Use an 8-character Windows NTLM password? Congratulations, your password may be unlocked after only 2.5 hours

HashCat, an open source password recovery tool, is now able to unlock Windows NTLM passwords from eight characters or less in a very short period of time, less than 2.5 hours.

HashCat, an open source password recovery tool, is now able to unlock Windows NTLM passwords from eight characters or less in a very short period of time, less than 2.5 hours.

Back in the past a bit, in 2011, security researcher Steven Myer proved that eight-character (53 bit) passwords can be broken within 44 days if you use a GPU. and rainbow tables - tables are pre-calculated to reverse hash functions.

Another well-known developer, Jeff Atwood, reported in 2015 that the average password length most people use is about 8 characters and since then, nearly 4 years have passed. but without any indication that things have changed a lot, it is simply a difficult habit to give up. And with the fact that about 620 million stolen web information is about to be sold this week on a black web market, now is the time to be more suitable for mankind to make a radical revolution. in using and managing passwords.

1. Google launches a "god" Password Checkup utility that makes your passwords more secure

In a post on Twitter on Wednesday, February 13, those responsible behind the HashCat software project said the HashCat version 6.0.0 beta was completely manually adjusted, using up to 8 Nvidia GTX 2080Ti GPU in an offline attack, exceeding the standard NTLM unlocking speed standard is 100GH / sec (gigahash per second).

"The current benchmark password cracking speed shows the fact that just how complex the 8-character minimum passwords can still be cracked in less than 2.5 hours by Using such hardware-based attack mechanisms, the eight-character password was outdated, 'a hacker with a pen name Tinker shared on Twitter.

Confirming an outdated 8-character password may seem a bit sudden, but at least we must admit that it has become quite insecure in the context of attacks on Windows-based organizations and Active Directory tends to increase rapidly. As you know, NTLM is an old Microsoft authentication protocol and has been replaced with Kerberos. However, according to the Tinker pseudonym, NTLM is still used to store local Windows passwords or in NTDS.dit files in Active Directory Domain Controllers (Active Directory Domain Controllers).

Of course, stronger hashing algorithms will take longer to crack, but sometimes the intensity of the commands will be longer. Try a small comparison, when IBM achieved the percentage of hash cracking of 334 GH / s with NTLM and Hashcat in 2017, they could only manage 118.6 kH / s with bcrypt and Hashcat. But those who are trying to unlock hash passwords can pay for cloud services in exchange for the necessary computing power.

1. Azorult Trojan steals user passwords while running in the background like Google Update

The Tinker pen name also estimates that the required GPU power investment will require an amount of about $ 10,000. However, others claim that the computational power needed to unlock 8-character NTLM passwords can be rented in Amazon's cloud utility for just $ 25.

The latest NIST instructions indicate that modern passwords are required to be at least 8 characters long, but some online service providers don't even require that much. When Troy Hunt security researcher checked the average minimum password length at different sites last year, he found that while Google, Microsoft and Yahoo forced users to set passwords not less. over 8 characters, Facebook, LinkedIn and Twitter only require a minimum of 6.

According to the pseudonym Tinker, the eight-character password is used as a benchmark because that is the number that many security organizations and many IT policies of companies recommend to set the minimum password length. . In fact, over the years, we have pushed the idea of ??focusing more on complexity (uppercase letters, lowercase letters, numbers and symbols) of passwords, so the task of remembering each password individually also become much more complicated. This, along with a few other small factors that make users choose to use passwords of the minimum length allowed, simply so they can remember their complex passwords more easily.

So until new security advancements appear and change everything, how long is the password safe enough? Tinker proposed a set of five-year random words, in which each word contained a certain number of characters, and to make it easier to remember, you could set a password in a phrase that was meant or familiar to you, for example, 'correcthorsebatterystaple'.

Also, if possible, you should consider using an additional password management application, with two-factor authentication enabled in all cases. In this regard, you can refer to our list of "Best current password management software" to choose a suitable tool for you. Good luck!

1. Android apps contain malicious code that uses motion sensors to avoid detection