Security

# Use an 8-char Windows NTLM password? Don't. Every single one can be cracked in under 2.5hrs

## CorrectHorseBatteryStaple once again more secure and memorable than ff3sd21n

By Thomas Claburn in San Francisco 14 Feb 2019 at 22:56 164 SHARE ▼


HashCat, an open source password recovery tool, can now crack an eight-character Windows NTLM password hash in less time than it will take to watch Avengers: Endgame.

In 2011 security researcher Steven Meyer demonstrated that an eight-character (53-bit) password could be brute forced in 44 days, or in 14 seconds if you use a GPU and rainbow tables – pre-computed tables for reversing hash functions.

When developer Jeff Atwood said as much in 2015, the average password length was about about eight characters and there's no

indication things have changed much. With some 620 million stolen web credentials coming up for sale this week on a dark web market, now's as good a time as any for a password review.

In a Twitter post on Wednesday, those behind the software project said a hand-tuned build of the version 6.0.0 HashCat beta, utilizing eight Nvidia GTX 2080Ti GPUs in an offline attack, exceeded the NTLM cracking speed benchmark of 100GH/s (gigahashes per second).

"Current password cracking benchmarks show that the minimum eight character password, no matter how complex, can be cracked in less than 2.5 hours" using that hardware rig, explained a hacker who goes by the pseudonym Tinker on Twitter in a DM conversation with *The Register*. "The eight character password is dead."

It's dead at least in the context of hacking attacks on organizations that rely on Windows and Active Directory. NTLM is an old Microsoft authentication protocol that has since been replaced with Kerberos. According to Tinker, it's still used for storing Windows passwords locally or in the NTDS.dit file in Active Directory Domain Controllers.

## Processing arsenal

More robust hashing algorithms take longer to crack, sometimes orders of magnitude longer. As a point of comparison, when IBM was getting hash cracking rates of 334 GH/s with NTLM and Hashcat in 2017, it could only manage 118.6 kH/s with bcrypt and Hashcat. But, given a suitably short password, those attempting to crack hashed passwords can break out their wallets and pay cloud services for the necessary compute arsenal.

Tinker estimates that buying the GPU power described would require about $10,000; others have claimed the necessary computer power to crack an eight-character NTLM password hash can be rented in Amazon's cloud for just $25.

NIST's latest guidelines say passwords should be at least eight characters long. Some online service providers don't even demand that much.

When security researcher Troy Hunt examined the minimum password lengths at various websites last year, he found that while Google,

Microsoft and Yahoo set the bar at eight, Facebook, LinkedIn and Twitter only required six.

Tinker said the eight character password was used as a benchmark because it's what many organizations recommend as the minimum password length and many corporate IT policies reflect that guidance.

**Either my name, my password or my soul is invalid – but which?**

READ MORE

"Because we've pushed the idea of using complexity (upper case letters, lower case, numbers, and symbols), it's hard for users to remember individual passwords," Tinker said. "This does, among other things, cause users to pick the minimum length allowed, so that they can remember their complex password. As such, a large percentage of users choose the minimum requirements of eight characters."

So how long is long enough to sleep soundly until the next technical advance changes everything? Tinker recommends a random five-word passphrase, something along the lines of the four-word example popularized by online comic XKCD, "correcthorsebatterystaple."

That or whatever maximum length random password via a password management app, with two-factor authentication enabled in either case.

Via Twitter DM, HaveIBeenPwned admin Troy Hunt told *The Register* that while web apps are increasingly using better hashing algorithms than NTLM, like bcrypt, "I always make my passwords dozens of random characters generated by 1Password." ®

Tips and corrections

164 Comments



**MORE** Windows Security Software