International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 06 Issue: 06 | June - 2022 Impact Factor: 7.185 ISSN: 2582-3930

Most Used Password Cracking Techniques

Abhisek Kumar Shandilya[1*], Chethan R[2*],Dr. Zafar Ali Khan[3+]

*School of Engineering, Presidency University Bengaluru, Karnataka, India

+Dept. Of Computer Science, School of Engineering, Presidency University Bengaluru, Karnataka, India.

Abstract

Passwords are the most widely used way to secure information and a platform is considered safe to the level of its weakest point users are constantly being educated about making harder or unpredictable passwords as well as one-time passwords or with the introduction of biometrics and password-less account that send a notification to the user's electronic device the average user habits have not changed but with the introduction of new technology password cracking techniques have changed in this paper we take a look at the widest used password cracking methods Phishing, Malware, Social engineering, Brute force attack, Dictionary attack we also take a look at how these methods have evolved and also how GPU have affected Brute force and Dictionary attack and the number of losses due to password cracking and also where they are used and for what cause are they used and also the problem with using hashing to store password

Keywords

password cracking, GPU, Brute force attacks, Dictionary attacks, Hashing, link guard algorithm, ben Clark algorithm

introduction

The Internet is a large network connecting people on many computers. people can share information and converse through the Internet from any location, as long as there's an Internet connection. The Internet was made on January 1st, 1983, And the first password ever created was made in 1961. At MIT, with an operating system called compatible time Sharing system. Innes a recent survey it was sound at 13:00 percent. Of people. Have been acknowledged that they have been hacked in 2018. If you were to calculated number of accounts, they have an average and 13%. That is more than 2.5 billion accounts hacked in just 2018. That is 5,000,000 accounts in it. That was lost to just hacks. In this paper, we take. A look at what are the hacjing techniques that hackers used the most in order to get access to these accounts and also how companies store them. Passwords use hashing in order to protect them even though the. Companies' infrastructure is compromised.

1.Phishing

Phishing could be a common tactics employed by cyber attackers within which they fight to steal personal and financial information about us. There are differing kinds of phishing like smishing, which is attempted through SMS. Spear phishing,

which is hyper-targeted attempt within which a message looks like from a source which you recognize personally. Whaling, a shot geared toward a high ranked official in a organization. And many other. To prevent from Phishing is to Extremely cautious about the message we receive , and verify requests for information through another means.

2.Malware

Malware (short for "malicious software") may be a file or code, that's delivered to you over a network, which can steal your information or cause a virtual attack and behave because the attacker wants. Providing device for an attacker to use an infected machine, Sending spam from the infected machine to unsuspecting targets, Investigating the infected user's local network and Stealing sensitive data are the common objectives of malware. There are differing kinds of malware like Botnets, Crypto jacking, Malvertising (malware + advertising), Polymorphic malware and plenty of more .To prevent from malware we must always regularly update our systems. aside from this we've firewalls, network Intrusion Prevention System(IPS),deep packet inspection(DPI).

3.Social Engineering.

Social engineering is a very broad malicious activity accomplished by criminals through human interactions. It uses psychological manipulation to trick and creating mistakes of freely giving the information to the criminal. This usually happens in one or multiple steps in offender or criminal. First investigates the target. Which he wants to. Break into hi invest. He tries to find potential points of entry of weakness in the security protocols, after which he proceeds with the attack. The criminal then tries to gain the trust of the target in order to get the information through them. Or break security practices. Social engineering. Has many other techniques, such as baiting-it beating it which uses the victims greed to the advantage by doing false promises. They also use scareware in. Which uses. The victims fear to the advantage. This is extremely clever, as this is very highly used, such as in bank frauds when. the criminal acts as, An official personal whereas he is not in order to get the use the victim to devote information in order, crack passwords such as OTP.

4.Brute force attacks

Brute force attack is the type of attack that the attackers use assuming that the password can be anything of any length the hacker starts by assuming that the password is one character or the minimum amount of characters that can be used as the password for the account to the max length the account protection supports these types of attacks are used form a long time and are not automated by programs a brute force attack is guaranteed to succeed given enough time and that there are no countermeasures for it deploy by the account security policies 4 digits pins that only contain numbers that are the smallest pin used for account security alone has 10000 combinations if we were to take the average length of password which is 9 length consulting of alphabeted capital and small separately, numbers and special character we have a total of 94 possible characters to fill in each place this results to 572,994,802,228,616,704 possible combinations. Currently, the most effective method used to prevent brute force is to put a certain amount of login tries after which the account is blocked or a CAPTCHA test is done

GPU usage in brute force method

GPU is designed for mathematical operation since it is responsible for drawing things onto your screen, however. This is not what increases the performance of the brute force method with the use of GPU. A high-end CPU has 16 cores and 32 threads at max in retail space whereas a high-end GPU from Nvidia the most dominant GPU hardware maker provider provides 1280 cores in its most use GPU that has the most market holding which is called the Nvidia 1060 whereas AMD which is the second most dominant GPU provider gives 2560 cores whereas a high-end GPU from Nvidia has 3960 cores which are the RTX 3080 unlike CPU, GPU can parallelize loads compared to GPU which do tasks iteratively due to which a password that might take an entire year to crack with the use of a CPU can be cracked in 10 minutes with the help of CPU

5.Dictionary attacks

Dictionary attacks are attacks in which the attacker has a list that can be the possible passwords. The attacker obtains this list from data leaks, dictionary, and the most commonly used passwords since the list is finite and does not have an infinite limit like brute force have an infinite number of possible passwords to guess hence requiring fewer resources than brute force attacks this method is used usually to break into a system with weak password rules. currently the most effective method used to prevent brute force is to put a certain amount of login tries after which the account is blocked or a CAPTCHA test is done

Hashing

hashing is a technique used to turn the password into a short string of letters and numbers using an encryption algorithm it also needs to efficiently find or store them.

When a website is hacked, and the password is tried to be accessed the hacker gets the encrypted “hash” instead of the password that is created by an algorithm one of the most common has to function is MD5() which returns a 32-character string form input. Hashing is a one-way function it maps data of variable length to a fixed length. there are many hashing methods such as MD5, and Secure Hash Algorithms (SHA), such as SHA-1 and the SHA-2 family that include the widely used SHA-256 algorithm. Currently, the most vetted hashing algorithm providing the most security is bcrypt.

2 most used passwords in the world as per leaked password leaks in the dark web

Your String =123456

MD5 Hash e10adc3949ba59abbe56e057f20f883e

Your String =123456789

MD5 Hash 25f9e794323b453885f5181f1b624d0b

Protection algorithm:

algorithm is a Ling guard algorithm is a basic algorithm used to check whether the link send in email is safe for use or not it achieves this by comparing the link with how similar it is with a trusted known site it first extracts DNS from the link and analysis it if the two links that is a trusted and untrusted link it is then compared after which the Ip of trusted and non-trusted site is compared.

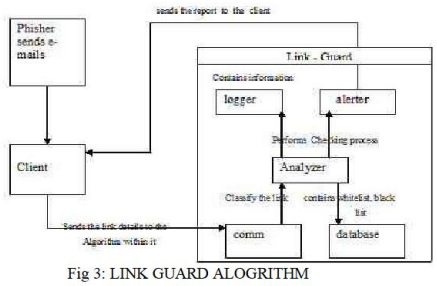

Fig 3: LINK GUARD ALOGRITHM

11. Intelligent Phishing Website Detection and Prevention System by Using Link Guard Algorithm

Ben Clark algorithm:

The complexity of a password decides how long it will take to crack it hence an algorithm to check the strength of password by finding its entropy, carnality is quit commonly used to determine if the password is strong without password being send to the computer this is achieved my detecting the amount if numbers, lower- and upper-case characters in the password.

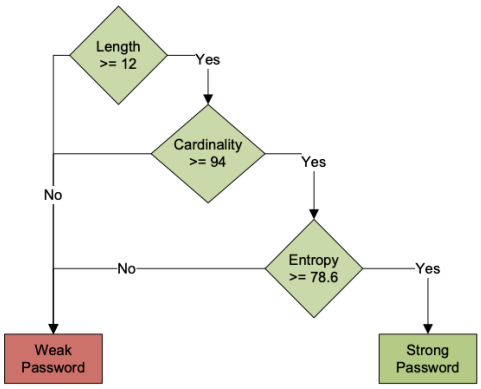

***Fig. 5** Decision Tree of algorithm's logic*

10 Rtfm: Red Team Field Manual. Ben Clark Algorithm To Ensure And Enforce Brute-Force Attack-Resilient Password In Routers

Current work:

With the above algorithm we can prevent unauthorized access by making the password strong to begin with or by checking if the link send is valid and safe or not but the question remain s h ow to save the data if account is compromised which we put forward a algorithm that uses encryption to encrypt the data in the account but the password is only one part of the encryption key we use the unique identifier imei number that is unique for every device to make a 2nd part of password using hashing to make a complete key that will be then used to decrypt the data in the case of lost password it would be possible only from the device where the account is registered and using hashing the imei is stored in separate secure server in case the password lost is of a company the account can be hardware locked and also location locked with location at very precious level

Conclusion and Future Work:

As the Internet became more mainstream and important to our life, it has become. More threatening for a person to be using the same password. Hence, in order to prevent this. Companies and businesses have started to implement group policies of having strong passwords. In both commercial and private spaces with large companies such as Google and Microsoft Using Password accounts now and using phones as verification. But one of the issues is that Even if password-less authentication works for your app, you may have to depend on the user having a password somewhere else in the end. In the case of brute force It is notice that even though it is possible to enforce policies in order to prevent brute force from breaking into online accounts, it is impossible to prevent it from breaking into accounts that are offline, such as compressed files which can be used for storing in important information as many organizations store extremely sensitive information in offline areas. Another issue. What was noticed was when storing passwords using hashing, which is a one-way method. In order to retrieve information, it was impossible. As the passwords or one way and hence the data encrypted by these sorts were impossible to retrieve.

Reference

1. https://www.password-depot.de/en/know-how/brute-force-attacks.htm
2. https://www.redteamsecure.com/terms-glossary/brute-force-attack-and-dictionary-attack#:~:text=Brute%2Dforce%20Attack%20and%20Dictionary,variations%20on%20a%20few%20passwords.
3. https://www.computerweekly.com/feature/The-problem-of-passwords-and-how-to-deal-with-it
4. https://security.stackexchange.com/questions/118147/how-are-gpus-used-in-brute-force-attacks
5. https://www.md5hashgenerator.com/
6. https://www.cnbc.com/2022/02/27/most-common-passwords-hackers-leak-on-the-dark-web-lookout-report.html
7. https://www.getcybersafe.gc.ca/en/blogs/phishing-introduction
8. https://www.paloaltonetworks.com/cyberpedia/what-is-malware#:~:text=As%20software%20designed%20to%20interfere,gain%20access%20to%20sensitive%20information
9. https://www.imperva.com/learn/application-security/social-engineering-attack/#:~:text=Social%20engineering%20is%20the%20term,in%20one%20or%20more%20steps.
10. Rtfm: Red Team Field Manual. Ben Clark Algorithm To Ensure And Enforce Brute-Force Attack-Resilient Password In Routers
11. Intelligent Phishing Website Detection and Prevention System by Using Link Guard Algorithm
12. Cynthia Dwork, Andrew Goldberg, and Moni Naor. On Memory-BoundFunctions for Fighting Spam. In Proc. Crypto 2003, 2003. [5] EarthLink.ScamBlocker.http://www.earthlink.net/software/free/toolbar/.
13. David Geer. Security Technologies Go Phishing. IEEE Computer, 38(6):18–21, 2005.
14. John Leyden. Trusted search software labels fraud siteas ˝safe˝.http://www.theregister.co.uk/2005/09/27/untrusted search/.
15. Microsoft. Sender ID Framework. http://www.microsoft.com/mscorp/safety/technologies/senderid/default.mspx.