Universiti Teknologi MARA
Cawangan Melaka

PCMJ

Progress in Computing and Mathematics Journal

volume 1

https://fskmjebat.uitm.edu.my/pcmj/

Progress in Computing and Mathematics Journal
College of Computing, Informatics, and Mathematics
Universiti Teknologi MARA Cawangan Melaka, Kampus Jasin
77300, Merlimau, Melaka Bandaraya Bersejarah

PCMJ

Progress in Computing and Mathematics Journal

volume 1

Progress in Computing and Mathematics Journal (PCMJ)
College of Computing, Informatics, and Mathematics
Universiti Teknologi MARA Cawangan Melaka, Kampus Jasin
77300, Merlimau, Melaka Bandaraya Bersejarah

EDITORS

PCMJ
Progress in Computing and Mathematics Journal
volume 1

PREFACE

Welcome to the inaugural volume of the **Progress in Computing and Mathematics Journal (PCMJ)**, a publication proudly presented by the College of Computing, Informatics, and Mathematics at UiTM Cawangan Melaka.

This journal represents a significant step in our commitment to fostering a vibrant research culture, initially providing a crucial platform for our undergraduate students to showcase their intellectual curiosity, dedication to scholarly pursuit, and potential to contribute to the broader academic discourse in the fields of computing and mathematics. However, we envision PCMJ evolving into a beacon for researchers both nationally and internationally. We aspire to cultivate a space where groundbreaking research and innovative ideas converge, fostering collaboration and intellectual exchange among established scholars and emerging talents alike.

The manuscripts featured in this first volume, predominantly authored by our undergraduate students, are a testament to the hard work and dedication of these budding researchers, as well as the guidance and support provided by their faculty mentors. They cover a diverse range of topics, reflecting the breadth and depth of research interests within our college, and set the stage for the high-quality scholarship we aim to attract in future volumes.

As editors, we are honored to have played a role in bringing this journal to fruition. We extend our sincere gratitude to all the authors, reviewers, and members of the editorial board for their invaluable contributions. We also acknowledge the unwavering support of the college administration in making this initiative possible.

We hope that PCMJ will inspire future generations of students and researchers to embrace research and innovation, to push the boundaries of knowledge, and to make their mark on the world of computing and mathematics.

Editors
Progress in Computing and Mathematics Journal (PCMJ)
College of Computing, Informatics, and Mathematics
UiTM Cawangan Melaka

TABLE OF CONTENTS

PCMJ

Progress in Computer and Mathematics Journal (PCMJ)
volume 1 [October, 2024]
e-ISSN: 3030-6728
Website: fskmjebat.uitm.edu.my/pcmj

COMPARATIVE ANALYSIS OF PASSWORD CRACKING TOOLS

AHMAD SYAHIR AMZAR BIN ZULKAFLI
Universiti Teknologi Mara
syahirzulkafli7401@gmail.com

Article Info

Received: February 2024
Accepted: August 2024
Available Online: October 2024

Abstract

This comparative analysis aims to evaluate and compare various password cracking tools that are available in the market to provide an insight of its effectiveness, capabilities, and efficiency as well as provide a clear guideline of the best way on how to mitigate the risk from being the victim of password attack. The research methodology involves testing and analysing most famous password cracking tools which as John the Ripper, Hashcat, WPScan, and Hydra. The tools will be evaluated based on its performance, success rate, etc. Other than that, this project will also performing a wide variety of password attacking method such as brute force, rule based, and etc to assess their performance and effectiveness of each tool. Overall, this comparative analysis seeks to give a comprehensive understanding of password cracking tools which can be contribute to the field of cybersecurity by identifying the most effective tools and technique. In the end, a complete guideline on the best password practices can be used to avoid from any threat from password attack.

Keywords: Password cracking tools, Hashcat, John the Ripper, WPScan, Hydra, Comparative analysis

INTRODUCTION

Based on Yisa, Baba, Olaniyi (2016), password cracking can be defined as the recovery of plaintext passwords from an encrypted file where it is stored. Password has been widely used as a main choice of authentication in various type of medium such as computers, network, smart door lock, and bank account. However, the increasing number of password cracking techniques and tools has posed a significant threat for everyone to ensure their password is secure. According to Tobias Lundberg (2019), human tend to choose a password that they can be easily remembered and use the password on many things instead of choosing a password randomly. This is because they want to avoid forgetting their password.

You can easily change the formatting of selected text in the document text by choosing a look for the selected text from the Quick Styles gallery on the Home tab. You can also format text directly by using the other controls on the Home tab. Most controls offer a choice of using

the look from the current theme or using a format that you specify directly (Li & Gramatica, 2020; Tropsha, 2021).

What makes this project interesting is that it addresses the vulnerabilities associated with password and can enhance the overall password security using password cracking tools. According to Caitlin Jones (2022), over 61% cases of data breach happened in 2022 cause of compromised passwords and username. The result, it causes a breach of sensitive information being exposed in the public. One notable case that are shocking the world was Yahoo data breach that occurred in 2013 and 2014 which affected billion of user accounts. This breach associated with weak passwords practices that are easily guessable password by the hacker to gain access to Yahoo's system by exploiting weak passwords used by Yahoo's employees.

LITERATURE REVIEW

Alongside the evolution of password cracking tools and methods. It is inevitable that there are plenty of research and analysis on comparing different kind of password cracking tools that are available in the market. However, the goal of the pass studies and this particular analysis is quite similar.

RESEARCH ARTICLE 1

In research done by Shejina Nazar and Rini Kurian (2021), where there comparing other tools such as Hydra, WPScan, and Nerack by using only brute force attack to see which tools are faster and more efficient when performing brute force attack to crack a password. However, the comparative analysis only focusses on one attacking method while using different kind of tools to test the effectiveness of the tools.

RESEARCH ARTICLE 2

Other research made by Disha Pahuja and Prerna Sidana (2021), where using several applications, cracking methods in Kali Linux Operating System. In this research, they used

Hashcat, John the Ripper and Fcrackzip as their tools to compare. They are cracking password through various types of lengths and combinations to find the most effective tools between those three. Similar to research article 1, this analysis also using 1 type of attack which is brute force to test out the effectiveness of the tools when performing this type of attack.

RESEARCH ARTICLE 3

Older research was done by John A. Chester (2015), where he examined the nature of password cracking and modern applications. In the research paper, he studies several applications, methods of cracking across different medium. In 40 this comparison, he uses John the Ripper, RainbowCrack, Cain and Abel, LOphtCrack, Aircrack-NG, and Hashcat by performing dictionary attack, brute force, and rainbow tables attack.

RESEARCH ARTICLE 4

Other related works include that Han, Wong, and Chao (2014) where they perform a survey on password cracking methods, import technologies of password cracking, and the countermeasures against password cracking. Throughout this research, they aim to spread the knowledge about computer security and password cracking to common audiences as well as IT security professionals. This research on the other hand only discusses about password cracking method used by hacker. There is no demonstration on how these attacks perform when using password cracking tools.

RESEARCH ARTICLE 5

This research article was written by Bakker, M., Jagt, R. (2010) where they are testing on effect of GPU in password cracking. Tools that used in this project is BarsWF bruteforce, Extreme GPU Bruteforcer, IGHASHGPU, and Elcommsoft which allow to brute force password using multiple GPUs simultaneously. According to them, tools such as John the Ripper, Cain, and Able does not support GPU-based cracking. Throughout the research, they use various range of hashes such as NTLM, DCC, MD5, and Oracle 11g. In this study, they use four high end GPU to find the most reliable result. Based on the result, there are significant

different between actual performance gain between GPU versus CPU based password cracking. This is due to large amounts of processing cores available in a GPUs.

PROPOSED RESEARCH

As for this comparative study, Hashcat, John the Ripper, and Aircrack-NG will be used the tools that will be compared together using various kind of attack method such as brute force, rainbow tables, hybrid attack and rule-based attack. 41 This research aims to provide a comprehensive analysis on how these password cracking tools perform towards different kind of attack. In the end, this analysis will provide an outcome on which are the best tools can be used on certain circumstances.

METHODOLOGY

There are 2 categories of password cracking tools which is online and offline. The frequency of online attack is not as much as offline attack as it requires more skills and sometimes impossible to crack as it layered by many types of security protection (Yisa, Baba, and Olaniyi, 2016). They also add that offline attack is used when the hacker has the access to the password database and try to decrypt the password without any direct interaction with the website. This project will use 2 offline password cracking tools and 2 online password cracking tools.

HASHCAT

A free password cracking tools for Windows, MacOS, and Linux that is quite powerful. Named as the world's fastest and most advanced password recovery utility, it uses rule-based attack mechanism and multi-threading. Hashcat supports a broad range of Chester 7 hashes. Besides, Hashcat manages to come up with workable and convincing solution to crack passwords by using precomputed word references, rainbow table and even a brute force attack. Moreover, it also includes a built-in benchmarking system, a thermal watchdog, and support for more than 200 hash types that are implemented with speed 7 improvement. Hashcat Mask Attack is frequently preferred by users over Hashcat brute force attack since it tends to finish the procedure much quicker and effectively by limiting the keyspace of passwords. Other than

that, secret key representation in Hashcat is mostly associated with hash keys such as MD-5, SHA, and WHIRLPOOL.

JOHN THE RIPPER

Develop by Openwall, John the Ripper is an open-source software and considered as one of the most popular password cracking tools. It is accessible on many platforms such as Unix/Linux, Windows, MacOS, OpenVMS. John the Ripper supports hundreds of hash and cipher type such as MD-5, SHA-1, and SHA-256. It was created primarily to detect weaknesses in UNIX passwords but also can be used to crack poor Windows LM hashes. Dictionary attack is one of the simplest ways to crack a password, hence, John the Ripper can fully utilize it. It uses words from a word list that are typically found in dictionaries to test text 48 strings. However, John the Ripper has no capabilities to perform vulnerability analysis.

HYDRA

Hydra is one of the most powerful brute-force online password crackers. The amount of protocol supported by Hydra is significant when compared to its competitors which is up to 50 protocols such as Apple Filing Protocol (AFP), Cisco Authentication Authorization and Accounting (AAA), HTTP, HTTPS, and MySQL. It is written in Java and can be run in Linux or Unix, Mac OS, and Windows. Since this tool is open source, hence, it can be easily expanded to provide more support of protocols and applications in the future. Other advantages of Hydra is that its provide both Command-Line (CLI) and Graphical User Interface (GUI) for user to interact with. According to Moyle, E. (2022), “It is designed to be parallelized, meaning that multiple thread can operate in parallel to optimize efficiency and speed up the brute-forcing process.

WPSCAN

WPScan an open-source tools that is not specifically developed for password attack. Instead, the main purpose of WPScan is security scanner for WordPress website. It first version was released back in 2019. WPScan is a WordPress black box scanner that allows security professional to execute the malicious files or activities safely. It identifies WordPress

vulnerabilities, outdated software, and weak passwords. Hence, it also features as a password attacker to identify any weak password. WPScan only available in command-line environment to work efficiently. Other features for WPScan are it equipped with various security tools and CI/CD pipelines. To help security professionals and penetration tester, WPScan includes more than 21,000 known security vulnerabilities in its database. WPScan constantly evolving by adding new features and fix any issues to improve its capabilities and performance. Therefore, it become more famous among WordPress community as a tool for them to use for scanning security vulnerabilities.

RESULT AND DISCUSSION

Based on the characteristics of passwords that have been discussed in previous chapter. A set of passwords that consists of 4 common, 4 weak, 4 medium, and 4 strong passwords is created. In result, a total of 16 passwords will be tested to analyze the performance, success rate, and capabilities of each tool.

PERFORMANCE

$$\text{Average} = \frac{\text{Sum of Values}}{\text{Number of Values}}$$

Figure 1: Formulae of Average

To calculate the performance accurately, a mathematical equation of average has been used to compare between the tools. The “Sum of Values” means the total number of times acquired by the tools when cracking the whole set of passwords. While “Number of Values” means the total of passwords that the tools have crack in a set. (Thakur, 2023). Hence, both values will be divided. Therefore, after calculating, a bar graph can be generated to have a better overview.

PCMJ
Progress in Computer and Mathematics Journal (PCMJ)
volume 1 [October, 2024]
e-ISSN: 3030-6728
Website: fskmjebat.uitm.edu.my/pcmj

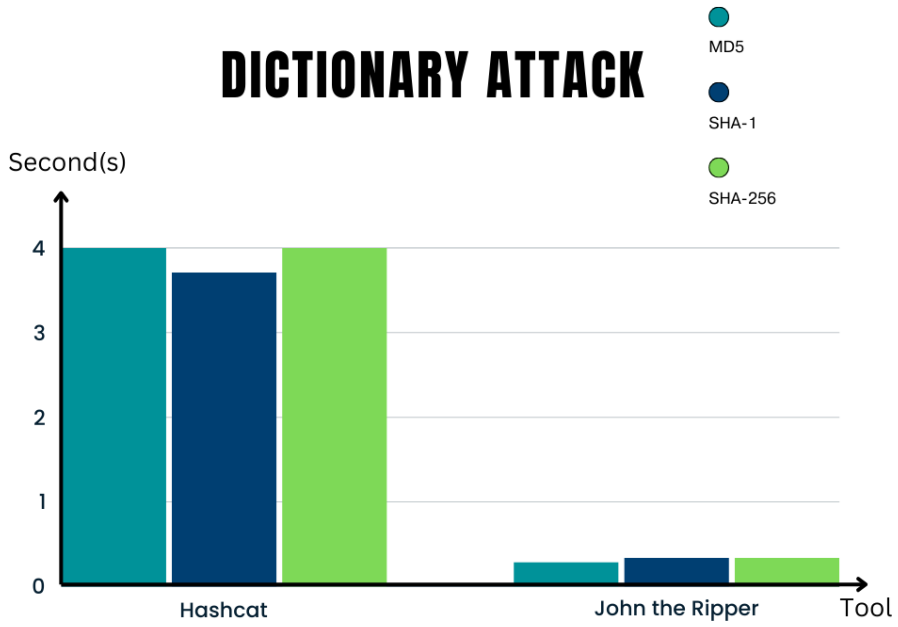

Figure 2: Time average of Dictionary Attack

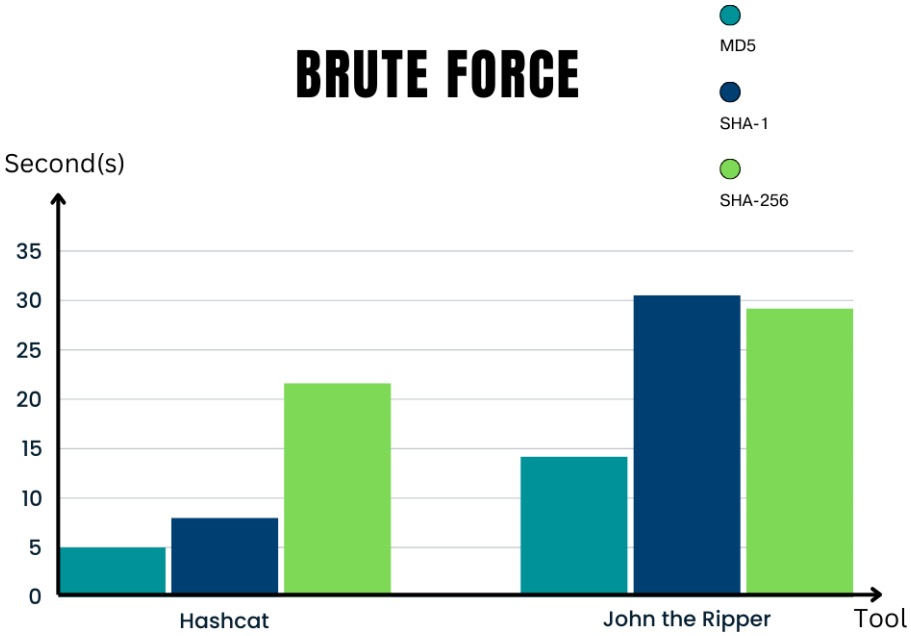

Figure 3: Time average of Brute-Force

PCMJ
Progress in Computer and Mathematics Journal (PCMJ)
volume 1 [October, 2024]
e-ISSN: 3030-6728
Website: fskmjebat.uitm.edu.my/pcmj

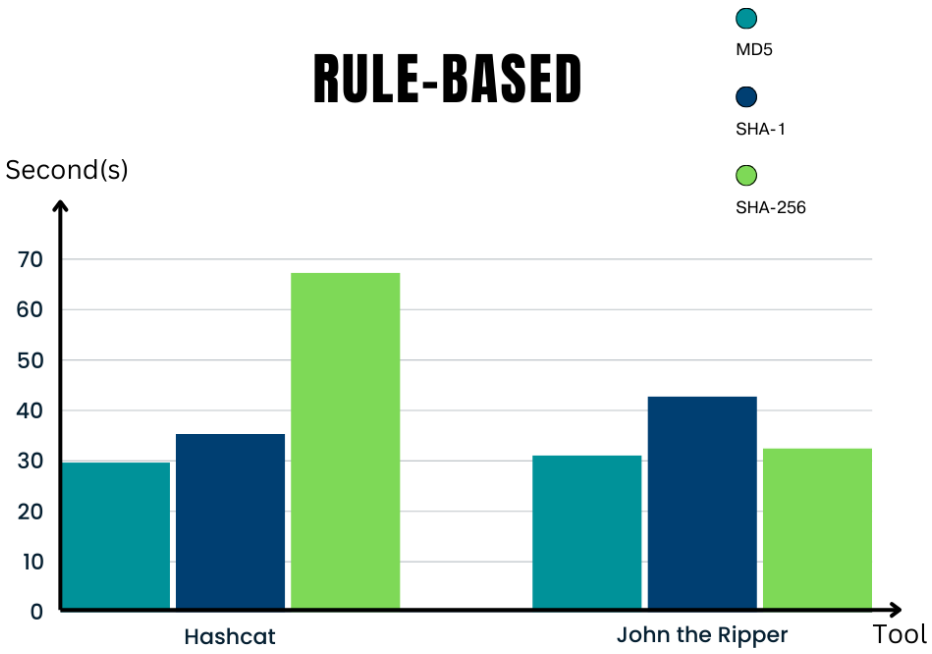

Figure 4: Time average of Rule-based

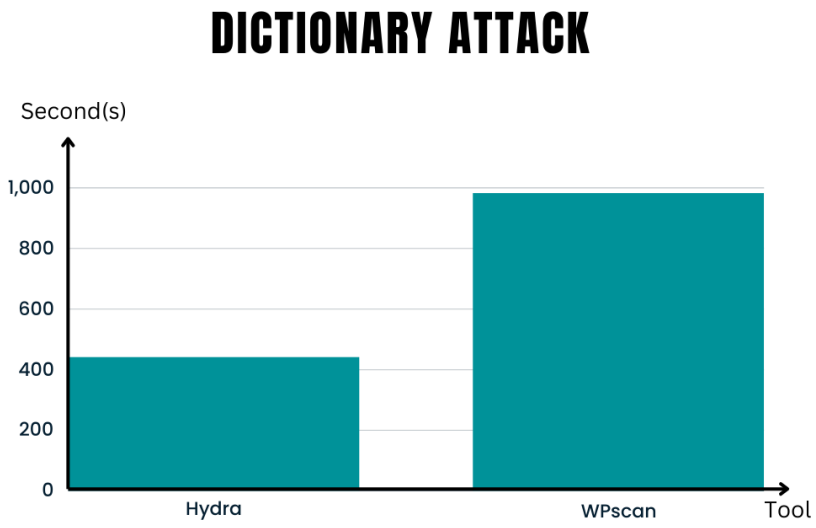

Figure 5: Time average of Dictionary Attack

PCMJ
Progress in Computer and Mathematics Journal (PCMJ)
volume 1 [October, 2024]
e-ISSN: 3030-6728
Website: fskmjebat.uitm.edu.my/pcmj

SUCCESS RATE

Based on figure 6. A mathematical equation of percentage is taken to calculate the success rate of password cracking tools. To calculate it, the "Value" means that the number of successful cracked password by the tools. While "Total of Value" is the total number of passwords in the set. After getting those value, it will be multiplied by 100 to get a percentage. (khoros.com, 2024) Therefore, after calculating, a bar graph can be generated to have a better overview.

$$\text{Percentage} = \frac{\text{Value}}{\text{Total of Value}} \times 100$$

Figure 6: Formulae of Percentage

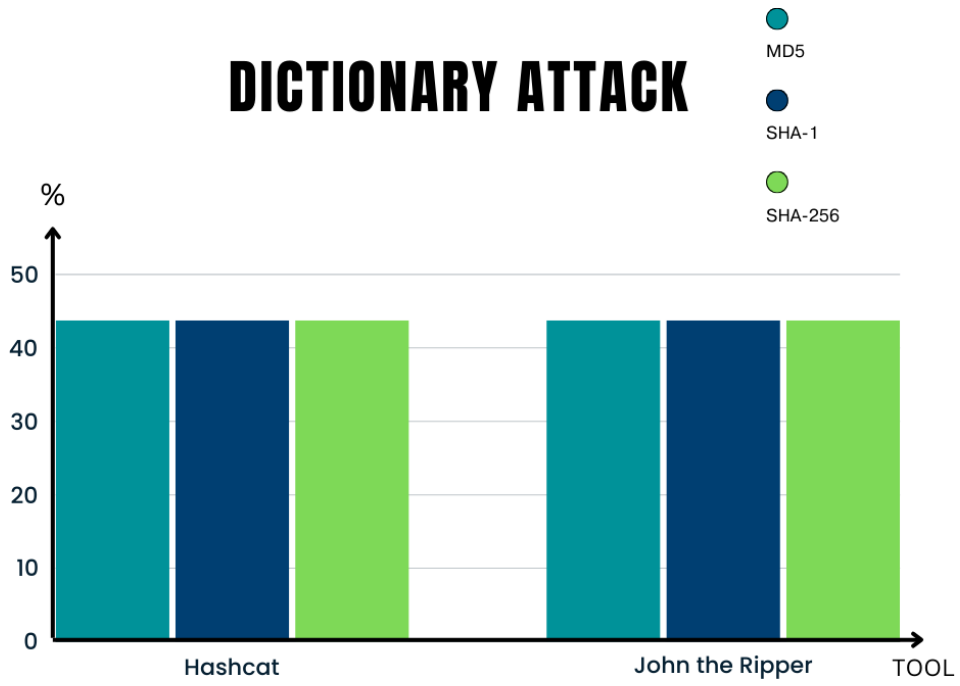

Figure 7: Dictionary Attack Success Rate

PCMJ
Progress in Computer and Mathematics Journal (PCMJ)
volume 1 [October, 2024]
e-ISSN: 3030-6728
Website: fskmjebat.uitm.edu.my/pcmj

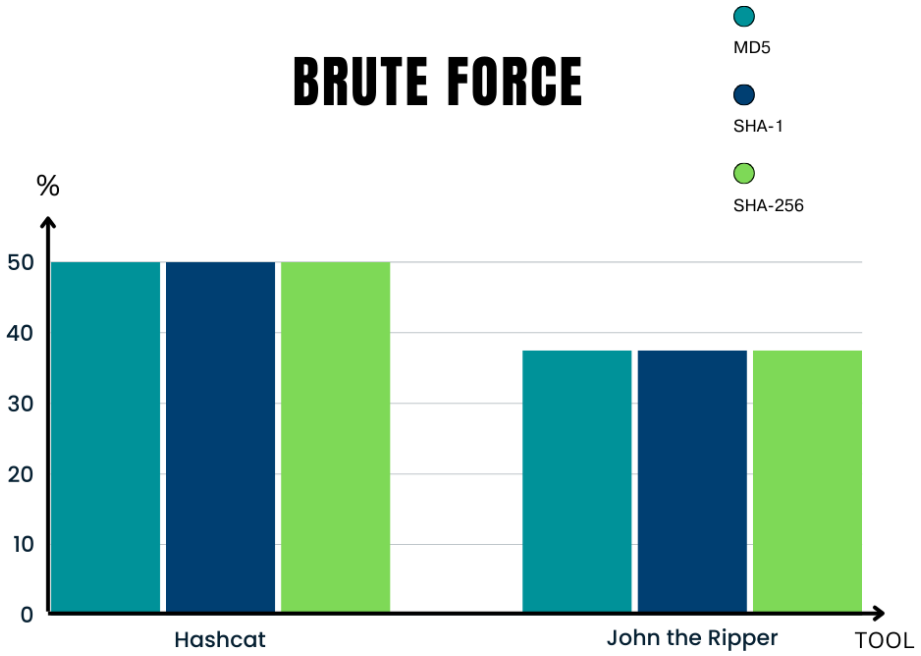

Figure 8: Brute-force Success Rate

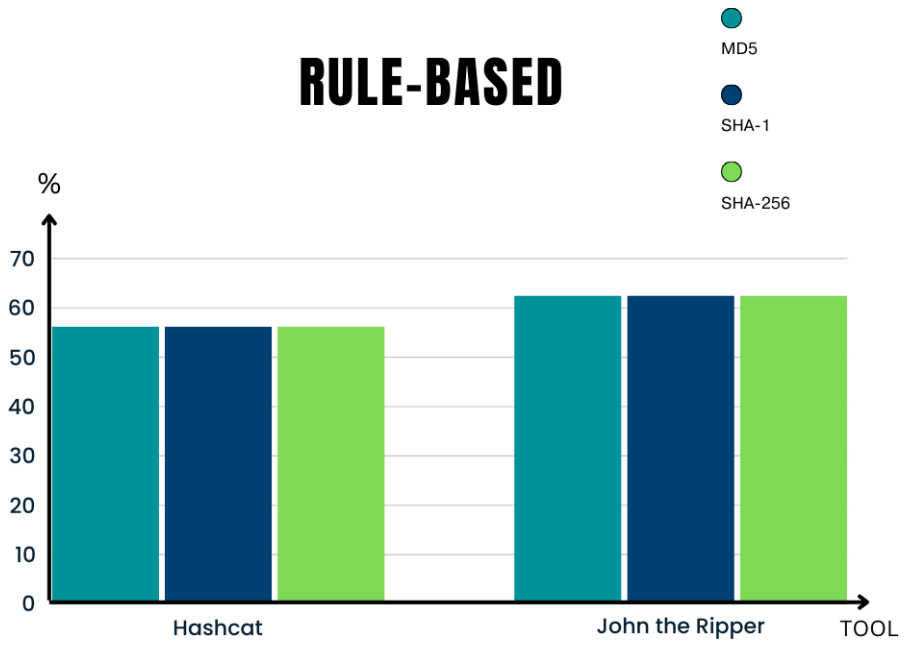

Figure 9: Rule-based Success Rate

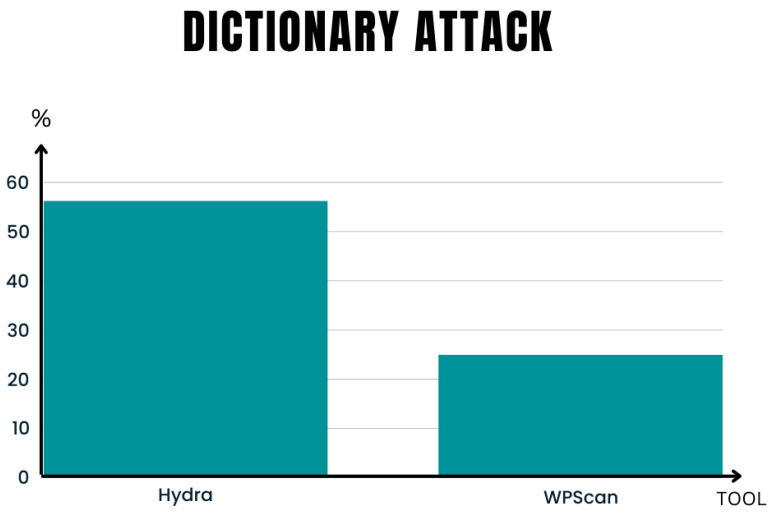

Figure 10: Dictionary Attack Success Rate

REFERENCES (APA 7TH EDITION)

Christian, B., & Peterson, R. (2022) Sarbanes-Oxley Compliance Using COBIT and Open-Source Tools. (pp. 31-57). Syngress.

Yisa, L. V., Baba, M., Olaniyi, T. E. (2016). Review of Top Open Source Password Cracking Tools. International Conference on Information and Communication Technology and Its Application.

He, S., Fu, J., Chen, C., Guo, Z., (2020). Research on Password Cracking Technology Based on Improved Transformer. Journal of Physics: Conference Series.

Chester, A. J. (2015). Analysis of Password Cracking Methods & Applications. University of Akron

Pahuja, D., Sidana, P., (2021). Implementing and Comparing Different Password Cracking Tools. International Research Journal of Engineering and Technology (IRJECT).

Shi, R., Zhou, Y., Li, Y., Han, W., (2021). Understanding Offline Password-Cracking Methods: A Large-Scale Empirical Study

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. Advances in High-Performance Computing Research and Application. https://www.mdpi.com/2076-3417/13/10/5979

Rajah, P., Dastane, O., Bakon, K., Johari, Z. (2020). The Effect of Bad Password Habits on Personal Data Breach. International Journal of Emerging Trends in Engineering Research.

PCMJ

Progress in Computing and Mathematics Journal

UNIVERSITI TEKNOLOGI MARA
Cawangan Melaka

eISSN 3030-6728