4d0d14f6c	pooy5u

(26+10)^6 = 2176782336 Möglichkeiten

Hash 400

Ihre Aufgabe besteht darin, die folgenden Hashwerte zu knacken. Als Hashfunktion wird MD5 eingesetzt. Salt wird nicht verwendet. Die Passwörter bestehen aus jeweils 7 Zeichen, welche Kleinbuchstaben oder Großbuchstaben sein können. Das Knacken könnte mehrere Stunden dauern.

- Für Passwörter mit bekanntem, umfangreichem Muster verwendet man die Parameter:
  1. -a 3 (Bruteforce Attack)
  2. -m 0 (MD5 Hashes)
  3. -o ./found400.txt (Output File)
  4. ./hash400.txt (Hash File)
  5. -1 ?u?l ?1?1?1?1?1?1?1 (Mask: 1 = lowercase + uppercase)

    - hashcat -a 3 -m 0 -o ./found400.txt ./hash400.txt -1 ?u?l ?1?1?1?1?1?1?1 --force

MD5 Hashwert	Passwort
04c6f2b543295d713bc6c2880fb0bb9e	EueDiva
481f9fa6053b5a05b7f1ed58099dc664	SsQESIX
800a6f838cf54681d1e755abaf30a1b2	scPEZjK

(26+26)^7 = 1028071702528 Möglichkeiten (Via NVIDIA GTX960 ~3:00min)