

Forum:[Hack Forums](#)

Thread: [Any way to "brute-force" my true-crypt pass? I know parts of my pass...](#)

Wozniak - August 21, 2015, 4:26 pm

Okay so today I realized that for some reason the place i stored my TC password is sort of gone. I know part of my password (ik this can be helpful in some brute-forcing tactics) but I do not think I know the order.

(I dont want to say too much) I certainly know how it starts off, and I think i know the amount of special characters.

Can anyone help me out?

-- Sorry ahead of time if I post short replies. I broke my keyboards space and i'm actually pasting spaces to use them. (no key maps for me, it also took a while to type this). I busted all my cash and can't afford a new one for like 2 weeks.

chick3nman - August 21, 2015, 5:59 pm

(Aug 21, 2015 04:26 PM)_Wozniak_ Wrote: [\[CITE\]](#) Okay so today I realized that for some reason the place i stored my TC password is sort of gone.

I know part of my password (ik this can be helpful in some brute-forcing tactics) but I do not think I know the order.

(I dont want to say too much) I certainly know how it starts off, and I think i know the amount of special characters.

Can anyone help me out?

-- Sorry ahead of time if I post short replies. I broke my keyboards space and i'm actually pasting spaces to use them. (no key maps for me, it also took a while to type this). I busted all my cash and can't afford a new one for like 2 weeks.

It actually may be possible to do but i need to know a few more things before i can give you an idea of how to get it done. How long is the unkwown portion of the pass? And the total pass length? Also do you know the encryption order you chose when setting up? Is it full disk encryption or just a file container? How important is this to you(because depending on the questions before this, it could cost a little bit to get this done)?

Wozniak - August 21, 2015, 6:57 pm

(Aug 21, 2015 05:59 PM)chick3nman Wrote: [\[CITE\]](#) It actually may be possible to do but i need to know a few more things before i can give you an idea of how to get it done. How long is the unkwown portion of the pass? And the total pass length? Also do you know the encryption order you chose when setting up? Is it full disk encryption or just a file container? How important is this to you(because depending on the questions before this, it could cost a little bit to get this done)?

I am unsure of the potential costs...

But to create it I basically ran thru the wizard creating a hidden volume on a non-system drive.

The password length was around 22 characters long.

The password probably looked like (# = hidden for security reasons, \$=special char):

l#####14###\$Vxmod#ol##a

I thought it was that (obviously the actual chars rather than #'s :P) but after trying it different ways I got nothing.

And as for the data on the drive; I really want it back, but I won't say I need it to live. It was only created as a testing for me of TrueCrypt since I thought I'd use it more, but I never did.

Don't misunderstand though, I would love it back, but if it won't happen, I'll look into other file/drive-encryption methods and move some new data on it.

hintss - August 21, 2015, 7:22 pm

And how many of those 22 characters do you know?

Wozniak - August 21, 2015, 7:26 pm

(Aug 21, 2015 07:22 PM)hintss Wrote: [\[CITE\]](#) And how many of those 22 characters do you know? Well I thought all.

I know that every word in the censored password does exist.

I think the order may be incorrect.

I know what the password contains, I based the "22 chars" on the part of the password I remember; which I was sure I had close, yet doesnt work.

(sorry if I didnt answer anything you wanted)

FastCrypt - August 22, 2015, 12:02 am

This will take you too much time to crack.

chick3nman - August 22, 2015, 12:11 am

(Aug 21, 2015 07:26 PM)_Wozniak_ Wrote: [\[CITE\]](#) Well I thought all.

I know that every word in the censored password does exist.

I think the order may be incorrect.

I know what the password contains, I based the "22 chars" on the part of the password I remember; which I was sure I had close, yet doesnt work.

(sorry if I didnt answer anything you wanted)

Ok so 22 characters is a lot. Assuming we know what the password SHOULD be, then we can attempt permutations and common misspellings and stuff like that pretty easily. Also, since you said you just followed the wizard, I'm going to assuming that the volume was made using the default encryption that is selected in the menu. As for cost, it really depends. If the attacks have to get much more technical than the ones I described, or if the keyspace for them grows too large, it could cost a good amount. Attacks beyond basic-moderate can take days or even weeks. I'd set a budget for this, sort of like a bounty. That way anyone who want's to attempt it knows how much work to do before it becomes no longer worth it to attempt to recover the password.

Wozniak - August 22, 2015, 6:36 am

(Aug 22, 2015 12:11 AM)chick3nman Wrote: [\[CITE\]](#) Ok so 22 characters is a lot. Assuming we know what the password SHOULD be, then we can attempt permutations and common misspellings and stuff like that pretty easily. Also, since you said you just followed the wizard, I'm going to assuming that the volume was made using the default encryption that is selected in the menu. As for cost, it really depends. If the attacks have to get much more technical than the ones I described, or if the keyspace for them grows too large, it could cost a good amount. Attacks beyond basic-moderate can take days or even weeks. I'd set a budget for this, sort of like a bounty. That way anyone who want's to attempt it knows how much work to do before it becomes no longer worth it to attempt to

recover the password.

-Sigh-

Well, I think I got everything I needed.

Thanks for all the info guys!

I think I will....just forget the data that was on it; seems to be my best option.

Thanks again!