

Forum:[Hack Forums](#)

Thread: [Is this a fast MD5 crack program?](#)

FormerlyS - January 10, 2015, 4:42 am

I have a wordlist of 225.000 words, take a random one and MD5 encrypt it. Then I feed it into the program and it cracks it in 1.383849 second.

Is that fast or slow?

Thanks in advance and sorry for the semi-LQ post, there's just not more to say about it ?

FormerlyS - January 10, 2015, 4:57 am

(Jan 10, 2015 05:48 AM)Yani Wrote: [\[CITE\]](#) An MD5 "crack" program either bruteforces the hash or uses a rainbowtable to reverse the hash.

If it's a bruteforcer, the speed depends on how long the original string is and how fast it can actually compute hashes.

If it's a rainbow table, the speed depends on how fast it can look through the table, and how big the table is.

I know that, but my question is, as it uses a dictionary or "rainbow table" if I'm right (a wordlist), is this fast?

FormerlyS - January 10, 2015, 6:28 am

(Jan 10, 2015 07:24 AM)Spl3n Wrote: [\[CITE\]](#) It is not possible to say it is "fast" or "slow" based on a single bruteforce run. The word could be at the start of the list, and find it instantly whatever the wordlist size.

Moreover, "Slow" and "Fast" are really difficult to evaluate if you don't precise the context.

For instance, your bruteforce speed is ridiculously slow compared to NSA.

Or it could be really fast if you're using a 3 Mhz processor.

Give us more details about your configuration.

Ok let's say it was at the bottom line. Would it be fast?

FormerlyS - January 10, 2015, 6:38 am

(Jan 10, 2015 07:31 AM)Yani Wrote: [\[CITE\]](#) Let's say the wordlist is 5 lines. Then no, it's amazingly slow.

Let's say the wordlist is 1 gazillion trillion billion lines. Then yes, it's fast.

You see what we are trying to say? It depends.

In the OP I said:

(Jan 10, 2015 05:42 AM)PS3™ Wrote: [\[CITE\]](#) I have a wordlist of 225.000 words.

Maybe that's what caused the confusion

FormerlyS - January 10, 2015, 6:45 am

(Jan 10, 2015 07:43 AM)Spl3n Wrote: [\[CITE\]](#) I repeat : without a configuration context, we can't say anything.

Anyway, I guess you are using an individual computer, and you want to compare your speed with others individual computer.

Your speed is slow. 225kH/s is not a good speed for MD5 cracking.

Using my GPU - it is not a specially good GPU - I can bruteforce MD5 at a 1303.3 MH/s speed.

Ok thank you!

That's what I was wondering.

And for configuration context, I don't really know what you mean, it just gets them from the dictionary and I chose the last one.

chick3nman - January 10, 2015, 6:50 am

(Jan 10, 2015 07:38 AM)PS3™ Wrote: [\[CITE\]](#) In the OP I said:

Maybe that's what caused the confusion

I can parse and completely compare a dictionary in OclHashcat on my graphics card at speeds of 4-6GH/s with good rules, 8-9GH/s without rules or when using mask/bruteforce attacks. 8GH/s is 8,000,000,000 words a second. The difference in time to actually get up to speed and to be done with a list of your size is negligible. My workload will never get filled and it will never achieve it's full possible calculation speeds. It may finish in a few seconds, which is a lot longer than it should take at full speed, but that's not an accurate measure of my speed.

To say that your speeds are slow or fast wouldn't be fair because your dictionary is just too small. If you have a dictionary that is much much larger, and you time how long it takes to run to the final word in it, you can get a fairly accurate measure of your speed(in hashes compared per second H/s). If your attack is this small, it could never make it to max speed so you could be getting a wildly inaccurate speed measurement.

FormerlyS - January 10, 2015, 6:55 am

(Jan 10, 2015 07:51 AM)Spl3n Wrote: [\[CITE\]](#) That all depends what hardware you are using for computing your MD5 hashes.

Even with a wordlist, you still have to compute MD5 for each word, compare it and iterate to the next one.

That's why I insist on knowing the hardware you are using for this bruteforce : is it GPU-based ? CPU-based ?

If you don't know, what tool are you using ? John the Ripper ? John the Ripper OMP version ? Hashcat ? OclHasht ? ...

The thing is that I made my own bruteforcer so that's why I want to know if it's fast. It doesn't have any configuration.

It's made in Java and I'm running it on my MacBook Air 11" mid 2012.

FormerlyS - January 10, 2015, 7:09 am

(Jan 10, 2015 08:07 AM)Spl3n Wrote: [\[CITE\]](#) Great, this thread is a bit more interesting now :-)

Well, even if your tool is not competitive with the already existing tools, kudos for making your own bruteforce.

Thank you. I'll try to improve it and add some things and then post back here.

FormerlyS - January 14, 2015, 10:46 pm

(Jan 14, 2015 11:38 PM)annez1976 Wrote: [\[CITE\]](#) please can you crack/decrypt this one .??.i'm so newbie ..it just the same trouble i've been looking for a days without result online.

f9b18c901b865b5c7b8fe37d7731a014

and give me your paypal email,,there's small gift for it,,

What language is it in? As that would have the most chance. I don't think I'll be able to crack it with a worlist though.

chick3nman - January 14, 2015, 11:48 pm

(Jan 14, 2015 11:38 PM)annez1976 Wrote: [\[CITE\]](#) please can you crack/decrypt this one .??..i'm so newbie ..it just the same trouble i've been looking for a days without result online.
f9b18c901b865b5c7b8fe37d7731a014

and give me your paypal email,,there's small gift for it,,

If you could not spam post this like 10 times, that'd be great. Makes us more willing to help you if you don't spam the forum. A single post should be enough for us to see it and attempt it.

32 char means its most likely MD5 or RIPEMD-160. I'll add it to my list as soon as the current job finishes.