PASSWORD STRENGTH STUDY USING THE ZXCVBN ALGORITHM AND BRUTE-FORCE TIME ESTIMATION TO STRENGTHEN CYBERSECURITY

Whisnu Yudha Saputra[1*]; Sugiarti[2]; Haris Junianto[3]; Didit Suhartono[4].

Informatics[1, 2, 3, 4]
Amikom Purwokerto University, Banyumas, Indonesia[1, 2, 3, 4]
amikompurwokerto.ac.id[1, 2, 3, 4]
21sa1026@mhs.amikompurwokerto.ac.id[1*], 21sa1031@mhs.amikompurwokerto.ac.id[2],
21sa1002@mhs.amikompurwokerto.ac.id[3], didit@amikompurwokerto.ac.id[4]
(*) Corresponding Author

Abstract— *This research analyzes password strength based on its length and complexity using brute force attack simulations. The study begins with collecting password data from various sources to ensure sufficient variation in complexity levels. Next, the passwords are evaluated using the Zxcvbn algorithm, which provides a strength score as well as information about the time required to crack them. The same passwords are also evaluated using Brute-force Time Estimation to calculate the estimated time required to crack the password. After both algorithms have been evaluated, the results are analyzed to find the correlation between the Zxcvbn score and the estimated brute force time. The results of the data analysis are then visualized in the form of graphs or diagrams to facilitate understanding and assessment of password security. This simulation estimates the time required to guess a password, depending on the level of password complexity. Although the simulation results show that long and complex passwords are more secure, the actual strength of the password is highly dependent on the tools used by the attacker. In addition, digital security is not only limited to passwords, but also depends on various loopholes that can be exploited, such as personal data leaks or software vulnerabilities. Therefore, a comprehensive security approach is essential to protect users from potential cyberattacks. This study aims to provide in-depth insights into the strength and vulnerability of passwords and the effectiveness of algorithms in assessing password security.*

Keywords: *brute-force estimation, password, zxcvbn.*

Abstrak—*Penelitian ini menganalisis kekuatan password berdasarkan panjang dan kompleksitasnya dengan menggunakan simulasi serangan brute force. Penelitian ini dimulai dengan pengumpulan data password dari berbagai sumber untuk memastikan variasi yang cukup dalam tingkat kompleksitas. Selanjutnya, password tersebut dievaluasi menggunakan algoritma Zxcvbn, yang memberikan skor kekuatan serta informasi tentang waktu yang dibutuhkan untuk memecahkannya. Password yang sama juga dievaluasi menggunakan Brute-force Time Estimation untuk menghitung estimasi waktu yang diperlukan untuk memecahkan password. Setelah kedua algoritma melakukan evaluasi, hasilnya dianalisis untuk mencari korelasi antara skor Zxcvbn dan estimasi waktu brute force. Hasil dari analisis data kemudian divisualisasikan dalam bentuk grafik atau diagram untuk memudahkan pemahaman dan penilaian terkait keamanan password. Simulasi ini memperkirakan waktu yang diperlukan untuk menebak password, tergantung pada tingkat kompleksitas password. Meskipun hasil simulasi menunjukkan bahwa password yang panjang dan kompleks lebih aman, kekuatan password sebenarnya sangat bergantung pada alat atau tools yang digunakan oleh penyerang. Selain itu, keamanan digital tidak hanya terbatas pada password, tetapi juga bergantung pada berbagai celah yang bisa dimanfaatkan, seperti kebocoran data pribadi atau kelemahan perangkat lunak. Oleh karena itu, pendekatan keamanan yang komprehensif sangat penting untuk melindungi pengguna dari potensi serangan siber. Penelitian ini bertujuan memberikan wawasan mendalam mengenai kekuatan dan kerentanan password serta efektivitas algoritma dalam menilai keamanan password.*

Kata Kunci: *estimasi brute-force, zxcvbn, kata sandi.*

INTRODUCTION

In the rapidly evolving digital era, information security has become a critical issue (Kovba & Moiseenko, 2021). Amid the increasing use of the internet and online systems, threats to the security of personal and organizational data are becoming more complex. Therefore, protection is needed that is able to protect digital organizational infrastructure and individual data privacy (Temitayo Oluwaseun Abrahams et al., 2024), one of the main lines of defense used to protect digital information is a password (Kim & Lee, 2023). However, the reality shows that many users still use weak and easily guessable passwords, putting them at significant risk of cyberattacks (Rifai et al., 2023).

A strong password is not only the key to protecting user data, but also an important part of maintaining the overall integrity of the system (Sarkar & Nandan, 2022). As hacking methods like brute-force attacks become more sophisticated, techniques for evaluating and enhancing password strength become highly relevant. The Zxcvbn algorithm, designed to evaluate password strength based on character combinations, length, and patterns, has become a popular tool in helping users create stronger passwords (Hong et al., 2021). On the other hand, brute-force time estimates provide a realistic perspective on how quickly a password can be cracked by modern computers using the brute-force attack method. Brute force cracks passwords, login credentials and encryption keys using trial and error hacking (Sharaa & Thuneibat, 2024). Losses due to hacking are both financially and reputationally costly, cyber attacks can also result in huge losses in economic damage (Kokaji & Goto, 2022). Hackers can collect information based on search engines such as the web, tools and techniques used by hackers (Chudasama & Bhavsar, 2022). So it is essential for individuals and organizations to create effective protection strategies.

This research begins with the collection of password data from various sources to ensure sufficient variation in complexity levels. Next, the password is evaluated using the Zxcvbn algorithm, which provides a strength score and information about the time required to crack it. Then, the same password is also evaluated using Brute-force Time Estimation to calculate the estimated time needed to crack the password using the brute-force method. After both algorithms performed the evaluation, the results were analyzed to find the correlation between the Zxcvbn score and the brute-force time estimate. Finally, the results of the data analysis will be visualized in the form of graphs or diagrams to facilitate understanding and assessment related to password security.

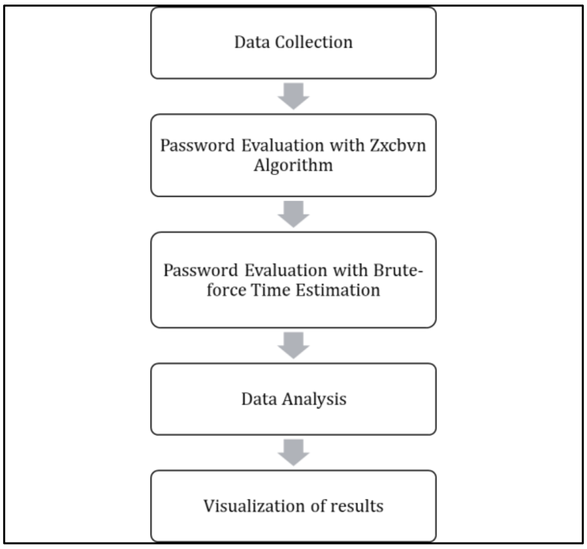
This research focuses on evaluating password strength using a combination of the Zxcvbn algorithm and Brute-force Time Estimation. The goal is to identify common weaknesses in passwords and provide an understanding of how effective this algorithm is in measuring password security levels. Additionally, this research aims to analyze the algorithm's performance under various password conditions, ranging from simple to highly complex, as well as how the estimated brute-force time can give an indication of the difficulty level in breaching the password's security.

In previous research, the John the Ripper program which implemented the modified zxcvbn algorithm was proven to be able to reduce the password hacking ratio for end users and admins, but this can be useful if the program provides a fairly good estimate of password strength for users (Sedláček, 2022). Apart from that, the use of brute-force techniques is a powerful way to access data which over time has been modified and released by cybercriminals (Verma et al., 2022).

Through this research, it is hoped to make a significant contribution to developing more effective cybersecurity strategies, particularly in the context of creating passwords that are resistant to cyber attack threats. The combination of Zxcvbn and brute-force time estimation will not only help users and developers understand the importance of strong passwords but also provide a stronger foundation for enhancing security in the continuously evolving digital environment.

MATERIALS AND METHODS

Research Flow


Data Collection
Password Evaluation with Zxcbvn Algorithm
Password Evaluation with Brute-force Time Estimation
Data Analysis
Visualization of results

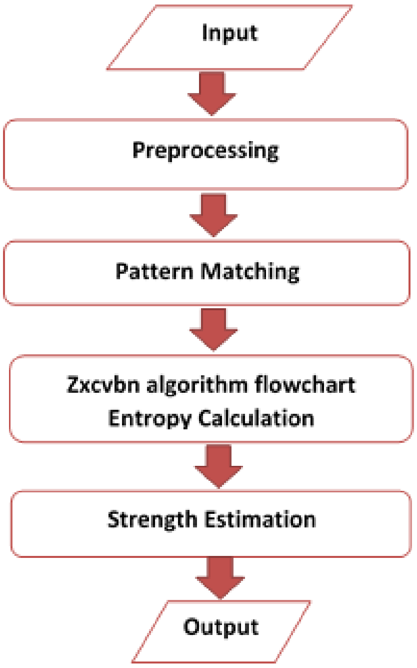
Source: (Research Results, 2024)

Figure 1. Research Flow

Based on Table 1, this research begins with the collection of password data from various sources to obtain a variety of complexities. Then, the password is evaluated using the Zxcvbn algorithm to measure its strength, followed by an evaluation using Brute-force Time Estimation to measure the cracking time. The evaluation results are analyzed to find the correlation between the Zxcvbn score and the brute-force time estimation. Finally, all these findings will be visualized in graphs or diagrams, providing clear insights into the strength and vulnerability of passwords and the importance of using strong passwords.

Zxcvbn

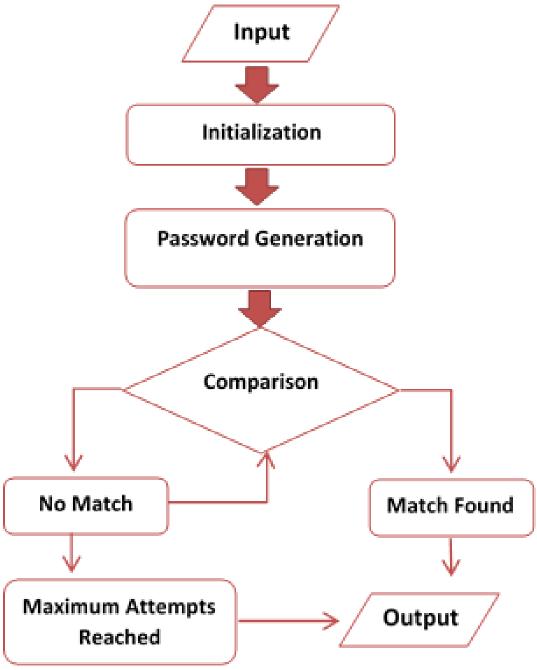
The Zxcvbn algorithm is an algorithm used to measure password strength, based on the number of arrangement patterns from the password entropy calculation. The assumption of password entropy is conservative and serves as a barrier measure (Chowdhury, 2024). This algorithm is designed to provide a realistic estimate of how easily a password can be guessed by an attacker. Zxcvbn considers various patterns, such as the use of common words, letter-to-number substitutions, keyboard sequences, and other patterns, thereby providing a more accurate assessment compared to traditional methods like counting password length and complexity. The flowchart which describes Zxcvbn Algorithm can be seen in Figure 2 below:



Source: (Research Results, 2024)
Figure 2. Zxcvbn Algorithm Flowchart

Brute-force Time Estimation

Brute-force Time Estimation Algorithm is a method used to solve problems by testing each possibility one by one until the correct solution is found (Alkhwaja et al., 2023). The process of Brute-Force Time Estimation is explained in the flowchart in Figure 3. Which explains the Brute Force algorithm solves the problems in a very simple, easy and uncomplicated way. This algorithm is often implemented to calculate the time required to crack a password by trying all possible character combinations randomly. Brute-force attacks typically focus on cracking passwords and decrypting encryption keys, exploiting computational power to guess various sequences of possible combinations (Sharaa & Thuneibat, 2024).

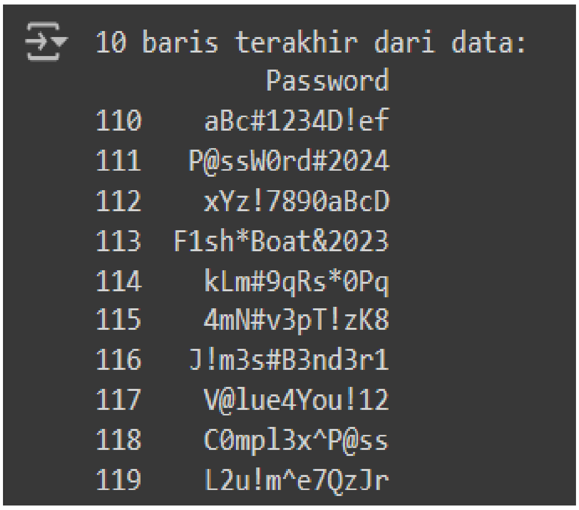


Source: (Research Results, 2024)
Figure 3. Brute-Force Time Estimation Flowchart

RESULTS AND DISCUSSION

Data

The author collected data from the Kaggle Common Passwords dataset, which consists of 10,000 entries. From this dataset, the author performed a selection based on character length and character type, including combinations of letters and numbers, combinations of numbers and punctuation, combinations of letters and punctuation, and combinations of all three. This selection process aims to cover various conditions and levels of password complexity, ranging from simple to more complex. This variation is important to ensure that the research includes the types of passwords commonly used by users and provides relevant results regarding password strength. From the selection of the data, 120 password entries were obtained, which will subsequently undergo strength testing as shown in Figure 4 Password Data Sample.



```
10 baris terakhir dari data:
          Password
110    aBc#1234D!ef
111   P@ssW0rd#2024
112    xYz!7890aBcD
113  F1sh*Boat&2023
114    kLm#9qRs*0Pq
115    4mN#v3pT!zK8
116   J!m3s#B3nd3r1
117    V@lue4You!12
118    C0mpl3x^P@ss
119    L2u!m^e7QzJr
```

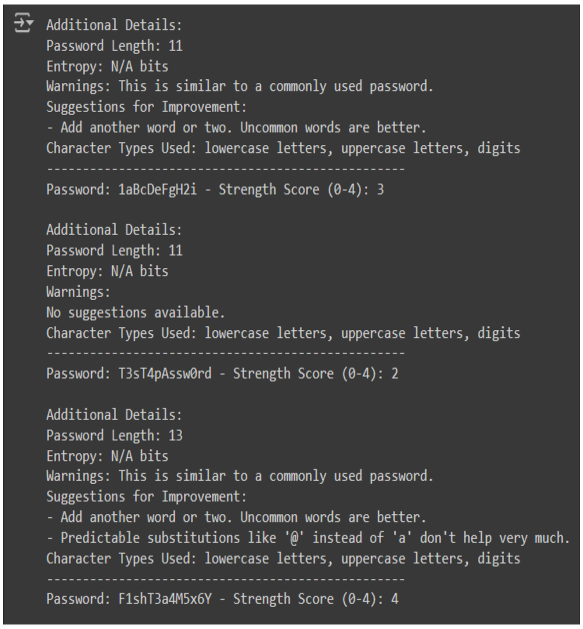
Source: (Research Results, 2024)

Figure 4. Password Data Sample

Password Evaluation with Zxcvbn Algorithm

At this stage, each password is tested using the zxcvbn function, which then generates a strength score on a scale of 0 to 4. This scale indicates the strength of the password, where a score of 0 means very weak and a score of 4 means very strong. In addition to the score, the algorithm also provides additional details such as entropy, which measures the level of randomness of the password in bits, as well as warnings if the password contains certain weaknesses, such as the use of easily guessable patterns. If the password is weak, the algorithm offers suggestions to strengthen it, such as adding special characters or avoiding the use of common words.

The algorithm also checks the types of characters used in the password, such as lowercase letters, uppercase letters, numbers, and symbols. The more varied the types of characters used, the more complex the password becomes. At this stage, it also allows for bulk password evaluation, where passwords are read from a CSV file and analyzed one by one. Each evaluation result displays the strength score, entropy, warnings, and the combination of characters used, providing a more detailed picture of the security of the tested password. With this approach, Zxcvbn provides a more in-depth evaluation and helps users understand how difficult their passwords are to crack. The following Figure 5 shows the results of password testing using the Zxcvbn algorithm, where the results indicate how each password is analyzed and scored based on its strength.



```
Additional Details:
Password Length: 11
Entropy: N/A bits
Warnings: This is similar to a commonly used password.
Suggestions for Improvement:
- Add another word or two. Uncommon words are better.
Character Types Used: lowercase letters, uppercase letters, digits
--------------------------------------------------
Password: 1aBcDeFgH2i - Strength Score (0-4): 3

Additional Details:
Password Length: 11
Entropy: N/A bits
Warnings:
No suggestions available.
Character Types Used: lowercase letters, uppercase letters, digits
--------------------------------------------------
Password: T3sT4pAssw0rd - Strength Score (0-4): 2

Additional Details:
Password Length: 13
Entropy: N/A bits
Warnings: This is similar to a commonly used password.
Suggestions for Improvement:
- Add another word or two. Uncommon words are better.
- Predictable substitutions like '@' instead of 'a' don't help very much.
Character Types Used: lowercase letters, uppercase letters, digits
--------------------------------------------------
Password: F1shT3a4M5x6Y - Strength Score (0-4): 4
```

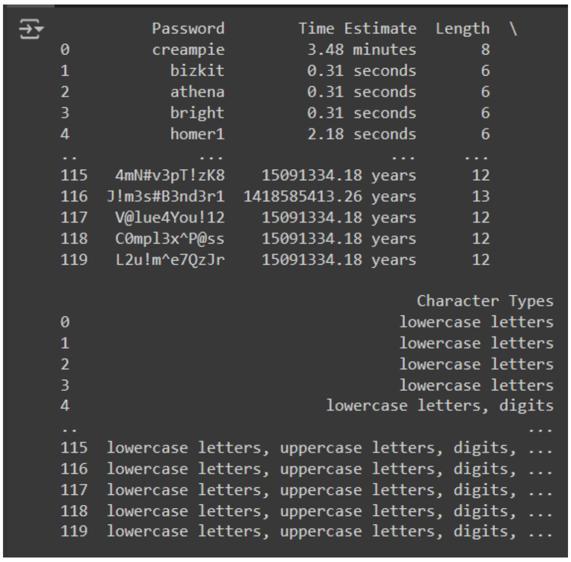
Source: (Research Results, 2024)

Figure 5. Password Testing Using the Zxcvbn Algorithm

Password Evaluation with Brute-force Time Estimation Algorithm

In the Password Evaluation stage using the Brute Force Algorithm, the approach used is to estimate how long it would take to guess a password using the brute-force method, which involves trying every possible combination of characters sequentially until the password is found. This algorithm considers the character size used in the password, such as lowercase letters, uppercase letters, numbers, and symbols. Based on the characters present in the password, the algorithm will calculate the number of possible combinations. The first step is to determine the size of the character set used. For example, if a password only contains lowercase letters, the size of the character set is 26 (for the letters a to z). If the password also contains numbers or symbols, the size of the character set will increase according to the types of characters involved. The length of the password is then combined with the size of the character set to generate the possible number of combinations. After calculating the total combinations, the algorithm then divides that number by the brute-force attack speed (in this case, assumed to be 1 billion attempts per second) to produce an estimated time required. The time estimation results are converted into various time units, such as seconds, minutes, hours, days, or even years, depending on the magnitude of the results as shown in Figure 6. The Password Testing

Process using the Brute-force Time Estimation Algorithm.



```
            Password        Time Estimate  Length  \
0           creampie         3.48 minutes       8
1             bizkit         0.31 seconds       6
2             athena         0.31 seconds       6
3             bright         0.31 seconds       6
4             homer1         2.18 seconds       6
..               ...                  ...     ...
115     4mN#v3pT!zK8    15091334.18 years      12
116    J!m3s#B3nd3r1  1418585413.26 years      13
117     V@lue4You!12    15091334.18 years      12
118     C0mpl3x^P@ss    15091334.18 years      12
119     L2u!m^e7QzJr    15091334.18 years      12

                                          Character Types
0                                      lowercase letters
1                                      lowercase letters
2                                      lowercase letters
3                                      lowercase letters
4                              lowercase letters, digits
..                                                    ...
115  lowercase letters, uppercase letters, digits, ...
116  lowercase letters, uppercase letters, digits, ...
117  lowercase letters, uppercase letters, digits, ...
118  lowercase letters, uppercase letters, digits, ...
119  lowercase letters, uppercase letters, digits, ...
```

Source: (Research Results, 2024)

Figure 6. The Password Testing Process Using the Brute-Force Time Estimation Algorithm

Result Analysis

1. Zxcvbn Algorithm Result Analysis

Table 1. Zxcvbn Algorthm Result Analysis

Password	Score	Length	Character Types	
456321	0	6	digits	
kahlua	1	6	lowercase letters	
front242	1	8	lowercase letters, digits	
23031990	1	8	digits	
patience	1	8	lowercase letters	
2031982	1	8	digits	Explanation of Score:
Batman	0	6	lowercase letters, uppercase letters	0: Very Weak
fuck69	1	6	lowercase letters, digits	1: Weak
1a2b3c4d	1	8	lowercase letters, digits	2: Fairly Strong
654321	0	6	digits	3: Strong
taylor	0	6	lowercase letters	4: Very Strong
Letmein1	1	8	lowercase letters, uppercase letters, digits	
r2d2c3po	1	8	lowercase letters, digits	
billyboy	1	8	lowercase letters	
F1shT3a4M5x6Y	4	13	lowercase letters, uppercase letters, digits	
Q1u2i3c4k5S6	4	12	lowercase letters, uppercase letters, digits	
aBc#1234D!ef	4	12	lowercase letters, uppercase letters, digits, symbols	
F1sh*Boat&2023	4	14	lowercase letters, uppercase letters, digits, symbols	

Source: (Research Results, 2024)

The results of the password testing in Table 1. The analysis results of the Zxcvbn Algorithm show variations in password strength levels based on their characteristics. Passwords with only numbers or lowercase letters, such as 456321, Batman, and Taylor, have a score of 0 or 1, which means these passwords are classified as very weak or weak, because they are easy to predict and can be hacked using brute-force methods. Passwords that consist only of numbers, such as 23031990 and 2031982, are also considered weak even though they are of sufficient length. Passwords with a combination of uppercase letters, lowercase letters, numbers, and symbols, such as F1shT3a4M5x6Y and F1sh*Boat&2023, score 4, indicating that these passwords are very strong. A combination of more complex characters and a longer password increases security, as it multiplies the number of combinations that hackers need to guess (Kheshaifaty & Gutub, 2021). This analysis shows the importance of using character variations and sufficiently long passwords to avoid security vulnerabilities.

2. Time Estimation Brute-Force Algorithm Analysis Result

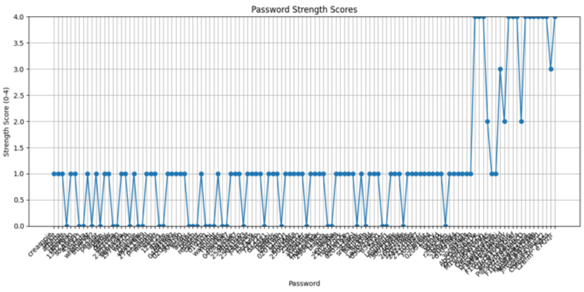
Table 2 Time Estimation Brute-Force Algorithm Analysis Result

Password	Time Estimate	Time (seconds)	Length	Character Types
homer1	2.18 seconds	2,176782336	6	lowercase letters, digits
southern	3.48 minutes	208,8270646	8	lowercase letters
456321	0.00 seconds	0,001	6	digits
front242	47.02 minutes	2821,109907	8	lowercase letters, digits
Victoria	14.85 hours	53459,72853	8	lowercase letters, uppercase letters
Thomas	19.77 seconds	19,77060966	6	lowercase letters, uppercase letters

Password	Time Estimate	Time (seconds)	Length	Character Types
AbcD3fG7hI9	1650.07 years	52036560684	11	lowercase letters, uppercase letters, digits
F1shT3a4M5x6Y	6342863.37 years	2,00029E+14	13	lowercase letters, uppercase letters, digits
Q1u2i3c4k5S6	102304.25 years	3,22627E+12	12	lowercase letters, uppercase letters, digits
aBc#1234D!ef	15091334.18 years	4,7592E+14	12	lowercase letters, uppercase letters, digits, symbols
P@ssW0rd#2024	1418585413.26 years	4,47365E+16	13	lowercase letters, uppercase letters, digits, symbols
C0mpl3x^P@ss	15091334.18 years	4,7592E+14	12	lowercase letters, uppercase letters, digits, symbols
L2u!m^e7QzJr	15091334.18 years	4,7592E+14	12	lowercase letters, uppercase letters, digits, symbols

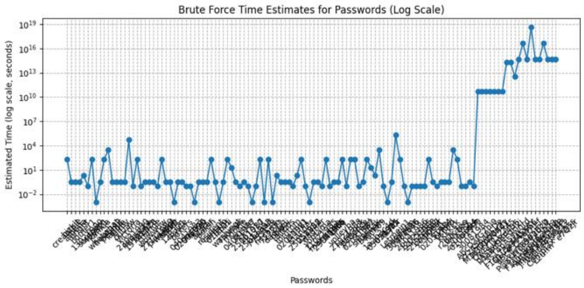
Source: (Research Results, 2024)

The test results in Table 2, Brute-Force Time Estimation Algorithm Analysis Results show that simple passwords consisting of only lowercase letters or numbers, such as homer1 and 456321, are very vulnerable to brute-force attacks and can be cracked in seconds. Passwords that combine uppercase and lowercase letters, such as Victoria and Thomas, are slightly stronger, but can still be cracked in a relatively short period of time, ranging from a few minutes to hours. On the other hand, more complex passwords with a combination of uppercase, lowercase letters, numbers, and symbols, such as AbcD3fG7hI9 and F1shT3a4M5x6Y, show a much longer estimated brute-force time, ranging from thousands to millions of years. Long and complex passwords, such as P@ssW0rd#2024 and L2u!m^e7QzJr, offer a very high level of security, with estimated brute-force times that can reach hundreds of millions to billions of years. Overall, the use of passwords that are long and contain a variety of character types is highly recommended to increase security from brute-force attacks (Verma et al., 2022).



Source: (Research Results, 2024)
Figure 7. Visualization Graph of Brute-Force Estimation Algorithm Test Results

Figure 7 Visualizes the Brute-Force Estimation Algorithm Test Results graph, showing password strength score assessed on a scale of 0 to 4. Many passwords at the bottom of the graph tend to have low scores, with most ranging around 0.5 to 1. However, there are some passwords that have scores close to 4, indicating that there is some variation in password strength within the dataset. The right graph shows the approximate time taken to guess the passwords by brute force, using a logarithmic scale (seconds). The estimated time to guess most passwords ranges from 0.01 seconds to 100 million seconds (approximately 3.17 years), but there are some passwords that take billions of years to guess, indicating that they are much harder to guess. Overall, most passwords appear to be relatively weak, but there are some passwords that are strong enough to withstand brute force attacks for very long periods of time.



Source: (Research Results, 2024)
Figure 8. Visualization Graph of Zxcvbn Algorithm Testing Results

Figure 8 visualizes the Zxcvbn Algorithm testing results graph, where the analysis shows that passwords considered strong are generally at least 12 characters long. This length is considered more secure because it significantly increases the time required for brute-force attacks. The Zxcvbn algorithm, for instance, estimates the time required to crack a password based on its length and complexity. Longer passwords exponentially increase this time, making them more resistant to brute-force attempts.

In addition to length, passwords that use a variety of character types, such as a combination of uppercase letters, lowercase letters, numbers, and symbols (e.g., punctuation marks), are also considered stronger. This combination of character types increases complexity and reduces the likelihood of a password being easily guessed (Chakraborty et al., 2022). Thus, to obtain a strong password, it is recommended to use at least 8 characters with a variety of uppercase letters, lowercase letters, numbers, and symbols (Blancaflor et al., 2021).

CONCLUSION

Based on testing and analysis on a total of 120 test data passwords with various conditions, the results show that longer and more complex passwords take much longer to crack using the brute-force method compared to simple passwords. Passwords with more diverse character combinations show a higher level of security in the face of various hacking scenarios, so it can be concluded that the strength of a password is greatly influenced by its length and complexity. Passwords that are at least 12 characters long and combine uppercase letters, lowercase letters, numbers, and symbols prove to be more difficult to guess, especially in the face of brute force attacks. Conversely, passwords that are too short or only use one type of character are more vulnerable to attacks and can be guessed in a much shorter time. However, it is important to note that this research is only a simulation, and the actual strength of the password is highly dependent on the tools used by the attacker. Even the most sophisticated security systems can be compromised if users lack the necessary training and awareness (Ozkan-okay et al., 2023). In addition, hacking is not only done through passwords, but can also take advantage of various other gaps from users, such as personal data leaks, use of insecure software, or other security omissions. Therefore, maintaining digital security requires a holistic approach, including strengthening passwords and paying attention to other security practices.

REFERENCE

Alkhwaja, I., Albugami, M., Alkhwaja, A., Alghamdi, M., Abahussain, H., Alfawaz, F., Almurayh, A., & Min-Allah, N. (2023). Password Cracking with Brute Force Algorithm and Dictionary Attack Using Parallel Programming. *Applied Sciences (Switzerland)*, *13*(10). https://doi.org/10.3390/app13105979

Blancaflor, E. B., Dela Cruz, M. R. A., Espanola, J. M. V., Laurena, L. R. V., Maranan, J. W. J., & Pinza, M. G. D. (2021). Password Strength Assessment on a Laptop Device using an Online Password Recovery Tool Cain & Abel. *ACM International Conference Proceeding Series*, 16–22. https://doi.org/10.1145/3483816.3483820

Chakraborty, N., Mukherjee, M., Li, J., Shojafar, M., & Pan, Y. (2022). Cryptanalysis of a Honeyword System in the IoT Platform. *IEEE Internet of Things Journal*, *9*(4), 2614–2626. https://doi.org/10.1109/JIOT.2021.3080676

Chowdhury, A. N. (2024). Analyzing Password Strength: A Combinatorial Entropy Approach. *Conference: The 22nd International Conference on Computer and Information Technology*, *January*. https://doi.org/10.5281/zenodo.10487696

Chudasama, D., & Bhavsar, R. (2022). Technical Methods of Information Gathering. *Journal of Web Engineering and Technology*, *8*(3), 1–5. https://doi.org/10.37591/JoWET

Hong, K. H., Kang, U. G., & Lee, B. M. (2021). Enhanced Evaluation Model of Security Strength for Passwords Using Integrated Korean and English Password Dictionaries. *Security and Communication Networks*, *2021*. https://doi.org/10.1155/2021/3122627

Kheshaifaty, N., & Gutub, A. (2021). Engineering Graphical Captcha and AES Crypto Hash Functions for Secure Online Authentication. *Journal of Engineering Research*, 69–80. https://doi.org/10.36909/jer.13761

Kim, S. J., & Lee, B. M. (2023). Multi-Class Classification Prediction Model for Password Strength Based on Deep Learning. *Journal of Multimedia Information System*, *10*(1), 45–52. https://doi.org/10.33851/jmis.2023.10.1.45

Kokaji, A., & Goto, A. (2022). An analysis of economic losses from cyberattacks: based on input–output model and production function. *Journal of Economic Structures*, *11*(1). https://doi.org/10.1186/s40008-022-00286-4

Kovba, D. M., & Moiseenko, Y. Y. (2021). The Digital Society in the 21st Century: Security Issue. *KnE Social Sciences*, *2020*, 444–451. https://doi.org/10.18502/kss.v5i2.8387

Ozkan-okay, M., Yilmaz, A. A., Akin, E., Aslan, A., & Aktug, S. S. (2023). A Comprehensive Review of Cyber Security Vulnerabilities ,. *Electronics*, *12*(1333).

Rifai, A., Meliyani, A., Chyntia, P., & Sakti, I. A. (2023). Penerapan Metode Technology Threat Avoidance Theory Terhadap Tingkat Kesadaran Data Privasi Pengguna Media Sosial. *Journal of Information System Research (JOSH)*, *4*(3), 1026–1032. https://doi.org/10.47065/josh.v4i3.3081

Sarkar, S., & Nandan, M. (2022). Password Strength Analysis and its Classification by Applying Machine Learning Based Techniques. *2022 2nd International Conference on Computer Science, Engineering and Applications, ICCSEA 2022*, *April*, 4–9. https://doi.org/10.1109/ICCSEA54677.2022.9936117

Sedláček, J. (2022). Empirical evaluation of passwords : influence of the modified zxcvbn. *Linz : Trauner Verlag*, 269–276. https://doi.org/https://doi.org/10.35011/IDIMT-2022-269

Sharaa, B. Al, & Thuneibat, S. (2024). Ethical hacking: real evaluation model of brute force attacks in password cracking. *Indonesian Journal of Electrical Engineering and Computer Science*, *33*(3), 1653–1659. https://doi.org/10.11591/ijeecs.v33.i3.pp1653-1659

Temitayo Oluwaseun Abrahams, Sarah Kuzankah Ewuga, Samuel Onimisi Dawodu, Abimbola Oluwatoyin Adegbite, & Azeez Olanipekun Hassan. (2024). A Review of Cybersecurity Strategies in Modern Organizations: Examining the Evolution and Effectiveness of Cybersecurity Measures for Data Protection. *Computer Science & IT Research Journal*, *5*(1), 1–25. https://doi.org/10.51594/csitrj.v5i1.699

Verma, R., Dhanda, N., & Nagar, V. (2022). Enhancing Security with In-Depth Analysis of Brute-Force Attack on Secure Hashing Algorithms. *Proceedings of Trends in Electronics and Health Informatics*, 513–522. https://doi.org/10.1007/978-981-16-8826-3_44