INTERNATIONAL JOURNAL OF ACADEMIC RESEARCH IN BUSINESS & SOCIAL SCIENCES

Vol 14, Issue 9, (2024) E-ISSN: 2222-6990

A Comparative Analysis of Offline and Online Password Cracking Tools

Nor Adora Endut
UiTM Melaka Kampus Jasin Malaysia
Email: noradora@uitm.edu.my

Nor Azylia Ahmad Azam
UiTM Shah AlamMalaysia

Ahmad Syahir Amzar Zulkafli
UiTM Melaka Kampus Jasin Malaysia

To Link this Article: http://dx.doi.org/10.6007/IJARBSS/v14-i9/22996 DOI:10.6007/IJARBSS/v14-i9/22996

Published Date: 26 September 2024

Abstract

This study aims to evaluate and compare different password cracking tools that are available in the market like John the Ripper, Hashcat, WPScan, and Hydra to provide insights in their effectiveness in terms of average response time and success rate. The comparative analysis process involves testing and analyzing these tools based on performance, success rate, and different password attacking methods. The study also aims to conduct an empirical comparison of the password cracking tools based on the characteristics of features, ease of use, as well as community support and user guide. The results outline the success rate and performance analysis of both online and offline password attacks based on various password combinations. The study aims to contribute to cybersecurity by identifying the most effective tools and techniques for mitigating password attacks.

Keywords: Password Cracking Tools, Hashcat, John The Ripper, Wpscan, Hydra, Comparative Analysis.

Introduction

Password cracking can be defined as the recovery of plaintext passwords from an encrypted file where it is stored. Passwords have been widely used as the main choice of authentication in various platforms such as computers, networks, smart door locks, as well as various mobile applications such as internet banking. However, the increasing number of password cracking tools has posed a significant threat for users to ensure their passwords are secure. Humans tend to choose passwords that can be easily remembered such as their birthdays due to the convenience and ease to memorize them (Florencio et al, 2019). In addition, humans frequently demonstrate the habit of reusing these easily remembered passwords repeatedly across multiple platforms (Li et al., 2021; Kumar et al., 2022). These practices pose major security compromise as easily guessable and reused passwords are more susceptible to brute-force attacks, unauthorized access, dictionary attacks and phishing attempts (Smith et al., 2019).

Threat actors find these vulnerabilities and compromises by using password cracking tools that are readily available in the market to perform cyber-criminal activities. These tools use algorithms to repeatedly guess the password until the correct one is found. The usage of password cracking tools to gain unauthorized access to computer systems, networks, or data is in violation of various cyber security laws unless it is explicitly authorized by the owner of the system for legitimate purposes such as to recover lost or forgotten passwords, or for penetration testing and forensics investigation. Shi, Zhou, Li, and Han (2021) highlighted that despite the extensive historical use of password cracking tools there has been limited in-depth research focusing on the systematic and detailed analysis of popular password cracking tools in the market.

These tools vary in that they can be used either online or offline. The tools also vary in terms of effectiveness depending on several characteristics such as password complexity, hashing, ease of use and password length. The effectiveness variations are due to several factors such as password complexity, hashing, ease of use as well as password length. For example, John the Ripper or Crackstation is suitable for remote password recovery, while Brutus can help to recover hidden passwords in platforms such as Windows. Thus, organizations or individuals may find it difficult to choose the most suitable tool for their password security assessments. This study also analyzes the password choices to identify the vulnerabilities and password strength.

Password Cracking Tools

A password can be defined as a secret word or phrase that consists of a combination of alphabets, numbers and special characters used to gain access to a specific location, computer system of service. The frequency of password attacks is much higher compared to other authentication methods since it is the most common type of authentication (Papathanasaki, Maglaras & Ayres 2022). Password cracking tools have also evolved with the existence of artificial intelligence (AI). A study done by Home Security Heroes, a cybersecurity firm in 2023 displayed how quickly a password can be cracked through the use of AI in password cracking tools. They concluded that 51% of common passwords can be cracked in less than one minute, 65% in under an hour, 71% in under one day and 81% can be cracked in under one month. They suggest that passwords of 18 characters or longer are considered safe to avoid being cracked.

There are two categories of password cracking tools used in this study namely online and offline tools. The frequency of online attacks is not as much as offline attacks as it requires more skills and sometimes are even unsuccessful since it is layered by many types of security protection. Offline attacks are used when the hacker has the access to the password database and tries to decrypt the password without any direct interaction with a particular website or login page. As such, these attacks will avoid from any alert to trigger the victim.

Offline Password Cracking Tools

Passwords are stored in a database as a form of hash functions instead of plain text. There are several hash functions available such as MD5, SHA-1 and SHA-256. These hashes have different levels of resistance towards password cracking tools. Offline password attacks are not attempting to crack directly towards the server. Rather, the process attempts to obtain a copy of the password hashes using other security breach techniques like brute force, dictionary, rainbow or using a hybrid method. Only after the correct credential will be used to attempt a login at the server. Therefore, it is invisible to the security team and not easy for them to notice that there is an attempt at password cracking (Shi et al., 2021).

Online Password Cracking Tools

Online password cracking attack is a way of guessing the credentials at the login interface. This type of attack requires trying a large number of username and password combinations until the correct credentials are found. Unlike offline password cracking tools, this may trigger an alarm to security teams as the attacker attempts to login to the page many times and the team may block the attacker’s IP address to avoid any successful attempts. Online password cracking speeds are limited by the speed of the network instead of the GPU power. Each of the credential’s guess will be sent over the network to the respective server to be validated. The repeated communication between the user's device and authentication server may take time and largely rely on the speed of the network between the authentication server and the device.

Password Setup

To test the capabilities of the password cracking tools especially in terms of performance and success rate a set of passwords that range from common, weak, medium, and strong password has been setup. To ensure that this test is valid, several literature has been studied to gather the characteristics of weak, medium, and strong passwords. For common passwords, a few passwords will be directly taken from the largest password compilation, namely, rockyou.txt. For strong passwords, Guo et al (2019) state the main characteristics of secure and strong passwords are:

- Consists of 12 characters long or more
- Combine uppercase, lowercase, numbers, and special characters
- Are not built based on common names, persons, pet, movie characters, or brand

Based on the above criteria, 4 strong passwords have been created to be used during the password attack. For weak passwords, the characteristics are:

- Consists of fewer than 8 characters
- The word can be found in dictionary either English dictionary or other languages
- Are built based on names of family members, pets, friends, or movie characters
- Are based on easily gained information such as birthdays, plate number, or home address
- Consists of word or number patterns like aaabbb, qwerty, zyxwvuts, or 123321

4 medium strength passwords were also created for the password attack. A combination of weak and strong passwords was then taken to generate a list of medium passwords having the characteristics as follows:

- Consists of between 8 to 12 characters
- Includes at least one or two combination of lowercase, uppercase, numbers, or special characters
- Does not include easily guessable information
- Are not based on pattern or keyboard sequences such as qwerty, asdfgh, or abc123.

Table 1 summarizes the characteristics of weak, medium and strong passwords.

Table 1
Characteristics of Weak, Medium and Strong Passwords

Features	Weak	Medium	Strong
Length	Less than 8 characters	Ranging from 8 to 12 characters	12 or more characters
Character Types	Only use one type of character	Includes at least 2 types of characters	Includes all types of characters
Susceptibility to Guessing	Consists of information is very susceptible to guessing	Does not consist of information is very susceptible to guessing	Does not use any personal information or dictionary words
Patterns	Use predictable patterns or keyboard sequence	Does not use predictable patterns or keyboard sequence	Completely random and unpredictable

System Architecture

In the testing of offline password cracking tools, only the end devices are involved as it will be working with already obtained database of passwords. These tools crack directly against hashing algorithms. The significant advantage of these tools is that the attacker can leverage on the GPUs power to accelerate the cracking process. Figure 1 shows the system architecture for the offline password cracking tool. The end device, a laptop equipped with CPU and GPU, runs the tools to optimize the GPU power during the cracking process. The tools installed on this laptop are Hashcat and John the Ripper, which both run on Kali Linux. The two tools are used to attack using the hash function MD5, SHA-1 and SHA-256. If the attack is successful, the tools will generate the cracked password in plaintext.

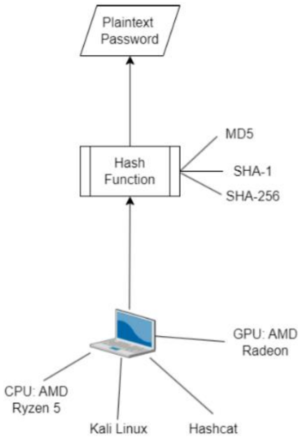

Figure 1. System architecture for offline password cracking tools

Online password cracking tools operate on a network and perform the attack directly at the target login system. Factors of network performance and hardware capabilities play a crucial role in determining the time taken to crack the password. Online password cracking tools might have a lower chance of successful attack due to the risk of being blocked from accessing the system by the administrator should any malicious attempts are detected. Figure 2 shows the system architecture for the online password cracking tool. The end device, a laptop is equipped with CPU and GPU. To capture the packet a packet capturing tool called Burp Suite, which is specialized for capturing HTTP/HTTPS request is used. The online cracking tools, namely Hydra and WPSCan are run on Kali Linux. A WordPress login page is built to simulate a target login page. Then, the login page constantly communicates with the authentication server during the authentication process whenever the tools provide possible credential combinations to the login page until the correct combination is found.

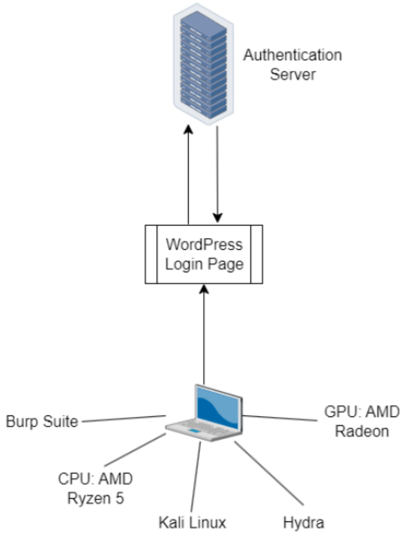

Figure 2. System architecture for online password cracking tools

Results and Discussions

Average Response Time (s)

Offline Password Cracking Tools

To ensure fairness of testing, both offline password cracking tools use the same wordlist which is rockyou.txt. These passwords satisfy the characteristics of weak, medium and strong passwords as highlighted in the previous section. Two offline password cracking tools that were used are Hashcat and John the Ripper. Using the Dictionary attack, the times taken to crack the passwords for MD5, SHA-1 and SHA-256 hashing algorithms were measured and then the average time taken by each tool to crack the passwords is calculated. Figure 3 displays the average response time in seconds taken to crack the password from rockyou.txt using Hashcat and John the Ripper for each of the hashing algorithms using the Dictionary attack.

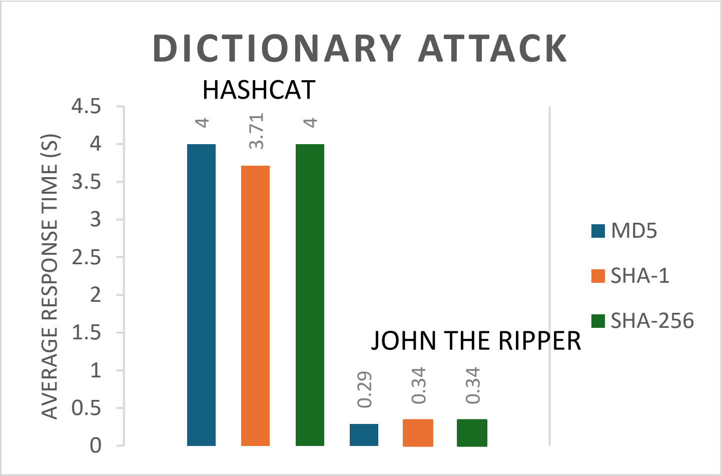

Figure 3. Average response time (s) of offline password cracking tools using the Dictionary attack

There is an obvious margin between the average time taken by John the Ripper and Hashcat in cracking the passwords in the wordlist. John the Ripper can quickly search through the large wordlist of rockyou.txt to find the correct password. John the Ripper takes on average of only 0.29 seconds to find the password in MD5 compared to Hashcat which is 4 seconds on average. While for SHA-1, John the Ripper needed 0.34 seconds rather than 3.71 seconds in Hashcat. Next, SHA-256 recorded the same time as SHA-1 which is 0.34 seconds and 4 seconds in Hashcat. Therefore, John the Ripper faired significantly better than Hashcat in performing the Dictionary attack.

Figure 4 displays the average response time in seconds taken to crack the password from rockyou.txt using Hashcat and John the Ripper for each of the hashing algorithms using the Brute Force attack. When it comes to brute-force attack, Hashcat definitely performs better with much less time taken to crack the set of passwords. For MD5, Hashcat recorded a time of 5 seconds on average rather than 14.2 seconds in John the Ripper. Meanwhile, in SHA-1 Hashcat requires an average of 8 seconds to perform a brute force attack while John the Ripper needed 30.53 seconds on average. Next, Hashcat records a slightly better time in average of 21.63 seconds compared to John the Ripper, 28.2 seconds when cracking SHA-256. Therefore, based on the result and analysis, Hashcat is better in optimizing hardware capabilities especially during attack method that requires high-processing power such as Brute Force.

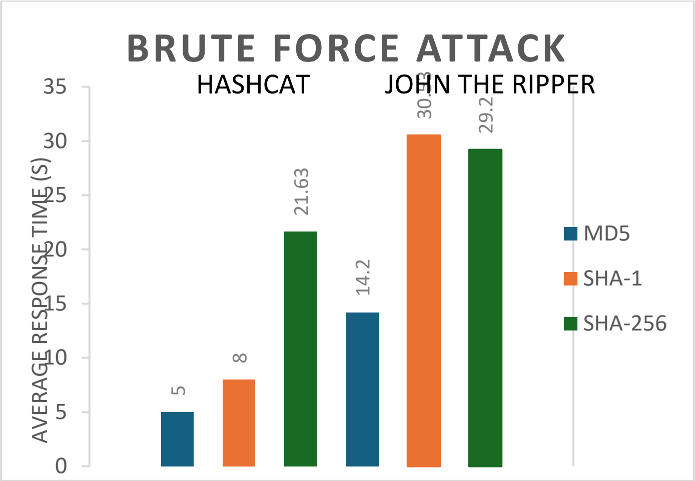

Figure 4. Average response time (s) of offline password cracking tools using the Brute Force attack

Figure 5 displays the average response time in seconds taken to crack the password from rockyou.txt using Hashcat and John the Ripper for each of the hashing algorithms using the Rule-based attack.

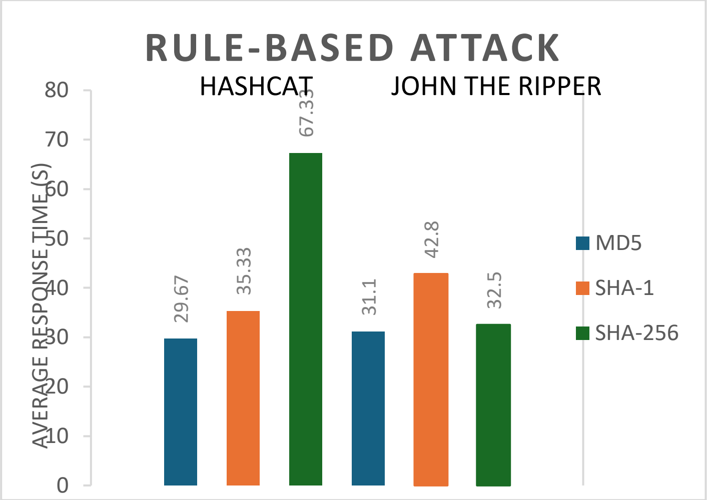

Figure 5. Average response time (s) of offline password cracking tools using the Rule-based attack

For rule-based attack, there is no clear winner in terms of average response time. For MD5, Hashcat shows the ability to crack in better time with recorded 29.67 seconds in average while John the Ripper need 31.1 seconds to crack the set of passwords. Next, Hashcat also shows a better performance in cracking SHA-1 using rule-based attack. Figure 21 shows that it can crack a set of passwords in just 35.33 seconds rather than 42.8 seconds in John the

Ripper. However, SHA-256 works better with John the Ripper with recorded 32.5 seconds and 67.33 seconds in Hashcat.

Online Password Cracking Tools

Figure 6 displays the average response time in seconds taken to crack the password via Dictionary attack using two online password cracking tools namely Hydra and WPScan.

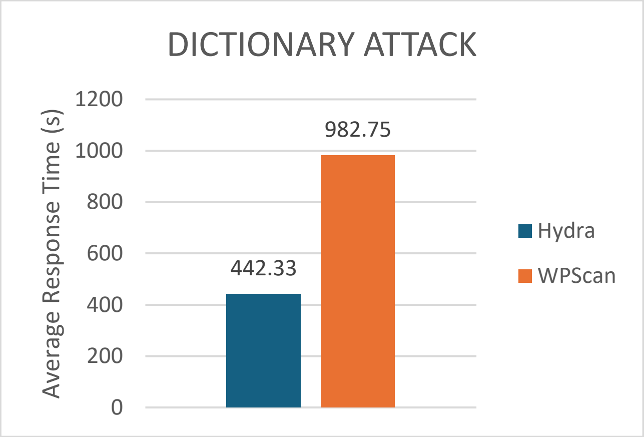

Figure 6. Average response time (s) of online password cracking tools using the Dictionary attack

Both online tools require a handful amount of time to crack even a simple password. This is due to its nature that relies on both hardware and internet connections as they require two-way communication between devices and authentication server. However, WPScan only successful cracked much smaller number of passwords, which will discussed more on success rate. Therefore, Hydra seems to be better in terms of performance as it successfully cracked more passwords.

Success Rate

Success rate evaluation is to understand the effectiveness of password cracking tools when performing a password attack. It involves the ability of these tools to decipher passwords under varying condition such as hash type and password complexities. To calculate the success rate, a mathematical equation of percentage is used on how many passwords can the tool crack when a given a set of passwords. 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 values, it will be multiplied by 100 to get a percentage.

Offline Password Cracking Tools

To calculate the percentage, the number of successful cracked password will be divided with 16 which is the total number of passwords in the set. Figure 7 displays the success rate (%) for each offline cracking tool using Dictionary attack.

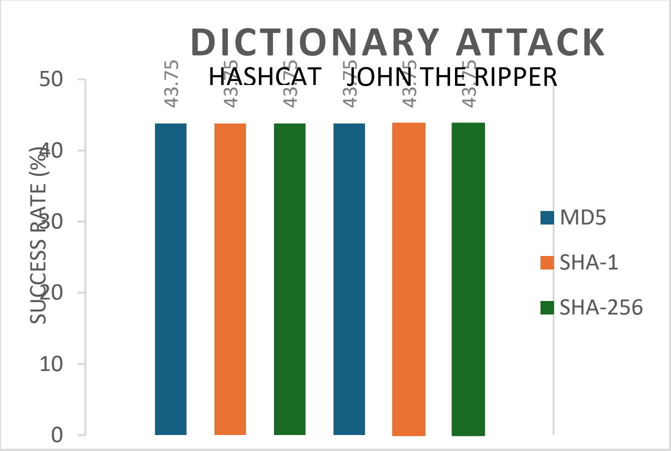

Figure 7. Success rate (%) of offline password cracking tools using the Dictionary attack

The result shows that both of the tools successfully utilize all of the passwords in the wordlist, rockyou.txt. Both Hashcat and John the Ripper record the same success rate, which is 43.75%, equivalent to 7 out of 16 passwords that have been successfully cracked.

Figure 8 displays the success rate (%) for each offline cracking tool using Brute Force attack.

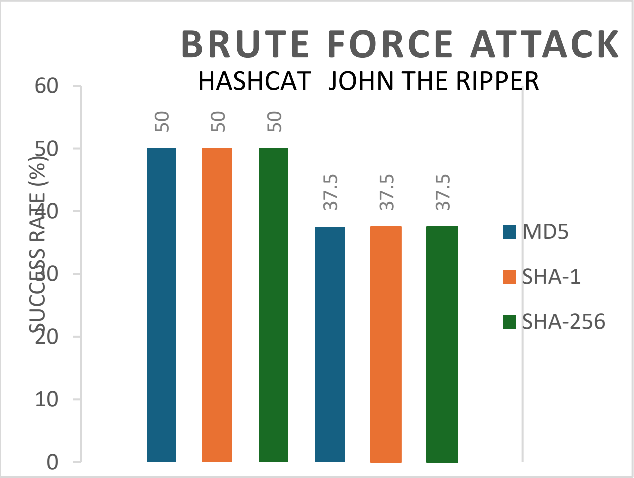

Figure 8. Success rate (%) of offline password cracking tools using the Brute Force attack

For brute-force attack, Hashcat shows a much higher success rate in cracking a set of passwords which recorded 50% of successful attack, equivalent to 8 out of 16 passwords. Compared to John the Ripper, which only achieved 37.5% of successful attacks, equivalent to 6 out of 16 passwords. Correlating the result above with the average response time, Hashcat successfully cracked a medium strength password within a reasonable timeframe. Meanwhile, John the Ripper was only able to crack the weak passwords with the same timeframe. This shows superiority in Hashcat's capability of cracking more complex passwords due to its hardware utilization.

Figure 9 displays the success rate (%) for each offline cracking tool using Rule-based attack.

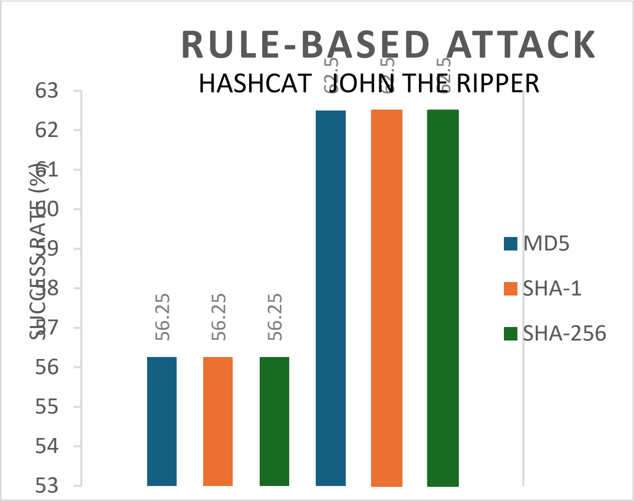

Figure 9. Success rate (%) of offline password cracking tools using the Rule-based attack

In the rule-based attack it is shown that John the Ripper is capable of utilizing the given wordlist and set of rules. This observation is proven by the fact that John the Ripper recorded 62.50% of successful attacks which is equivalent to 9 out of 16 passwords successfully cracked. Meanwhile, Hashcat only achieved 56.25% of successful attacks which is 8 out of 16 passwords.

Online Password Cracking Tools

Figure 10 displays the success rate (%) of password cracking attempts via Dictionary attack using Hydra and WPScan. In terms of success rate of online password tools, Hydra shows a significant advantage over WPScan with recorded rate of 56.25% which is equivalent to 9 out of 16 password successful cracked password. On the other hand, WPScan recorded a success rate of only 25%, 4 out of 16 successful cracked passwords. With these numbers, Hydra shows to be better in utilizing the wordlists given.

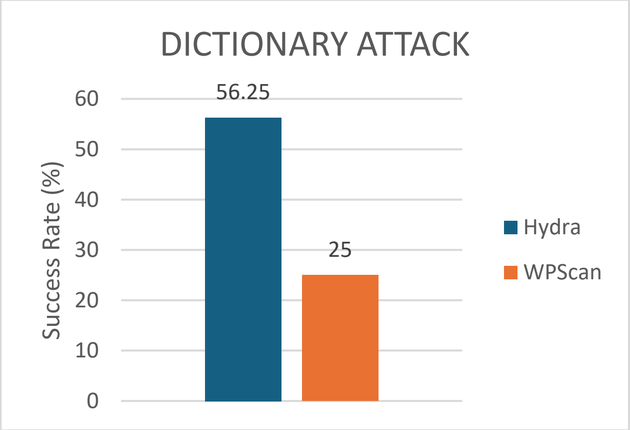

Figure 10. Success rate (%) of online password cracking tools using the Dictionary attack
Features

Offline Password Cracking Tools

When examining the feature sets of the two tools, the analysis discovers several key differences. John the Ripper supports GPU acceleration for certain hash types but has limited parallelism features. Hashcat, on the other hand, is capable of leveraging both CPU and GPU resources, and has advanced parallelism capabilities. Both tools, however, support a diverse range of hashing algorithms.

The ease of use also varies between the two tools. John the Ripper is generally considered more beginner-friendly, with a simpler command syntax. Hashcat, while offering more advanced features, may present a steeper learning curve for novice users when performing complex attacks.

Finally, this study takes a look into the community support and user guides available for each tool. John the Ripper benefits from a larger and more active community, but its help mode provides less detailed information. On the other hand, Hashcat has a smaller but responsive community, and its help mode offers more comprehensive guidance on the tool's features and usage.

Online Password Cracking Tools

In terms of features, Hydra provides a wider range of tools and supports more protocols, as well as a graphical user interface (GUI) that is called THC-Hydra. While WPScan is built specifically for testing security vulnerabilities on WordPress, Hydra offers more capabilities beyond just password cracking.

It is important to note that Hydra has a more complex command-line interface, requiring users to specify many details for a successful attack. In contrast, WPScan's command-line interface is much easier, as users can simply insert the URL. Regarding community support and user guides, this study finds that Hydra has less robust community support beyond GitHub, and fewer comprehensive documentation resources compared to WPScan, which has a better-established forum and more detailed user guides.

Conclusion

This study aims to evaluate and compare different password cracking tools that are available in the market like John the Ripper, Hashcat, WPScan, and Hydra to provide insights in their effectiveness in terms of average response time (s) and success rate (%). It also aims to conduct an empirical comparison of the password cracking tools based on the characteristics of features, ease of use, as well as community support and user guide. Based on the research objectives, we can highlight the findings in Table 2.

Table 2
Comparative analysis of offline and online password cracking tools

Comparative Parameters	Offline Password Cracking Tools	Online Password Cracking Tools
Average response time	Offline password cracking tools operate significantly faster as they rely solely on hardware capabilities, bypassing the	Online password cracking is much slower due to the additional factor of network latency, as each password and username combination must

	delays caused by network latency.	be sent over the network to the authentication server.
Success rate	Offline tools have a much higher success rate since they operate in an isolated environment where network administrators cannot detect the cracking process. Additionally, they do not require an internet connection, thus avoiding the risk of network interruptions.	Online tools have a lower success rate because once the system detects multiple failed login attempts, it may lock the target account and block the attacker's IP address. Furthermore, online tools require a continuous and stable internet connection to maintain the attack.
Features	Offline password cracking tools offer a wider array of features and attacking methods, such as dictionary attacks, brute-force attacks, rule-based attacks, and the use of rainbow tables. These tools support many hashing algorithms and can crack passwords obtained from password sniffing or leaked databases.	Despite supporting numerous protocols, online tools offer limited attacking methods. Tools like Hydra and WPScan primarily support brute force through wordlists and do not require obtaining hash values beforehand.
Ease of Use	Offline password cracking tools are generally easier to use, requiring only the hash value to initiate the attack. This simplicity results in less complex commands for performing the attack	Online password cracking tools are more complex to use, requiring the specification of host IP addresses, port numbers, and protocols. Users often need a packet sniffer to gather this information, adding to the complexity.
Community support and user guide	Offline password cracking tools benefit from a more active community, providing extensive resources such as research papers, journals, video tutorials, and articles to assist beginners.	Online tools like Hydra lack active community forums and have fewer educational resources, making them less accessible for new users.

In summary, the choice between online and offline password cracking tools may depend on the user’s need. However, the advantages offered by offline password cracking tools provide much more flexibility and ability to the users when performing the attack. This might include stealthiness, hardware utilization, cracking speed, and success rate. Therefore, security professionals should put a lot of concerns and attentions on the evolving threats of offline password cracking tools as it cannot be detected by the system.

Acknowledgement

The authors would like to acknowledge and express gratitude towards the technical knowhow and moral support provided by the College of Computing, Informatics and Mathematics in completing this research.

References

Florencio, D., Herley, C., & Van Oorschot, P. C. (2020). Passwords in the wild: Real-world patterns and how people use them. ACM Transactions on Computer-Human Interaction (TOCHI), 27(1), 1-39.

Guo, Y., Zhang, Z., & Guo, Y. (2019). Optiwords: A new password policy for creating memorable and strong passwords. Computers & Security, 85, 423-435.

Li, N., Wang, X., & Li, Y. (2021). Exploring the phenomenon of password reuse across online platforms. Journal of Cybersecurity, 7(1), 1-18.

Kumar, R., Kapoor, A., & Verma, R. (2022). Password reuse: A comprehensive study of user behavior across platforms. International Journal of Information Management, 62, 102071.

Papathanasaki, M., Maglaras, L., & Ayres, N. (2022). Modern Authentication Methods: A comprehensive survey. AI, Computer Science and Robotics Technology, 2022, 1–24. https://doi.org/10.5772/acrt.08

Shi, R., Zhou, Y., Li, Y., & Han, W. (2021). Understanding Offline Password-Cracking Methods: A Large-Scale Empirical Study. Security and Communication Networks, 2021, 1–16. https://doi.org/10.1155/2021/5563884

Smith, A. N., Zhang, D., & Smith, J. M. (2019). Exploring password vulnerability to dictionary attacks and phishing. Cybersecurity, 2(1), 1-14.