Impact of Encryption Strength on Password Cracking Time

Brown, Jaclyn (School: Hardee Senior High School)

The aim of this project was to understand and check the effect of encryption strength on the time it takes to breach passwords, which is a key aspect of cybersecurity. The research set out to find out the relationship between the complexity of different encryption algorithms and the time and resources they need for cryptanalysis solutions through using various encryption algorithms like MD5, SHA1, and SHA2-256. To analyze the time required to break the password dataset hashed with the help of Hashcat which is a password-cracking software program.The unexpected outcomes were very strong to support that stronger encryption algorithms have relative time and power increase to crack the passwords. Participating in this study gave me the realization that the longer the password the harder it'd break, is not always the rule.. An extremely long password may have a tiny hash, which can easily turn on a password cracking process. The task of choosing a password that would be completely secure is becoming tougher by the minute.I think the mixing of special characters with a regular password increases the attack difficulty, however my research indicates this is not the case. Hashcat software was very robust. It successfully cracked all the passwords in less than 20 seconds each time. The algorithms I applied were not the most powerful or the weakest; they were just the popular ones. What if I were to use the most powerful encryption that has ever been created, would there be any password that is safe? Besides broadening scientific knowledge, this research also adds value to society by enhancing privacy and security measures, thus making the public more confident in digital systems.

Awards Won: