e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:05/Issue:10/October-2023 Impact Factor- 7.868 www.irjmets.com

VERIFYING THE SECURITY OF GENEARL PASSWORD TECHNOLOGY

Kajal Dubey[*1]

[*1]B.Sc.Information Technology, B.K. Birla College, Kalyan, Maharashtra, India.

ABSTRACT

Password is becoming more essential part of our society as it occurs everywhere. A password is a personal key used to access a computer system or online account. It is a combination of characters, such as letters, numbers, and symbols, that give permission to user access while protecting with unauthorized access. Passwords are an essential part of security to protect sensitive information and gives privacy. It is very important to create strong and unique passwords to enhance your security. I conducted research on password security by exploring a tool to generate password lists and creating a random password list. Through analysis of the data from both manual and automated password lists, I was able to draw conclusions about the security of password technology. This helps identify any vulnerabilities or strengths in password protection methods.

Keywords: Passwords, Authorized individuals, Encryption, Strong Passwords, Vulnerabilities, Strengths.

I. INTRODUCTION

A password is your personal key to a computer system. Passwords help to ensure that only authorized individuals access computer systems. Passwords also help to determine accountability for all transactions and other changes made to system resources, including data also. In 1961, MIT computer science professor Fernando Corbato created the first digital password as a brilliant project problem-solver. When he built a giant time-sharing computer, several users needed their own private access to the terminals. This biggest problem have a smallest solution is ➔Give each user their own password. Bruce Schneier Password Safe was originally designed by Bruce Schneier and released as a free utility application. Since then, it has evolved considerably. The following table has links to pages detailing the release history of Password Safe since the project was made open source which means available for each an every one. People pick bad passwords, and either forget, write down, or resent good ones.[1]

A study by NordPass found that “password” was the fifth most popular password in 2020, used by 20,958,297 people universally. The top most four passwords of the year were “123456”, “123456789”, “12345”, and “qwerty”. We can protect data and password through encryption. Encryption is the process of encoding data in cryptography. Authentication protocols have been proposed that are resistant to password guessing attacks[2,3,4,5,6].

There are the two common techniques used to protect a password file :

- One-way encryption: One-way encryption is where the system stores only an encrypted form of the users password.
- Access control: Access control is where access to the password file is limited to one or very few accounts.

These attacks uses a pre-selected library of words and phrases to guess possible passwords. It operates under the assumption that users goes only to a basic list of passwords, such as "password," "123abc" and “123456”, etc. Few rules we can access to protect our data and password:

1. Use a phrase: Instead of a single word, create a longer phrase that is easy for you to remember but difficult for others to guess anyone.

2. Combining all things: Use a combination of uppercase and lowercase letters, numbers, and special characters in your password to protect it.

3. Avoid common patterns: Don't use sequential numbers or keyboard patterns like "zxcvb", “tyuiop”, or "123456".

4. Unique password for each platform: Avoid using the same password for multiple platform.

5. Enable two-factor authentication: Add an extra layer of security by enabling two-factor authentication whenever possible to give this access.

Note: For Remembering ➔ it's important to regularly update or change your passwords and keep them secure. For staying safe in online mode.

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:05/Issue:10/October-2023 Impact Factor- 7.868 www.irjmets.com

II. METHODOLOGY

Methodology of analysis and conclusions

❖ Here is the methodology followed by this research :

1. Researched for the tool to create a dictionary or password list generator.
2. Downloaded and setup the password list generator.
3. Created a manual password list which can be used generally.
4. Created a password list using password list generator.
5. Tallying the manual and automated password lists.
6. Taking out the conclusion if password technology is secured or not.

III. MODELING AND ANALYSIS

According to my analysis, I started by looking for a tool that could help to generate password lists. Researching various options is a great way to find the right tool for my needs. Once I found a suitable password list generator, I downloaded it and went through the setup process. This step is important to ensure that the generator is properly installed and ready to use according my needs. In addition to using the password list generator, I also created a random password list. This list can be used as a general reference for my research. Using the password list generator, I generated a password list automatically. This can save time and effort compared to manually creating the entire list. For comparing the effectiveness of the manual and automated password lists, I conducted a tally of the passwords in each list. This step helps me to understand differences or similarities between the two approaches. Through this analysis the data from the manual and automated password lists, I able to draw conclusions about the security of password technology. This evaluation will provide perception into the effectiveness of the generated passwords and their level of security. And after adding security measures, the info about this could even be published publically so it'll make them secure about their privacy. These are some staple items but another technique might be wont to enhance the safety of passwords.

IV. RESULTS AND DISCUSSION

Showing some results which, I did through this research. I took random 5 passwords through my personal information and after performing these all steps which I mentioned over in methodologies I got that 5 passwords over there which I took randomly in my mind sharing some results:

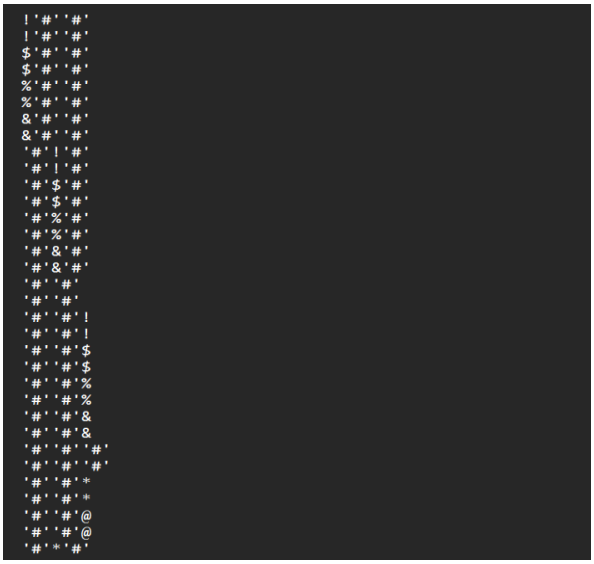

Figure 1: Analysis on Special Character.

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:05/Issue:10/October-2023 Impact Factor- 7.868 www.irjmets.com

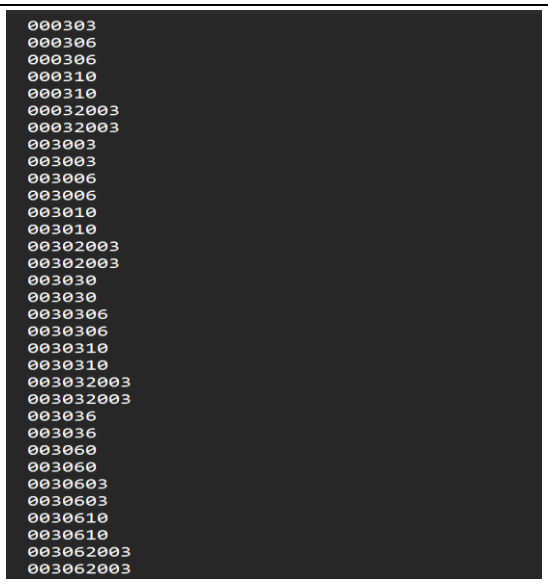

Figure 2: Analysis on D.O.B basis.

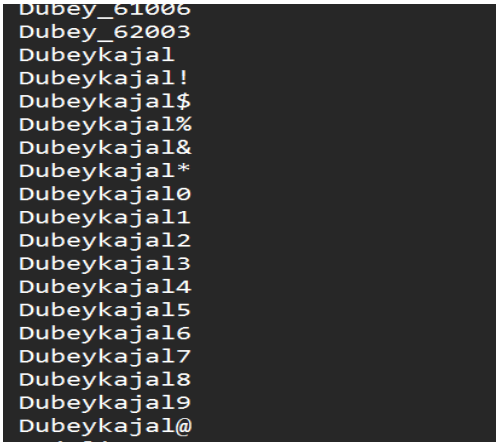

Figure 3: Analysis on Personal details[Name, S_name].

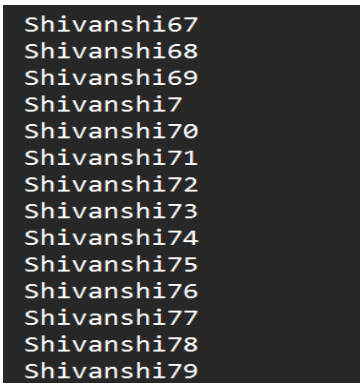

Figure 4: Analysis on Nickname Basis.

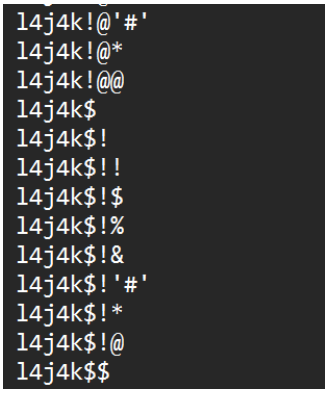

Figure 5: Analysis on Full Details Basis.

This is the complete research analysis. Firstly, I entered some values of my personal details like Name, Surname, Date of Birth, Nickname an all. After that I came to the conclusion that hackers can extract this password from our personal details so we should create a strong or different password except using our personal details. Normal users never get idea about the sanity of secured passwords so in order to make them secure developer should go with the mindset of securing their clients.

V. CONCLUSION

By all the proven results, we can conclude through this statement which is “we should set always strong password either its mix-up of uppercase and lowercase or don’t use that passwords which is correlated with

our personal details like [Name, Surname, D.O.B, Nick name or etc details]". People should always uses that type of password which is easily remember and tough to hackable.

ACKNOWLEDGEMENT

I would like to express my gratitude to my advisory Prof. Swapna Nikale who has give me this opportunity to publish the research paper as a part of curricular activity. Thanks to give support and deep guidance on writing this research paper.

VI. REFERENCES

[1] S. M. Bellovin and M. Merritt, "Encrypted Key Exchange: Password-Based Protocols Secure Against Dictionary Attacks", Proceedings of the LE.E.E. Symposium on Research in Security and Privacy, Oakland, May 19

[2] L. Gong, "Optimal Authentication Protocols Resistant to Password Guessing Attacks", Proceedings of the 8th IEEE Computer Security Foundations Workshop, County Kerry, Ireland, June 1995, pp. 24-29.

[3] T.M.A. Lomas, L. Gong, J.H. Saltzer, and R.M. Needham. Reducing Risks from Poorly Chosen Keys. In Proceedings of the 12th ACM Symposium on Operating System Principles, volume 23(5) of ACM Operating Systems Review, Pages 14-18, Litchfield Park, Arizona, December 1989.

[4] L. Gong, T.M.A. Lomas, R.M. Needham, and J.H. Saltzer. Protecting Poorly Chosen Secrets from Guessing Attacks. IEEE Journal on Selected Area in Communications, 11(5):648-656, June 1993.

[5] S. Bellovin and M. Merritt. Encrypted Key Exchange: Password-Based Protocols Secure Against Dictionary Attacks. In Proceedings of the IEEE Symposium on Research in Security and Privacy, pages 72-84, Oakland, California, May 1992.

[6] S. Bellovin and M. Merritt. Augmented Encrypted Key Exchange: A Password-Based Protocol Secure Against Dictionary Attacks and Password File Compromise. In Proceedings of the 1st ACM Conference on Computer and Communications Security, pages 244-250, Fairfax, Virginia, November 1993.