Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Volume 13, Issue 03 March 2024

# Non-Hashed Password Cracking Tool

Lakshmi Prasanna Pokuri
Department of CyberSecurity
CMR College of Engineering
& Technology
Hyderabad, India

Varshitha Nukala
Department of CyberSecurity
CMR College of Engineering
&Technology
Hyderabad, India

Vemuri Saicharan
Department of CyberSecurity
CMR College of Engineering
& Technology
Hyderabad, India

M. Uma Maheshwara Rao
Dept of CyberSecurity (Assistant.prof)
CMR College of
Engineering& Technology
Hyderabad, India

Reddyvari Venkateshwara Reddy
Dept of CyberSecurity (Associate.prof)
CMR College of
Engineering& Technology
Hyderabad, India

***Abstract*—In the area of digital security, authentication processes serve as a wall between valuable resources and outsiders, where passwords are at the core of user authentication.However,passwords vulnerability to hacking shows that there is need to both guarantee safety and facilitate recovery in case one forgets.That is how password cracking comes into play- a two-faced weapon that can ruin a defense but also help recover passwords. This article introduces an innovativeinitiative; developing a user friendly Graphical User Interface (GUI) for Non-Hashed Password Cracking Tool. This GUI application aims at democratizing the process of password cracking for different kinds of files such as ZIP, RAR, PDFfiles etc through seamless integration of dictionary based and brute-force techniques. Developed using Python's Tkinter library, this tool ensures the focus is on users by providing an intuitive interface,resilient error handling and live progress tracking as users go through the password recovery process.It aims at filling the gap between security and accessibility by enabling users to efficiently retrieve passwords for protected files thus affording them easy access to crucial data in a manner that is cost-effective and client-centric. A password cracker recovers passwords by various methods. This can entail comparing a list of terms to build up the password or keepingon guessing it using certain algorithms. This application aims at improving its user experience by providing an attractive visual interface, efficient error handling and tracking progress during the recovery process of the password.**

**The tool has been developed using Tkinter library for Python, which makes it easier for users to recover passwords from protected files in an effective and user-friendly manner thus allowing access to vital data.**

***Index Terms*—Password Cracking, Brute-Force Attack, Dictio-nary Attack, Graphical Interface(GUI)**

## I. INTRODUCTION

"Non-hashed password cracker" means a software solution to decrypt (or crack) passwords which are saved or transmitted without applying hashing algorithms. Hashing is aimed at protecting passwords by converting them into scrambled form that are nearly impossible to be recognized by computer processors. Nonetheless, some systems or apps may prefer storing or transmitting their passwords in plain text or reversible encryption making them vulnerable to interception or theft.

These password crackers, generally work by employing techniques like dictionary attacks where commonly used passwords or phrases are tested systematically or brute-force attacks which involve testing all possible combinations of characters until the right password is found.

It is important to note that trying to crack somebody's password without authority is illegal and unethical. One should only attempt to crack passwords after obtaining explicit permission from system administrators or owners for lawful security evaluation purposes.

This paper will examine the field of cybersecurity focusing on password cracking. It presents different attack methods as well as numerous tools that can be utilized in their execution. The rapid advancement of technology has brought forth a lot of free online available password cracking tools.[1]

This paper talks about different types of attacks on passwords and tools and gives general information on do'sand dont's

## I. PASSWORD CRACKING TECHNIQUES

Password cracking, also known as password hacking, is a major cyber threat where unauthorized people acquire other people's passwords. There are five main techniques that fall under this malevolent practice: Brute Force Attack; Dictionary Attack; Hybrid Attack; Rainbow Tables Attack and SocialEngineering attack.

### A. Brute Force Attack

This method is based on trial and error to extract penetration certificates or encryption keys. By systematic cycling hackers will try to gain advantage through all possible combinations accessing secure accounts or opening hidden web pages. Despite the past, violent attacks are still dangerous Becauseof their potential for effectiveness, albeit to varying degrees Deadlines based on strong passwords.

This is an old method of attack, but still effective and hackers love it a lot. Because it depended on the length As complicated as the password is, cracking it can get you all over the place from a few seconds to years.[2]

The big advantages of brute force attacks are that relatively simple to make and, given enough time as well with no wayto slow down the target, they work constantly. System-based system and any encryption key available can be give a crashby using a brute force attack. Of course, the amount of timeit takes brute force into a system to be a useful for metrics gauging that system's level of security.In other words.Brute Force attacks are very slow, because they have to run before by any possible combination of characters achieving their goals.[3]

### B. Dictionary Attack

In a dictionary attack, attackers use a pre compiled dictionary that includes common words, phrases, and character sets. This method is absolutely brilliant a form of brute force attack, where tools rapidly cycle through dictionary entries in an attempt to crack passwords. targeting passwords that can be used by individually, dictionary attacks aim to obtain sensitive, unauthorized information better than traditional methods of brutality.[4]

In its simplest form, a dictionary attack is a type of brutal attack where hackers make a quick list and try to guess the password of the user of their online account common combinations of words, phrases, and numbers. If a password is successfully cracked by a dictionary attack, a hacker canuse this to gain access to resources such as bank accounts, social media profiles and even encrypted ones Files types.This is when it can be a real problem the attacker.[5]

### C. Hybrid Attack

Hybrid attacks are like a blend of different strategies, aimedat making password cracking more efficient and successful. Essentially, hackers combine the strengths of various methods, such as dictionary attacks and brute force techniques, to exploit both known patterns and all possible combinations of characters in passwords. This approach increases the chances of breaking through security defenses.

To give you a clearer picture, imagine a typical hybridattack as a mix of a dictionary attack and a brute-force attack. In the dictionary attack part, hackers use a list of commonly used passwords or phrases (known as a wordlist)to try and match with the target password. Meanwhile, in the brute-force attack part, they systematically try every possible combination of characters to find the correct password. This combination of approaches allows hackers to cover a wider range of possibilities and increase their chances of success.[6]

### D. Rainbow Tables Attack

The rainbow tables attack method focuses on cracking password hashes stored in databases. When applications store passwords, they don't usually store them in plain text. Instead, they use cryptographic hash functions to encrypt passwords, turning them into a series of characters known as a hash.

Rainbow tables are essentially pre-computed tables that contain password hash values for each possible plaintext character combination. These tables allow hackers to quickly crack hashed passwords by comparing the pre-computed hash values with the hashes stored in the database. This comparison enables attackers to bypass security measures and gain unauthorized access to protected systems.

If hackers manage to obtain the list of password hashes,they can use rainbow tables to crack all the passwords very rapidly. This method significantly speeds up the process of cracking passwords compared to traditional brute-force or dictionary attacks.[7]

### E. Social Engineering Attack

Social engineering is a deceptive tactic used by malicious individuals to manipulate someone into taking certain actions by exploiting their emotions and decision-making process.

According to Digital Guardian, social engineering attacks often involve psychological manipulation, where unsuspectingusers or employees are tricked into divulging confidential or sensitive information. These attacks commonly occur through email or other forms of communication that evoke feelings of urgency, fear, or similar emotions in the victim.As a result, the victim may unwittingly disclose sensitive information, click on malicious links, or open harmful files,all of which can lead to security breaches or other harmful consequences.[8]

## II. Password Cracking Tools

In a well-designed password-based authentication system, the actual passwords of users are not stored directly. Instead, the system stores hashed versions of passwords, making it significantly harder for hackers or malicious insiders to gain access to user accounts. Hashing involves converting pass- words into a scrambled format using cryptographic algorithms,adding an extra layer of security.

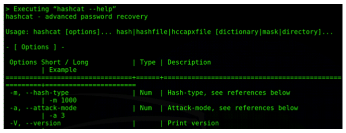
Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Volume 13, Issue 03 March 2024

Kali Linux is a widely respected security tool known for its versatility in tasks like penetration testing and network security. It offers various bootable options, such as virtual images and software installations, and is even compatible with devices like Raspberry Pis. IT security teams aroundthe world trust Kali Linux to assess their networks for vulnerabilities and defend against potential threats.[9]

Hackers commonly use password-cracking tools like Hashcat, John the Ripper, THC-Hydra, and OphCrack to carry out different types of attacks. These tools are capableof cracking passwords stored in various formats, including hashed passwords and encrypted files. Essentially, these tools provide hackers with the means to attempt different attack methods, such as brute force or dictionary attacks, to crack passwords and gain unauthorized access to systems or data.[10]

### A. *Hashcat*



```
> Executing "hashcat --help"
hashcat - advanced password recovery

Usage: hashcat [options]... hash|hashfile|hccapxfile [dictionary|mask|directory]...

- [ Options ] -

 Options Short / Long           | Type | Description
        | Example
================================+======+================================================
=========+======================
 -m, --hash-type                | Num  | Hash-type, see references below
        | -m 1000
 -a, --attack-mode              | Num  | Attack-mode, see references below
        | -a 3
 -V, --version                  |      | Print version
```

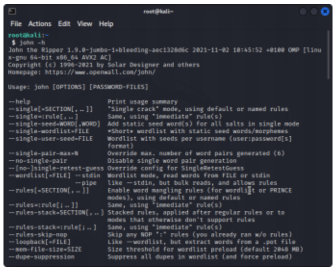
Fig. 1. Hashcat Tool

Hashcat is a well-known password-cracking tool valuedfor its flexibility and ability to handle over 300 different types of hashes. One of its key strengths is its high level of parallelization, which means it can crack multiple passwords across multiple devices at the same time.[9]

Typically, Hashcat comes already installed with Kali Linux, a popular operating system used for cybersecurity tasks. However, if you need to install Hashcat separately, you can do so by entering the provided command in the terminal.

installation : sudo apt-get install hashcat

### B. *John the Ripper*



```
root@kali:~
 $ john -h
John the Ripper 1.9.0-jumbo-1+bleeding-aec1328d6c 2021-11-02 10:45:52 +0100 OMP [linu
x-gnu 64-bit x86_64 AVX2 AC]
Copyright (c) 1996-2021 by Solar Designer and others
Homepage: https://www.openwall.com/john/

Usage: john [OPTIONS] [PASSWORD-FILES]

--help                    Print usage summary
--single[=SECTION[,..]]   "Single crack" mode, using default or named rules
--single=:rule[,..]       Same, using "immediate" rule(s)
--single-seed=WORD[,WORD] Add static seed word(s) for all salts in single mode
--single-wordlist=FILE    *Short* wordlist with static seed words/morphemes
--single-user-seed=FILE   Wordlist with seeds per username (user:password[s]
                          format)
--single-pair-max=N       Override max. number of word pairs generated (6)
--no-single-pair          Disable single word pair generation
--[no-]single-retest-guess Override config for SingleRetestGuess
--wordlist[=FILE] --stdin Wordlist mode, read words from FILE or stdin
                  --pipe  like --stdin, but bulk reads, and allows rules
--rules[=SECTION[,..]]    Enable word mangling rules (for wordlist or PRINCE
                          modes), using default or named rules
--rules=:rule[;..]]       Same, using "immediate" rule(s)
--rules-stack=SECTION[,..] Stacked rules, applied after regular rules or to
                          modes that otherwise don't support rules
--rules-stack=:rule[;..]  Same, using "immediate" rule(s)
--rules-skip-nop          Skip any NOP ":" rules (you already ran w/o rules)
--loopback[=FILE]         Like --wordlist, but extract words from a .pot file
--mem-file-size=SIZE      Size threshold for wordlist preload (default 2048 MB)
--dupe-suppression        Suppress all dupes in wordlist (and force preload)
```

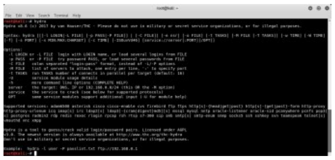
Fig. 2. John the Ripper

John the Ripper is another popular password-cracking tool that is widely used across different operating systems such as Linux, Unix, Mac OS X, and Windows. It's known for its versatility in cracking passwords for various platforms and file types, including web applications, compressed archives, and document files.

Additionally, there is a professional version of John the Ripper available, which provides enhanced features and native packages tailored for specific operating systems. Moreover, users have the option to download Openwall GNU/*/Linux, which includes John the Ripper as part of its software package.[9]

installation : sudo apt-get install john

### C. *THC-Hydra*



```
root@kali:~# hydra
Hydra v8.6 (c) 2017 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Syntax: hydra [[[-l LOGIN|-L FILE] [-p PASS|-P FILE]] | [-C FILE]] [-e nsr] [-o FILE] [-t TASKS] [-M FILE [-T TASKS]] [-w TIME] [-W TIME]
[-f] [-s PORT] [-x MIN:MAX:CHARSET] [-c TIME] [-ISOuvVd46] [service://server[:PORT][/OPT]]

Options:
  -l LOGIN or -L FILE  login with LOGIN name, or load several logins from FILE
  -p PASS  or -P FILE  try password PASS, or load several passwords from FILE
  -C FILE   colon separated "login:pass" format, instead of -L/-P options
  -M FILE   list of servers to attack, one entry per line, ':' to specify port
  -t TASKS  run TASKS number of connects in parallel per target (default: 16)
  -U        service module usage details
  -h        more command line options (COMPLETE HELP)
  server    the target: DNS, IP or 192.168.0.0/24 (this OR the -M option)
  service   the service to crack (see below for supported protocols)
  OPT       some service modules support additional input (-U for module help)

Supported services: adam6500 asterisk cisco cisco-enable cvs firebird ftp ftps http[s]-{head|get|post} http[s]-{get|post}-form http-proxy
http-proxy-urlenum icq imap[s] irc ldap2[s] ldap3[-{cram|digest}md5][s] mssql mysql nntp oracle-listener oracle-sid pcanywhere pcnfs pop3[
s] postgres radmin2 rdp redis rexec rlogin rpcap rsh rtsp s7-300 sip smb smtp[s] smtp-enum snmp socks5 ssh sshkey svn teamspeak telnet[s]
vmauthd vnc xmpp

Hydra is a tool to guess/crack valid login/password pairs. Licensed under AGPL
v3.0. The newest version is always available at http://www.thc.org/thc-hydra
Don't use in military or secret service organizations, or for illegal purposes.

Example:  hydra -l user -P passlist.txt ftp://192.168.0.1
root@kali:~#
```

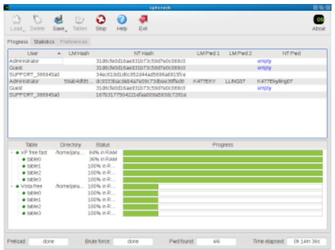
Fig. 3. THC-Hydra

THC-Hydra is a powerful online password-cracking tool designed to conduct brute-force attacks aimed at guessinguser credentials. It boasts support for a wide array of network protocols, making it highly versatile for various applications. Additionally, Hydra is easily extensible, allowing users to install new modules with ease.

Hydra supports numerous network protocols, including but not limited to Asterisk, AFP, Cisco AAA, FTP, HTTP, HTTPS, IMAP, LDAP, MySQL, Oracle, POP3, RDP, SMB, SSH, Telnet, and many more. This extensive protocol support enables Hydra to target a diverse range of systems and services, making it a valuable tool for security testing and penetration testing purposes.[9]

installation : sudo apt-get install hydra-gtk

### D. *OphCrack*



| User | LM Hash | NT Hash | LM Pwd 1 | LM Pwd 2 | NT Pwd |
|---|---|---|---|---|---|
| Administrator | | 31d6cfe0d16ae931b73c59d7e0c089c0 | | | empty |
| Guest | | 31d6cfe0d16ae931b73c59d7e0c089c0 | | | empty |
| SUPPORT_388945a0 | | 34ec619d1d6c952d44ad5896a6815fca | | | |
| Administrator | 59ab4dfd5... | dc9333bacde84a7e09c73dbee36ffed8 | K477EKY | LLING07 | K477Ekylling07 |
| Guest | | 31d6cfe0d16ae931b73c59d7e0c089c0 | | | empty |
| SUPPORT_388945a0 | | 167b3177504221dfaa009a5938c7281e | | | |

| Table | Directory | Status | Progress |
|---|---|---|---|
| XP free fast | /home/janu... | 64% in RAM | |
| table0 | | 36% in RAM | |
| table1 | | 100% in R... | |
| table2 | | 100% in R... | |
| table3 | | 100% in R... | |
| Vista free | /home/janu... | 100% in R... | |
| table0 | | 100% in R... | |
| table1 | | 100% in R... | |
| table2 | | 100% in R... | |
| table3 | | 100% in R... | |

Preload: done  Brute force: done  Pwd found: 4/6  Time elapsed: 0h 14m 36s

Fig. 4. OphCrack

OphCrack is a password-cracking tool that relies on rainbow tables, which are precomputed tables containing password hash values. It's mainly utilized for Windows systems but can also be used with Linux and Mac. OphCrack specializes in cracking LM and NTLM hashes, making it particularly effective for gaining access to Windows-based systems.

One convenient aspect of OphCrack is that it's available as a live CD, allowing for easy use without the need for installation.Additionally, it can be downloaded for free, making it accessible to anyone looking to test the security of Windows systems or recover lost passwords.[9]

## III. Password Cracking Tool Working

Password cracking can be a time-consuming process, often taking several days, particularly if the passwords are longand include many special characters. However, the use of specialized programs significantly simplifies this task.[11]

Hacking into an account can be achieved through various methods, and password cracking is among the most common techniques. This method involves employing computational and other approaches to bypass the password authentication step. Nowadays, there are even specialized tools specifically designed for password cracking.[12]

This can entail comparing a list of terms to build up the password or keeping on guessing it using certain algorithms. This application aims at improving its user experience by providing an attractive visual interface, efficient error handling and tracking progress during the recovery process of the password.

The Python code that has been developed creates a user-friendly graphical interface (GUI) application for cracking passwords of different file types. These include ZIP and RAR archives, web-based applications, and PDF files. Let's break down the working process of the code:

- The code begins by importing necessary libraries such as tkinter for GUI, pathlib for working with file paths, zipfile for ZIP file operations, pdfplumber for PDF operations, and others.

- The MainApplication class defines the main GUI application. It sets up the window with a title and dimensions. It also creates a canvas and loads an image onto it. Various labels, buttons, and entry widgets are created for user interaction.

- The start cracker method is triggered when the user clicks the ”Start” button. It determines the selected option from the combobox and calls the corresponding method to initiate the cracking process.

- The start zip cracker Method sets up a GUI for ZIP file password cracking. It allows the user to select a ZIPfile and a word list, then attempts to crack the password using the selected word list.

- The start zip bruteforce cracker Method is Similar tothe previous method, this one sets up a GUI for ZIPfile brute-force password cracking. It allows the user to specify parameters such as character set, minimum and maximum password lengths, and attempts to crack the password using brute-force.

- The start rar cracker Method will Sets up a GUI forRAR file password cracking. It allows the user to selecta RAR file and a dictionary file, then attempts to crack the password using the provided dictionary.

- The start rar bruteforce cracker Method will also Sets up a GUI for RAR file brute-force password cracking. Similar to the ZIP brute-force cracker, it allows the user to specify parameters and attempts to crack the password using brute-force.

- The start pdf bruteforce cracker Method will Sets upa GUI for PDF file brute-force password cracking. Itallows the user to specify parameters and attempts to crack the password using brute-force.

- The start pdf dictionary cracker Method will also Sets up a GUI for PDF file dictionary-based password cracking. It allows the user to select a PDF file and a dictionary file, then attempts to crack the password using the provided dictionary.

- BruteForcePDFCrackerApp and DictionaryPDFCrackerApp Classes define GUI applications specifically for PDF password cracking using brute-force and dictionary attacks, respectively. They allow users to input necessary parameters and attempt to crack the password.

- main Function class initializes the Tkinter application by creating a Tk instance and the MainApplication object, then starts the main event loop.

The Tk instance and the MainApplication object enableusers to interact with the graphical user interface (GUI) and start the password cracking processes. Throughout this process, robust error handling ensures that any exceptions are managed gracefully, while progress feedback within the GUI keeps users updated on the cracking status, including the number of attempts made and the estimated time remaining.

Security measures are also in place to ensure responsible use, such as confirming legal authorization for password cracking activities. Additionally, clear documentation is provided, offering instructions and licensing information to enhance usability and compliance.
brute-force attacks exhaustively try every possible password

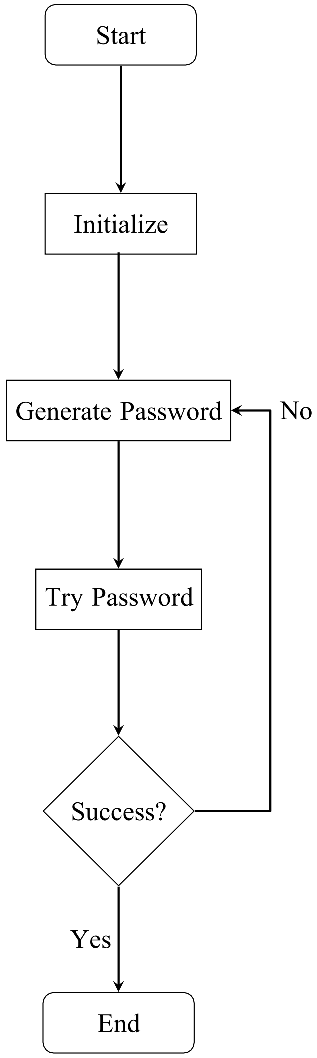
combination, while dictionary attacks leverage predefined lists of words or phrases.

Therefore these both attacks have their strengths and weaknesses, and the effectiveness depends on factors such as password complexity, length, and the sophistication of the attacker's tools and resources.

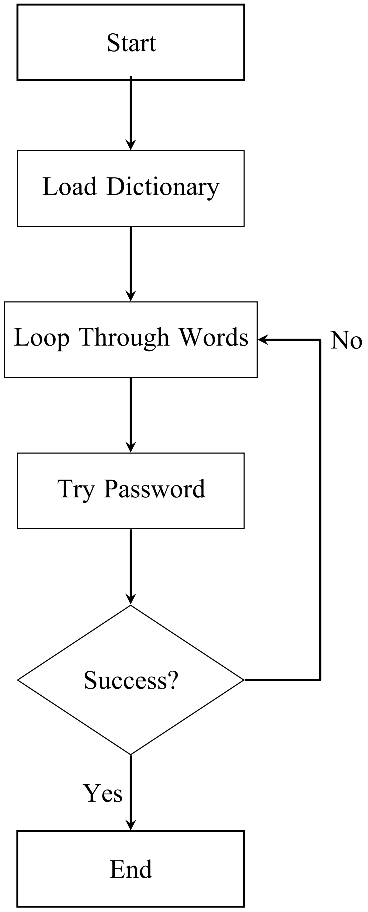
Both of these attacks aim to find the correct password through exhaustive methods (brute-force) or by testing against a list of common passwords or words (dictionary). If either attack is successful, the program notifies the user of the discovered password, granting access to the protected content.

Here is the working process of BruteForce and Dictionary Attack.

1) BruteForce Attack.



2) Dictionary Attack.



Overall, this code provides a user-friendly interface for various types of file password cracking, utilizing different techniques such as brute-force and dictionary attacks.

## IV. Result

The Python script provided seems to be a tool designed for cracking passwords used to protect ZIP, RAR, and PDF files. It's likely programmed to employ two common methods for guessing passwords: brute-force attacks, where it systematically tries every possible combination of characters, and dictionary attacks, where it uses a predefined list of common words or phrases. To use the tool, users would input details such as the type of file they want to crack and its location. They may also need to provide a dictionary file if they opt for a dictionary attack.

During the cracking process, the script likely communicates progress to the user, possibly through progress indicators or logs showing successful attempts at finding the password.Error handling is likely built-in to deal with issues like incorrect file paths or unsuccessful password attempts.

1) Main Window with both Bruteforce and Dictionary Methods

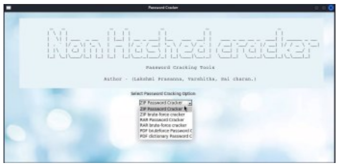


Fig. 5. Main Window

2) ZIP Password Cracker with Bruteforce Method

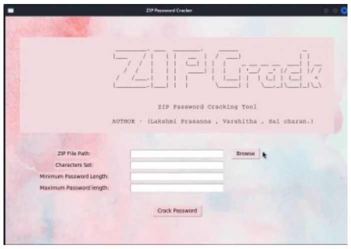


Fig. 6. ZIP-Bruteforce

3) ZIP Password Cracker with Dictionary Method

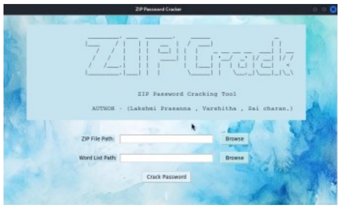


Fig. 7. ZIP-Dictionary

4) RAR Password Cracker with Dictionary Method

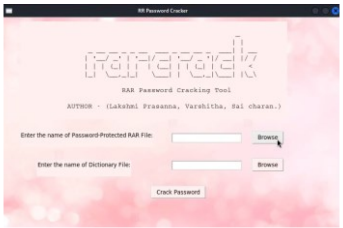

RR Password Cracker
rarcrack
RAR Password Cracking Tool
AUTHOR - (Lakshmi Prasanna, Varshitha, Sai charan.)
Enter the name of Password-Protected RAR File:
Browse
Enter the name of Dictionary File:
Browse
Crack Password

Fig. 8. ZIP-Dictionary

5) PDF Password Cracker with Bruteforce Method

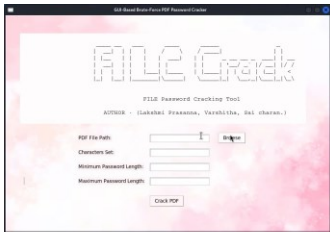
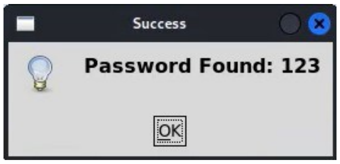

GUI-Based Brute-Force PDF Password Cracker
FILE Crack
FILE Password Cracking Tool
AUTHOR - (Lakshmi Prasanna, Varshitha, Sai charan.)
PDF File Path:
Browse
Characters Set:
Minimum Password Length:
Maximum Password Length:
Crack PDF

Fig. 9. Enter Caption

6) Result for the above File cracker



Password Found: 123

Fig. 10. Result

## V. ADVANTAGES AND DISADVANTAGES

Password-cracking attacks are on the rise, largely because many people use weak passwords and don't manage them securely. Cybercriminals are also getting better at cracking passwords using advanced tools and techniques. This is a serious problem because password cracking is illegal and unethical, and if caught, perpetrators can face severe legal consequences.

When passwords are cracked, it can cause a lot of damage. Personal and sensitive information can be stolen, leading to financial losses and harm to a person's reputation. For businesses and organizations, the consequences can be even more severe, including data breaches, financial repercussions, and damage to their reputation.

That's why it's crucial for both individuals and organizations to understand how password-cracking attacks work. By knowing the techniques used by cyber criminals, people can prioritize strong password security practices and take steps to protect themselves from unauthorized access to their accounts and sensitive information. It's all about staying one step ahead of the hackers and safeguarding our digital lives.[13]

The following are the Advantages and Disadvantages Of Non-Hashed Password Cracking Tool

1) Advantages

- Ensure that you have legal authorization to perform password cracking activities. Only crack passwords on files or systems that you have permission to test.

- Utilize comprehensive and diverse wordlists when attempting to crack passwords. These lists should include commonly used passwords, dictionary words, permutations, and variations.

- Conduct systematic brute-force testing within reasonable limits. Start with shorter passwords and progress towards longer ones, adjusting the character set as needed.

- Employ dictionary attacks using wordlists tailored to the specific application or target. These wordlists may include common passwords, phrases, or terms related to the target domain.

- Optimize your password cracking tool to utilize multi-threading or parallel processing capabilities, where possible, to enhance performance.

- Keep detailed records of your password cracking activities, including the methods used, results obtained, and any vulnerabilities identified. Report findings to relevant stakeholders promptly.

- Regularly update and customize wordlists based on emerging trends, new password patterns, andspecific target characteristics. Tailoring wordlists to the target domain can improve cracking success rates.

- View password cracking as a security assessment tool rather than an end goal. Identify weaknesses in password policies, user behavior, and system configurations to improve overall security posture.

2) Disadvantages

- Never attempt to crack passwords on systems or files without explicit authorization. Unauthorizedaccess or unauthorized cracking is illegal and unethical.

- Avoid using pirated or unauthorized password cracking tools. Utilize only legitimate and reputable tools that are obtained and used within the bounds of the law.

- Refrain from sharing cracked passwords with unauthorized individuals or entities. Passwords obtained through ethical hacking activities should be treated with confidentiality and used responsibly.

- Avoid conducting excessive or unreasonable password cracking attempts that could disrupt systems, networks, or services. Exercise caution to prevent denial-of-service or performance issues.

- Do not overlook legal, regulatory, or compliance requirements related to password cracking activities. Ensure compliance with relevant laws, regulations, and organizational policies.

- Do not misuse cracked passwords for unauthorized access, data theft, or malicious activities. Respect user privacy and security by handling cracked passwords responsibly.

- Respect user privacy and confidentiality when handling cracked passwords. Avoid accessing or disclosing sensitive information contained in cracked files or accounts.

- Don’t underestimate the importance of password complexity in password cracking. Consider factors such as password length, character diversity, and entropy when selecting cracking strategies.

By adhering to these advantages and disadvantages, secu- rity professionals can conduct ethical and effective password cracking activities while maintaining integrity, legality, and ethical standards.

## VI. CONCLUSION

This paper provides an overview of cybersecurity, focusing on passwords and their vulnerabilities. It discusses various potential attacks and how they are carried out, including the use of different tools for implementation.

A password cracker tool is introduced as software designed to recover or guess passwords for accessing computer systems, networks, or encrypted data. These tools are primarily usedto gain unauthorized access to protected resources.

Non-hashed password cracking is depicted as a complex aspect of cybersecurity that requires careful consideration of multiple factors. Security professionals are advised to adhere to certain guidelines to conduct password cracking activities effectively, ethically, and responsibly.

Strategies such as using appropriate tools and techniques, combining attack methods, and verifying cracked passwords are recommended to improve success rates while also respecting user privacy and confidentiality. It’s crucial to be aware of resource consumption, legal boundaries, and ethical considerations to prevent harm and comply with regulations.

The ultimate goal of non-hashed password cracking is to enhance security by identifying weaknesses in password policies, user behaviors, and system configurations. Bytreating password cracking as a security assessment tool and providing actionable recommendations for strengthening password security, organizations can better protect their assets and reduce the risk of unauthorized access.

## VII. References

[1] Tejaswi Kakarala, Aakif Mairaj, Ahmad Yazdan Javaid, ”A Real- World Password Cracking Demonstration Using Open Source Tools for Instructional Use,” University of Toledo, 2018. [Online]. Available: https://ieeexplore.ieee.org/document/8500257. [Accessed: February 29, 2024].

[2] Brute Force Attack,” Kaspersky, Available: https://www.kaspersky.com/resource-center/definitions/brute-force-attack, [Accessed: February 29, 2024].

[3] ”Brute Force Attack,” Cloudflare Learning, Available: https://www.cloudflare.com/en-in/learning/bots/brute-force-attack/, [Accessed: February 29, 2024].

[4] ”What is a Dictionary Attack?,” GeeksforGeeks, Available: https://www.geeksforgeeks.org/what-is-a-dictionary-attack/, [Accessed: February 29, 2024].

[5] ”What is a Dictionary Attack?,” Kaspersky, Available: https://www.kaspersky.com/resource-center/definitions/what-is-a-dictionary-attack, [Accessed: February 29, 2024].

[6] HYPR. ”Dictionary Attack,” HYPR Security Encyclopedia. [Online]. Available: https://www.hypr.com/security-encyclopedia/dictionary-attack. [Accessed: February 29, 2024].

[7] ”Rainbow Table Attack,” Beyond Identity Glossary, [Online]. Available: https://www.beyondidentity.com/glossary/rainbow-table- attack. [Accessed: February 29, 2024].

[8] Social Engineering Attacks to Watch Out For,” State of Security, [Online]. Available: https://www.tripwire.com/state-of-security/5-social-engineering-attacks-to-watch-out-for. [Accessed: February 29, 2024].

[9] Howard Poston, ”Popular Password Cracking Tools,” Infosec Institute, [Online]. Available: https://resources.infosecinstitute.com/topics/hacking/10-popular-password-cracking-tools/. [Accessed: February 29, 2024].

[10] Joseph Carson, ” Most Popular Password Cracking Tools and How to Protect Your Enterprise,” Delinea, [Online]. Available: https://delinea.com/blog/5-most-popular-password-cracking-tools-and-how-to-protect-your-enterprise. [Accessed: February 29, 2024].

[11] ”Password Hacker: How They Hack,” Okta, [Online]. Available: https://www.okta.com/identity-101/password-hacker/. [Accessed: February 29, 2024].

[12] Mindaugas Jancis ”Password Cracking Techniques: The Best Password Managers,” CyberNews, [Online]. Available: https://cybernews.com/best-password-managers/password-cracking-techniques/. [Accessed: February 29, 2024].

[13] ”What is Password Cracking?,” InfoSec Train, [Online]. Available: https://www.infosectrain.com/blog/what-is-password-cracking/. [Accessed: February 29, 2024].