Erledigt .dmg Image - das PASSWORT KNACKEN

Beitrag von „Leo Duke“ vom 31. März 2019, 20:59

Hallo an alle,

hat jemand von Euch das Passwort eines verschlüsselten .dmg Images schon geknackt?
Falls ja, bitte um Belehrung, also womit und wie wäre es sehr nett, thx.

Beitrag von „rubenszy“ vom 31. März 2019, 21:12

DMG aus dem Netz gezogen und kein PW dazu 🤔😉

Beitrag von „derHackfan“ vom 31. März 2019, 21:17

Ich weiß gar nicht ob solche Informationen bezüglich dem Knacken von Passwörtern und ein Hilfe bei irgendeiner .dmg aus dem Netz im Sinn der Forenregeln und im Interesse des Forum sind.

Beitrag von „umax1980“ vom 31. März 2019, 21:18

Ich denke, bei beiden Anfragen sind wir raus.

Kannst du bestimmt verstehen....

Beitrag von „griven“ vom 31. März 2019, 21:21

Da gibt es eigentlich nichts raus zu sein

Die Antwort auf die Frage ist einfach denn mal abgesehen von BruteForce gibt es keine Möglichkeit da es sich dabei ja um verschlüsselte Images handelt die ohne Passphrase (Hash) nun mal nicht zu entschlüsseln sind. Je nachdem wie komplex das PW ist kann BruteForce klappen oder eben auch nicht.

Beitrag von „Leo Duke“ vom 31. März 2019, 21:23

rubenszy
... nein, es ist mein altes Image mit alten wichtigen unterlagen.
Da ich das Image schon seit längerer Zeit nicht mehr benutzte, komme ich leider nicht rein.

derHackfan
Ich denke, nicht nur ich -hier im Forum- würde es gerne wissen.

umax1980
Warum? - verstehe ich nicht.

griven
... danke

Beitrag von „DonBronko“ vom 31. März 2019, 21:42

Vielleicht hilft dir das.

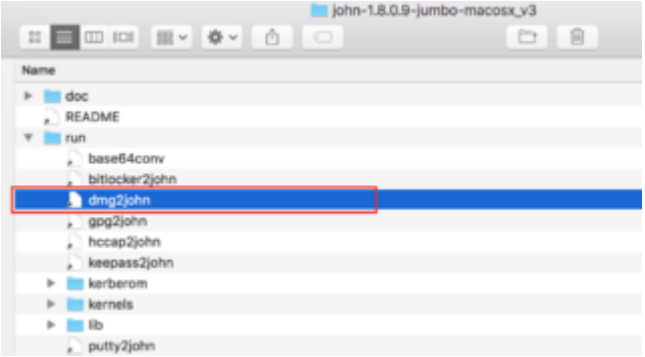
Damit hatte ich mal erfolgreich geschafft mein vergessenes Passwort für eine rar zu entschlüsseln.

Beitrag von „rubenszy“ vom 31. März 2019, 21:42

Es gibt zwei Methoden BruteForce dafür musst du aber wissen wie viel Zeichen das PW hat, ab 8 Zeichen wird es lustig, ab 10 geht es in Monate und ab 12 kannst du dir ausmalen wie lang dein Rechner läuft.

Die Hash Variante geht schneller aber leider hast du keine Nvidia Karte dann lohnt sich bei dir Hashcat nicht wirklich, dann musst du John the Ripper nehmen.

Nimmst das Viodeo von Quipper als Vorlage und statt zip2John ist es halt dann



Laden kannst du dir das tool halt hier https://openwall.info/wiki/joh...lds#Compiled-for-Mac-OS-X

Beitrag von „Leo Duke“ vom 31. März 2019, 21:58

DonBronko rubenszy
danke, Bros 👍 werde berichten 😎

Beitrag von „rubenszy“ vom 31. März 2019, 22:20

Deine CPU wird ordentlich was zu tun haben, die wird so extrem ausgelastet wie mit Prime95, schneller würde es mit Nvida gehen.

Beitrag von „Leo Duke“ vom 31. März 2019, 22:30

... Nvida oder meinst Du eine Nvidia Graka?

Beitrag von „LordSea“ vom 31. März 2019, 22:31

Nvidia Graka

Damit is es schneller

Beitrag von „rubenszy“ vom 31. März 2019, 22:31

Nimm Hashcat https://hashcat.net/hashcat/ kann jetzt auch AMD GPU's nutzen unter OpenCL

Beitrag von „Leo Duke“ vom 31. März 2019, 22:34

Okay, meine Herren

Beitrag von „griven“ vom 31. März 2019, 22:39

Er meint die Grafikkarten von NVIDIA die man zum berechnen nutzen könnte wobei ich

bewusst sage könnte

DMG Images sind mindestens mit 128 Bit-AES verschlüsselt wenn es doof läuft sogar mit 256 Bit-AES und beides wirst Du weder mit Deiner CPU noch mit einer NVIDIA Karte knacken können. Ich würde die Daten abschreiben oder scharf nachdenken ob mir die Passphrase nicht doch noch einfällt

---

Beitrag von „Patricksworld“ vom 1. April 2019, 17:18

> Zitat von griven
>
> oder scharf nachdenken ob mir die Passphrase nicht doch noch einfällt

Das würde ich auch machen. Und wenn dir Leo Duke auch nur teilweise Sachen einfallen wird dein Projekt vielleicht sogar machbar.

Also wenn du ungefähr weißt wieviele Zeichen du hattest ist das schon einmal ein Vorteil. Wenn du weißt welche Buchstaben oder zumindest ob nur Groß oder Kleinschreibung im Einsatz war, dann ist das auch ein Anfang. Rund um. Wenn du z.B. ein Standartpasswort häufig benutzt und nur etwas abwandelst, dann kann das schon gut machbar werden. Dann kannst du dir eine Wordlist z.B. mit crunch erstellen und die dann anwenden.

Ohne Dem, wird es wohl schwierig bis eher unmöglich. Dann bleibt dir nur darauf zu warten, bis die Verschlüsselung einmal geknackt wird und eine generelle Lücke aufweist. Oder du wartest darauf das man Quantencomputer anmieten kann. Dann dürfte das auch recht flott gehen.

Beitrag von „DSM2“ vom 1. April 2019, 17:28

Und wie weit ist dein Rechner Leo Duke ?

Beitrag von „rubenszy“ vom 1. April 2019, 17:35

Warten wir mal ab wie lange er mit Hashcat brauch, eine GPU+CPU braucht schon eine Weile

Mein WS AMD CPU 32/64 + 2x GTX 1070 TI hat gestern für ein 10 Zeichen PW, nur Buchstaben (groß und klein) + Zahlen 8 Stunden gebraucht und das bei voller Auslastung

Ich hoffe man nicht das er Sonderzeichen mit drin hat, dann zieht es sich richtig.

Beitrag von „griven“ vom 1. April 2019, 22:27

So meine Lieben bevor das ganze hier noch ausufert und sich durch die Tipps die hier gegeben werden am Ende noch der Soundflower Effekt einschleicht machen wir die Bude hier mal dicht und lassen den TE sein Glück versuchen auch und besonders in dem Wissen das das Unterfangen komplett aussichtslos ist.