

Forum:[Hack Forums](#)

Thread: [== SECRECY == >>> CHOOSING A SECURE PASSWORD <<<](#)

Pronouncer - July 22, 2017, 1:35 pm

Introduction

Thank you for clicking on the thread. As part of the group Secrecy, we will be releasing an informative thread on passwords and security of passwords.

There are countless different tutorials on the internet, on choosing a password, how to make it secure, what to do and what not to do. Many guides are good to look at in fact there was a kid who made a lot of money making passwords for people. The problem with all of these is I feel that they don't provide actual examples.

How are passwords broken into?

There are many different ways you can get your password exposed, leaked or maybe even discovered. A very popular way of this is through brute-forcing, dictionary attacks, and hybrid dictionary attacks.

What is brute force?

Brute force according to wikipedia is

"In cryptography, a brute-force attack consists of an attacker trying many passwords or passphrases with the hope of eventually guessing correctly. The attacker systematically checks all possible passwords and passphrases until the correct one is found."

So what does this mean exactly? Well, a hacker will setup a script or program inputting your username or email and that piece of software will try every single possibility of passwords there is. Depending on the site they are trying to brute force this could be quick or slow. Some sites will lock you out of the account after three tries for 24 hours, others will IP ban this makes brute-forcing incredibly slow especially if you have to utilize proxies to do so. The longer you set your password the harder it is for the program to get in.

What is a dictionary attack?

A dictionary attack is quite similar to brute force. A dictionary attack, however, does not try every single possible solution till it gets it right, dictionary attacks work best on large scales. What this does is try a username against a long list of commonly used passwords in hopes it hits. You would be really surprised how often this works, setting a unique password really does help from these.

What is a hybrid attack?

Now hybrid attacks are the same as a dictionary in ways however the attacker will set some parameters for the tool to try after the dictionary list. So normally it will try this list for example:

Password
Football
Soccer

but with a hybrid attack, the attacker is able to set the tool to try adding on numbers/letters after the password so the list would be

Password1

Password2

Password3

and continues until what the attacker has defined.

Lets do some maths

If your password was only using lowercase letters and was 6 characters long there would be around 310 million different possibilities. That may seem like a lot but its really not.

Mixing lowercase uppercase and digits in 6 characters is around 57 billion different combinations which take your time to calculate 300 attempts per second and figure out how long it'd take.

Making Passwords

So we have covered some things when it comes to breaking into passwords, now we have to talk about creating passwords so far we have well should have learned these things.

Not to use a password in a dictionary ?

Use a mix of letters upper case and lowercase ?

Use numbers and possibly symbols ?

Use 6+ Characters ?

We have a few options now for setting password we could do something like this

HMNIPIWBO2017

Seems random asf right? Definetly not in a dictionary anywhere but you may be questioning how am i supposed to remember that well lets break it down

H: Hi

M: My

N: Name

I: Is

P: Pronouncer

I: I

W: Was

B: Born

O: On

2017

Easier now right? Well, that is one way people have been doing it for a while.

Well, there are two other options one puts your passwords in the hands of someone else, the other allows you to be in full control and responsibility. This is Lastpass and Keepass

KeePass

KeePass is a tool that allows you to store your passwords on a piece of open source software that utilizes encryption and requires you to set a master password. The tool makes you manually enter users and passwords to sites you sign up on along with a password generator. This tool will save a backup file to your system which if you lose and forget your password well bye bye all your passwords.

LastPass

Well LastPass is a cloud password saving system which is really handy when using browsers, the biggest flaw is you trust your security in the hands of someone else. You will have to sign up and remember your master password. LastPass requires you to login to the plugin or program and it will save your passwords along with auto generate them.

Why Never to use the same password

You may be asking why not use the same password everywhere. Well if someone hacks your password and gains access to that do you really want them to have everything you digitally own? We see websites getting hacked in the days leading to hacked database breaches and password dumps, no site is safe from this not even HF. We have seen twitter been hacked, LinkedIn and more. Once a database gets leaked there is no going back people will instantly be trying to crack passwords and get into accounts to profit off.

Here is a good place to check if you have had your password hacked.

<https://haveibeenpwned.com/>

If you insist on using the same pass please for the love of god use 2 factor authentication.

Final Summary

These are some passwords you should never ever use for the love of God.

Spoiler ([Click to View](#))

Dont write your password down ?

Dont use words ?

Dont use personal information such as birthdays ?

Use different passwords on all sites (lastpass and keepass will help) ?

Use capitals lowercase symbols and numbers ?

Change password often ?

Thank you for taking the time to read this thread. We appreciate your effort and look forward to helping you out. If you are interested in joining us please read this thread.

<https://hackforums.net/showthread.php?tid=5673489>

DVS-01 - July 22, 2017, 1:41 pm

Just read it, another interesting and informative post by the group. Definitely good for users who don't have a clue how to keep their shit safe.

?ictor? - July 22, 2017, 8:20 pm

Very informative, great post from Secrecy

Monie - July 23, 2017, 8:46 pm

You need to consider a vector in which an attacker has a user's hashed password from a DB breach. Though it's just the hash, the rate at which you can check plaintexts increases astronomically in comparison to bruteforcing a login over HTTP.

I mention this because it's a fact that many people will re-use a password when they get lazy, even

if they try to follow the rules you've laid out in this thread.

The minimum of 6 characters you've mentioned might hold up in a remote attack, but definitely not in a local attack with the vector I've described.

ola78 - July 23, 2017, 9:33 pm

Nice contribution.

I love KeePass since years now. It's very nice, you can even set expire date to be sure to change passwords.

That's the most effective way to keep your passwords protected.

It's even faster to CTRL+B & CTRL+C than typing username and password ! Everybody should be already using this kind of tools.

EvoBlade - July 24, 2017, 6:59 am

was looking for this. Nice one

I probably going to switch to some password manager

tfti10001 - July 24, 2017, 11:36 am

interesting topic and helpful details. always gotta be on your ass in this world

andrius94 - July 24, 2017, 1:42 pm

simple and awesome. this should be common knowledge for everyone.

xX_l337_h4x0r_Xx - July 24, 2017, 1:48 pm

[https://en.wikipedia.org/wiki/Entropy_\(computing\)](https://en.wikipedia.org/wiki/Entropy_(computing)) more entropy in password is good, less entropy is bad.

Pronouncer - July 25, 2017, 11:00 am

I might add a bit on that thanks for the contribution

Bitcoin Market - July 25, 2017, 2:13 pm

thanks for this post i am very happy theres some guy like you in hf.

Pronouncer - July 31, 2017, 7:38 am

Still a good read for all beginners

Pronouncer - September 17, 2017, 2:38 pm

Bumping this as it is still a great read, look out for our student scheme

Pronouncer - September 21, 2017, 12:14 pm

Still a good read for beginners to be honest

LD_PRELOAD - September 21, 2017, 12:21 pm

no it's not

any password less than 16 chars is automatically shit

article assumes online brute force when realistically password strength is mostly relevant against hash cracking, where average computation is 2^{30} hashes / second

when discussing password security, length > character variation

x^y

x = more chars

y = more length

jedijingle - *September 21, 2017, 1:17 pm*

Good stuff to keep in mind, thanks very enlightening to a newbie.

Pronouncer - *December 23, 2017, 10:07 am*

Seems like common knowledge but its really not....