

Forum:[Hack Forums](#)

Thread: [How to crack MD5 hashes](#)

?Skiller - June 9, 2011, 3:25 pm

Probably already been posted, but I just thought I would make my own tutorial.

In case you did not already know, MD5 is not an encryption, and therefore cannot be decrypted, only cracked.

First off, download "Password Pro" from [here](#).

It is a zip file, so I suggest downloading [7zip](#).

Extract all of the files to one folder.

It should look similar to this.

[img]http://img508.imageshack.us/img508/2/11987894.png[/img]

For the purpose of this tutorial, I will be cracking this hash:

"6dcd0f272fbb7f6f8ff3a8a5e96c45aa:Ws)", which is formatted as "Hash:Salt", and is from VBulletin 4.x.x.

Open up notepad, paste in the Hash and salt, and save it anywhere on your computer, preferably in the same folder as Password Pro.

[img]http://img571.imageshack.us/img571/8668/56139940.png[/img]

Open up Password Pro and go to "File->Import"

[img]http://img228.imageshack.us/img228/6457/84755402.png[/img]

Find the place where you saved the text file with the hash inside of it, and open it.

Fill in the boxes as such.

[img]http://img36.imageshack.us/img36/3755/13377943.png[/img]

Note: The bottom is the formatting of the hash and salt in the text file, and the top is the algorithm for VBulletin 4.x

Now, go to "Audit->Preliminary Attack"

(For this hash, as it is simple, it should probably crack it with just this.)

[img]http://img861.imageshack.us/img861/4074/63893726.png[/img]

Hit the start button, and watch it go.

[img]http://img30.imageshack.us/img30/5355/70193249.png[/img]

If, in the case that a Preliminary Attack does not work, just repeat the previous steps with a Rainbow Attack (If you have a Rainbow Table), a Simple Dictionary Attack, or a Brute Force Attack.

Post your thoughts, or if this helped you.

123Password - June 9, 2011, 3:44 pm

Isnt this you know illegal to do.

?Skiller - June 9, 2011, 3:45 pm

(Jun 9, 2011 03:44 PM)123Password Wrote: [\[CITE\]](#) Isn't this you know illegal to do. It isn't illegal to crack a hash.

GreatDayChap - June 9, 2011, 3:48 pm

(Jun 9, 2011 03:44 PM)123Password Wrote: [\[CITE\]](#) Isn't this you know illegal to do. This is 'hack'forums, Your joking me right?

Btw: FIRST POST FUCK YEAH!

?Sean - June 9, 2011, 4:08 pm

Very nice tut! Thanks man helped me a lot.

king tulip - June 9, 2011, 4:08 pm

Thanks for the tut, I'll be using this in the future. Very helpful, nice job.

Yellow Hooded Coder - June 9, 2011, 4:55 pm

Nice job, easy to follow with the pictures.

b44manz - June 9, 2011, 5:10 pm

may i ask why would somebody want to crack md5 hashes and can you give me some more to do and tell me how this is useful

cannoner - June 9, 2011, 5:59 pm

I grabbed this from vbulletin 3.x.x, what settings do I need to use in password pro to try and reveal, and where can I get a good set of ranbow tables.

cannoner - June 9, 2011, 5:59 pm

Why are my posts being dup'd !!!! - I edited this one

ShadowKage - June 9, 2011, 6:03 pm

Nice tut now i can get other member pass :D

?Skiller - June 9, 2011, 6:09 pm

(Jun 9, 2011 06:03 PM)ShadowKage Wrote: [\[CITE\]](#) Nice tut now i can get other member pass :D There is a nice tutorial in the Forum Hacking section on getting Hashes and salts from VBulletin 4.x.x :p

Mash22 - June 9, 2011, 11:56 pm

awesome man keep the good work up!

NEWvikka(ifrogotmypass) - June 10, 2011, 12:36 am

Thank's alot.I was just looking for this!

?Skiller - June 11, 2011, 10:59 am

(Jun 10, 2011 12:36 AM)NEWvikka(ifrogotmypass) Wrote: [\[CITE\]](#) Thank's alot.I was just looking for this! Thanks for the feedback :).

TheBeast808 - June 30, 2011, 7:20 pm

I'm testing this, but the format I got from that database is like this:
id_number(I think):Username:hashed_password:e-mail

I don't see how you get the salt. Can you explain it to me?
I'll just post an example of one of the lines I have:
63:Shreyas:434e4dd8e21bbf25e4f0344ce5890548:shreyasyedekar@gmail.com

How do a get a salt from that? Is it in another table or what?

sexynsmartjenny - June 30, 2011, 8:58 pm

hey thanks i will try this out.

firefury87 - July 1, 2011, 10:06 am

(Jun 30, 2011 07:20 PM)TheBeast808 Wrote: [\[CITE\]](#) I'm testing this, but the format I got from that database is like this:

id_number(I think):Username:hashed_password:e-mail

I don't see how you get the salt. Can you explain it to me?

I'll just post an example of one of the lines I have:

63:Shreyas:434e4dd8e21bbf25e4f0344ce5890548:shreyasyedekar@gmail.com

How do a get a salt from that? Is it in another table or what?

When you import the Hash try using md5(md5(\$pass)) instead of md5(md5(\$pass).\$salt) and set formatting to Hash instead of Hash:Salt.

Give me a feedback if I've helped you or not since I haven't had a chance to try this as I've only followed examples by now, so it might help me if it worked for you. :)

micafire - July 3, 2011, 4:54 am

I have tried this and no luck, I don't know where to get the salt from.

It only has the whole hash itself, nothing else.

D3v1l@ - July 3, 2011, 8:56 am

nice post i will try :) thex for share bro

hgmilller - July 3, 2011, 9:51 am

nice tutorial, thanks for share.

In?sane? - July 3, 2011, 12:28 pm

I have made an video tutorial on how to use this, hope you don't mind. Im giving credits to you ofc.

http://www.youtube.com/watch?v=jBz8cY4XFGw&feature=channel_video_title

<https://hackforums.net/showthread.php?tid=1443901>

kristo199 - July 3, 2011, 12:47 pm

Easiest way to do it just use the online webpage

?Skinner - July 3, 2011, 9:41 pm

(Jul 3, 2011 12:47 PM)kristo199 Wrote: [\[CITE\]](#) Easiest way to do it just use the online webpage

You can't crack a salted hash with an online website.

firefury87 - July 4, 2011, 8:52 am

(Jul 3, 2011 09:41 PM)Twilight Sparkle? Wrote: [\[CITE\]](#) You can't crack a salted hash with an online website.

In my opinion, hash cracking web sites aren't as useful as having a proper software. Just last night I've tried over 10 websites and haven't been able to crack any of the hashes I've submitted, and they

were all non-salted.

md5this.com has cracked just one of my hashes and this week I've tried to crack over ~200, so one out of 200 isn't very encouraging.

?? ??????¢???I?™ - July 4, 2011, 9:04 am

Umm nice tut great job at explaining it

gizmodo - July 4, 2011, 4:07 pm

how about using bruteforce? im having a hardtime using bruteforce in passwordspro, im not sure if im setting it up correctly, i have used different md5 bruteforcer and they able to crack it in less than 25 minutes. however in my passwordspro it say it's finish but no password is showing. (Jul 4, 2011 08:52 AM)firefury87 Wrote: [\[CITE\]](#) In my opinion, hash cracking web sites aren't as useful as having a proper software. Just last night I've tried over 10 websites and haven't been able to crack any of the hashes I've submitted, and they were all non-salted.

md5this.com has cracked just one of my hashes and this week I've tried to crack over ~200, so one out of 200 isn't very encouraging.

thats why you need huge wordlist and good online md5 archive.

RiotousMind - July 5, 2011, 4:09 pm

Great tutorial. Are there any rainbow tables that won't kill my HD space? If not, that's fine. But how would I configure the use of rainbow tables with Passwords Pro?

?Skiller - July 5, 2011, 9:43 pm

(Jul 5, 2011 04:09 PM)RiotousMind Wrote: [\[CITE\]](#) Great tutorial. Are there any rainbow tables that won't kill my HD space? If not, that's fine. But how would I configure the use of rainbow tables with Passwords Pro?

Rainbow tables, at least good ones, are generally pretty large.

If you want to configure it to use Rainbow Tables:

Go to Settings, and then Rainbow Attack-> Rainbow Table.

Just right-click in the empty space, and select "Add".

noober1001 - July 5, 2011, 11:11 pm

Thank for this.

Do you have password list, which have all dictionary words?

Vendetta08 - July 6, 2011, 12:46 am

nice tut! thanks.. very easy to follow with the pictures! :d

Kadabraa - July 6, 2011, 3:05 am

Nice share, pretty simple to use but fuck it

tueur - July 6, 2011, 3:49 am

Is there an utility similar to crack SHA1 ?

tadeitto - July 6, 2011, 6:54 am

Nicely done.! pretty helpful. Gratz and keep working.!

firefury87 - July 6, 2011, 1:19 pm

(Jul 6, 2011 03:49 AM)tueur Wrote: [\[CITE\]](#) Is there an utility similar to crack SHA1 ?You can always Google whatever you're searching for, even the hash you want to crack.

I recommend HashCat, I'm new to it but it seems as effective as PasswordsPro.

Suit® - July 7, 2011, 6:24 am

Hmm... Does the preliminary attack not work on standard MD5's?
Coz mine just skips to say it's finished without doing anything. O.o
Nice find though. I probably have a bad installation or something

firefury87 - July 7, 2011, 9:23 am

Preliminary attack is just a quick check of hashes for matching to simple passwords like 123, qwerty, 9999, admin, lol, etc., passwords not so complex if you know what I mean, and also it checks for the passwords it previously cracked that are stored in PasswordsPro.dic file.
Try the hash from this tutorial, you'll see it'll get cracked in a sec with Preliminary Attack.

Ice Travanti - July 7, 2011, 10:31 am

Nice and clear tut, thanks a lot?

divo99 - July 7, 2011, 10:42 am

Anyone know for the hash pass below :

samaragj@aol.com: -t7C8cvA49HLbPt7b6w7HnRkvOEI-04tHZ8xZ8cYGGQ

mani.avancha@yahoo.com: bWVsQ7bm99D3VnWeLXcGgTvl4a9jn9-W_YqTWL6U03U

How to crack it pass ??

Thanks.

sataikage - July 7, 2011, 11:37 am

Thanks for it, sharing is caring.

ignite2030 - July 19, 2011, 11:31 am

Thank you! You've made it very easy to crack these hashes now ;).

Quick question:

Sometimes vb pws are saved with hash that is longer than 3 chars, is it possible to crack these using this tool?

?Skiller - July 19, 2011, 12:12 pm

(Jul 19, 2011 11:31 AM)ignite2030 Wrote: [\[CITE\]](#) Thank you! You've made it very easy to crack these hashes now ;).

Quick question:

Sometimes vb pws are saved with hash that is longer than 3 chars, is it possible to crack these using this tool?

Yes.

By default, VBulletin uses pretty large salts, and it is still possible to crack them.

Tainted Star - July 19, 2011, 12:13 pm

am having the same prob...and how can we crack them ?

ignite2030 - July 19, 2011, 1:11 pm

(Jul 19, 2011 12:12 PM)Skiller Wrote: [\[CITE\]](#) Yes.

By default, VBulletin uses pretty large salts, and it is still possible to crack them.

Thanks for the answer, will try to do some cracking later.

Tainted Star - July 19, 2011, 1:27 pm

Hash : db43e86a9372906b86fcaac68a160db2

Salt : 1\QNpb|oBG1_dRy~?%2f6W5>w-YY0pO7B*(LBp{|P

couldn't crack it with passwordpro :(

Help needed

Akolt - July 24, 2011, 12:40 am

thanks, very useful :D I had problems with this before

Prince™ - July 24, 2011, 5:44 am

I find myself difficult to crack md5 hashes with salt from a vbulletin board ? but this really taught me something nice tutorial ?

Mundial - July 24, 2011, 6:11 am

Yeah usually for me it can take literally months. These passwords take incredible long to crack unless you get lucky.

dyngtampen - August 18, 2011, 9:08 am

omfg, i have a vB passand salt and its gonna take 3 days lol :D

Hannibal Lecter - August 18, 2011, 9:17 am

Good job, reserved for the future!

msg is 2 short

p???? ? - August 18, 2011, 12:32 pm

Will test this as soon as there is little time

Thanks

Zeyn™ - August 18, 2011, 3:53 pm

Simply amazing!! Thank you. You're awesome. Keep it up bro ;)

Nukemonk - September 13, 2011, 7:27 am

Aren't rainbow tables useless against salted hashes since they are pre-computed?

!-Angelina-! - September 13, 2011, 7:10 pm

Normally how much days it take to bruteforce anythng ??

pratikpise92 - September 13, 2011, 9:05 pm

Nice job, easy to follow with the pictures.

Nukemonk - September 14, 2011, 2:49 am

(Sep 13, 2011 07:10 PM)!-Angelina-! Wrote: [\[CITE\]](#) Normally how much days it take to bruteforce anythng ??

That really depends on you'r hardware and the length to crack. The longer the text is the more combinations you have. [Here](#) you have a brute-force calculator.

Bago47 - October 12, 2011, 11:24 am

Does this work for a LM hashes? Atm cracking LM hash (i set it as it's a MD5), 1% done (time 15 mins).

koda-coder - October 13, 2011, 5:45 am

thamks for share mate

nice tut thx bro realy helped me out lol

hackeye - October 13, 2011, 11:19 am

why does this prog look like a trojan?

.
. .
. .
. .
. .
. .
. .
. .
. .

Nav - November 21, 2011, 10:33 pm

(Oct 13, 2011 11:19 AM)hackeye Wrote: [\[CITE\]](#) why does this prog look like a trojan?

.
. .
. .
. .
. .
. .
. .
. .
. .

It isn't a trojan it's safe. Thanks OP!

Interpreter31536 - November 22, 2011, 1:24 pm

Or you could just use Cain and Abel which is allot easier.. Nice TUT though!!

MaorS - December 27, 2011, 3:25 am

[img]<http://img266.imageshack.us/img266/1954/captureend.png>[/img]

WTF I need to do??

Camfrog - December 27, 2011, 4:39 am

Hey man, can you decrypt this with PasswordsPro, I think it's hash1 or something.

Code

472B486C726E4771696958352F6748793278724B52554951397234524C6F655968533273505738
672B444E65316D3479776833514C41533462676944616F45344B76355466365076432B6B667933
59486F476E7876513163306F78703566584D2B4E6952552B506A7A4965676C426B6B773758345
364685149586232753658516A4A4E392F424C537848494B4330316A2F3662424A2F4F662F456E
7659412B4C557543574C6778716374303D

krazyarker - December 27, 2011, 4:53 am

There are also websites that offer better md5 cracking because their dictionaries are alot bigger as their stored online