Continue

In an age where data protection and privacy are paramount, password-protected zip files serve as a common method for securing sensitive information. However, ethical hacking and cybersecurity professionals often need to access these files for legitimate reasons: assessing security vulnerabilities, recovering forgotten passwords, or conducting forensic investigations. This article explores the steps and tools necessary to crack a password-protected zip file using Kali Linux, a popular distribution tailored for penetration testing and security auditing. Ethical Considerations Before delving into the technical procedures, it is crucial to emphasize the ethical considerations involved in password cracking. Unauthorized access to files, regardless of the method used, is illegal and unethical. The techniques discussed here should only be applied to zip files and systems where you have explicit permission to test. Always adhere to the principles of ethical hacking and make sure your intentions are aligned with legal guidelines and ethical standards. Understanding Zip File Encryption A zip file is an archive file format that compresses one or more files into a single package, making it easier to transfer or store. When a zip file is password-protected, the contents can only be accessed after entering the correct password. The most common encryption methods used in zip files include: ZipCrypto: An older encryption method that provides only basic protection. AES (Advanced Encryption Standard): A more secure encryption method that is prevalent in modern compressions. Tools for Password Cracking Kali Linux comes equipped with several tools that can be employed to crack password-protected zip files. Some of the most popular tools are: fcrackzip: A simple and efficient command-line tool designed specifically for cracking zip file passwords. It can use brute-force attacks or dictionary attacks to locate the password. John the Ripper: A well-known password cracking software that supports various formats, including zip file passwords. Hashcat: A powerful password recovery tool known for its speed and effectiveness in password cracking. Preparing Your Environment Before starting the process, ensure you have Kali Linux installed and updated. You can run Kali Linux from a DVD, USB drive, or as a virtual machine. Update Your System: Begin by updating your package lists to ensure you have the latest versions of all installed tools: sudo apt update && sudo apt upgrade -y Install Necessary Tools: If the tools mentioned are not pre-installed, you can install them as follows: sudo apt install fcrackzip john hashcat -y Step-by-Step Guide to Cracking Zip File Passwords Method 1: Using fcrackzip Access Terminal: Open the terminal in Kali Linux. This is where you will execute your commands. Check the Zip File: Before proceeding, check the details of the zip file using the unzip command: unzip -l yourfile.zip This will list the contents of the zip file but will fail if the file is password-protected. Run fcrackzip: To crack the password using brute force, use the following command: fcrackzip -b -c a -l 1-6 yourfile.zip Here, -b indicates a brute-force attack, -c a specifies the character set (lowercase letters), and -l 1-6 indicates the length of the password (from 1 to 6 characters). Using a Dictionary Attack: If you have a list of common passwords, you can use a dictionary attack: fcrackzip -D -p /path/to/dictionary.txt yourfile.zip Replace /path/to/dictionary.txt with the path to your dictionary file. Analyze Results: After running the tool, if it finds the password, it will display it on the terminal. Use the discovered password to unzip the file: unzip -P discovered_password yourfile.zip Method 2: Using John the Ripper Prepare the Zip File: First, create a compatible format for John by converting the zip file into a hash format using the zip2john utility: zip2john yourfile.zip > zip_hash.txt Run John the Ripper: Now that you have the hash file, you can start cracking it using John: john zip_hash.txt Monitor Progress: You can check the status of the cracking process at any time by using: john --status Retrieve the Password: Once John finds the password, you can see the results by running: john --show zip_hash.txt Unzip the File: With the password now known, you can extract the contents: unzip -P discovered_password yourfile.zip Method 3: Using Hashcat Converting the Zip File: Similar to John, you can convert the zip file into a hash format: zip2john yourfile.zip > zip_hash.txt Running Hashcat: Now that you have the hash, you can run Hashcat on it. Specify the hash type as 13600 for zip files: hashcat -m 13600 zip_hash.txt /path/to/dictionary.txt Monitor the Progress: Hashcat provides a variety of options and flags to customize the attack. You can check the progress using: hashcat -D View the Cracked Passwords: Once completed, view the results using: hashcat --show zip_hash.txt Extract the Contents: Finally, use the discovered password to unzip the file: unzip -P discovered_password yourfile.zip Tips for Effective Password Cracking Use High-Quality Dictionaries: The effectiveness of a dictionary attack largely depends on the quality and relevance of your password list. Consider using specialized lists that contain common passwords or variations of them. Combine Methods: If one method fails, trying another can prove fruitful. For example, first try dictionary attacks, then follow up with brute-force attacks if unsuccessful. Optimize Settings: Adjust your settings to accommodate large password lengths or wider character sets if you suspect a more complex password. Patience is Key: Cracking passwords, particularly strong ones, can take substantial time. Be patient and monitor progress regularly. Conclusion Cracking a password-protected zip file using Kali Linux requires a solid understanding of the associated tools and techniques. While the methods presented can be quite effective, always remember to operate within ethical and legal boundaries. Engaging in unauthorized access or attempting to crack passwords without permission is strictly against the law. This guide provided a comprehensive picture of how to approach cracking zip files, maintaining a focus on ethical practices and responsible use of acquired skills. As cybersecurity threats evolve, staying updated on the latest tools and techniques remains critical for anyone involved in the field. By utilizing the right strategies and tools, you can recover access to your own files or help organizations shore up their defenses against potential vulnerabilities. fcrackzip is a fast password cracker partly written in assembler. It is able to crack password protected zip files with brute force or dictionary based attacks, optionally testing with unzip its results. It can also crack cpmask'ed images.This package is useful for pentesters, ethical hackers and forensics experts.Installed size: 80 KBHow to install: sudo apt install fcrackzipDependencies:fcrackzipA Free/Fast Zip Password Crackerroot@kali:~# fcrackzip -h fcrackzip version 1.0, a fast/free zip password cracker written by Marc Lehmann You can find more info on USAGE: fcrackzip [-b|--brute-force] use brute force algorithm [-D|--dictionary] use a dictionary [-B|--benchmark] execute a small benchmark [-c|--charset characterset] use characters from charset [-h|--help] show this message [--version] show the version of this program [-V|--validate] sanity-check the algortihm [-v|--verbose] be more verbose [-p|--init-password string] use string as initial password/file [-l|--length min-max] check password with length min to max [-u|--use-unzip] use unzip to weed out wrong passwords [-m|--method num] use method number "num" (see below) [-2|--modulo r/m] only calculcate 1/m of the password file... the zipfiles to crack methods compiled in (* = default): 0: cpmask 1: zip1 *2: zip2, USE_MULT_TAB Display zip informationroot@kali:~# fcrackzipinfo --help fcrackzip version 1.0, zipinfo - tell me about a zip file written by Marc Lehmann You can find more info on USAGE: zipinfo file... the zipfiles to parse ZIP files, while convenient for compressing and grouping multiple files, can sometimes pose a challenge when encrypted with a forgotten passphrase. John the Ripper, often simply referred to as "John," offers a solution for attempting to retrieve or "crack" these passwords. In this comprehensive guide, we'll delve deep into how to use `John` for ZIP password recovery. fcrackzip is a lightweight utility designed specifically to address this, allowing users to recover lost ZIP passwords.Disclaimer: It's crucial to reiterate that attempting to crack ZIP files without proper authorization is both unethical and illegal. Always ensure you have explicit permission.1. Understanding John the Ripper:John the Ripper is a renowned open-source software designed for password cracking. Originally developed for UNIX, John now supports various platforms and has seen significant community contributions, most notably in the "John the Ripper Jumbo" community-enhanced edition, which we'll be focusing on given its broader support for numerous file formats.2. Setting Up Your Environment:Installation: Many Linux distributions have John available in their repositories. However, for our purposes, it's best to use the Jumbo version. It can be cloned from its official GitHub repository and compiled using the provided instructions.Dependencies: Ensure you have necessary dependencies installed, such as libssl-dev, which is required for some of John's functionalities.Before attempting to crack a password, John requires the cryptographic hash from the ZIP file:Utilize zip2john to extract this hash:zip2john /path/to/your/protected.zip > ziphash.txtThis command processes the ZIP and extracts the necessary hash into ziphash.txt.4. Understanding John's Cracking Methods:Simple Cracking:For a straightforward attack using John's default wordlist:john ziphash.txtWordlist Attack:Supply a custom wordlist with the --wordlist option:john ziphash.txt --wordlist=/path/to/custom/wordlist.txtA plethora of wordlists can be found online, including the famous RockYou list, which contains millions of passwords leaked in real-world breaches.Rules-Based Attack:John can utilize rules to mutate words from a wordlist, creating variations and potentially matching more passwords:john ziphash.txt --wordlist=/path/to/wordlist.txt --rulesIncremental Attack:This brute-force method tries all possible character combinations:john ziphash.txt --incremental=AllIt's worth noting that while powerful, incremental attacks can be incredibly time-consuming for complex passwords.Mask Attack:If you know specific details about the password structure (e.g., starts with four letters followed by four numbers), you can use a mask attack:john ziphash.txt --mask=?l?l?l?l?d?d?d?d5. Post-Cracking Steps:After John cracks the password, retrieve it with:john --show ziphash.txtThis command displays the ZIP file's name and its associated password.1. Introduction to fcrackzipfcrackzip is a fast password cracker partly written in assembler, designed to crack password-protected ZIP archives. It can work with various methods, ranging from simple brute force to more complex attacks using known parts of the ZIP password.2. Setting Up Your Environment:Installation:Most Linux distributions have fcrackzip readily available in their repositories. It can typically be installed using the package manager:sudo apt install fcrackzip # For Debian/Ubuntusudo yum install fcrackzip # For CentOS/RedHatsudo pacman -S fcrackzip # For Arch Linux3. Using fcrackzip to Crack ZIP Files:Brute Force Attack:If you have no idea about the password's structure or contents, a brute force attack tries all possible combinations:fcrackzip -b -u protected.zipHere, -b indicates a brute force attack, and -u is used to unzip the file with the found password to ensure its correctness.Dictionary Attack:For those with a list of potential passwords, a dictionary attack can be more efficient:fcrackzip -D -p /path/to/wordlist.txt -u protected.zip-D tells the tool to use a dictionary attack, while -p specifies the path to the wordlist.Known Characters:If you recall parts of the password, fcrackzip can use this information to reduce cracking time:fcrackzip -u -l 4-6 -c aA1! protected.zipHere, -l denotes the password length (in this case, between 4 and 6 characters), and -c defines the character set (a for lower-case, A for uppercase, 1 for numbers, and ! for special characters).Reference: I recently took part in a DFIR capture the flag with some colleagues. Participants were provided with a system disk image and asked to mount it and complete a number of challenges to discover various flags hidden within the data. Exercises like this are always both a lot of fun and a good way to share knowledge and learn - after all, there's no better time to pick up new techniques than in the heat of competition. I got most of the answers and finished joint second. One of the questions I didn't have time for, which I deprioritised as I would have needed to look up the methodology, involved discovering the password to an encrypted ZIP file to access the flag inside. To make sure I can complete similar challenges in future CTFs (or live scenarios), I decided to do some digging, crack a ZIP, and document my method. Creating a password-protected ZIP archive To emulate the conditions of the CTF, I needed to create a ZIP archive containing a text file with the would-be flag. Creating the text file is a simple as using echo to write some content to a file. echo "This is a secret file." > secretfile.txt We can then use 7-Zip to create a password-protected ZIP archive. The a option tells 7-Zip that we're adding files to an archive. We then specify the name of the archive and the file we wish to add. Finally, the -p option allows us to add a password - in this case, the very secure thisisapassword. Also note that the lack of a space isn't a typo - that's just the way 7-Zip wants the information to be provided. 7z a archive.zip secretfile.txt -pthisisapassword Now let's check that the password was properly applied to the archive using the GUI. We can see that if we open archive.zip, we can see the file listing inside, but if we double-click to open any of the files we receive a prompt and cannot see the contents without entering the correct password. Cracking the password-protected ZIP archive with fcrackzip The tool we'll use for discovering the password to our ZIP file is fcrackzip. We'll use the -v option to generate verbose output and keep track of what it's doing, and -u, which tells fcrackzip to attempt to use the guessed password to unzip the file to verify that it is correct and reduce the risk of false positives. We have two options as to how fcrackzip will attempt to guess the password. Firstly, we can use the -b option to perform a brute force attack, guessing every possible combination of characters. This is useful for cracking long, unique passwords, but not the quickest method if you think the password may actually just be a simple combination of words, numbers, and symbols. For these scenarios, we'd be better off performing a dictionary attack with -D. This guesses the password by trying every entry in a list of passwords. As such, fcrackzip requires you to provide a dictionary to use with -p. We'll use the popular rockyou.txt dictionary - a mainstay of the cyber security profession. fcrackzip -D -p rockyou.txt -v -u archive.zip When we hit return, fcrackzip will begin trying every password in the dictionary. When one of them successfully unzips the archive, it will stop and tell us what it is. The duration of this process depends on the dictionary, your computer's processing power, and the password's complexity, but in our case the password is so simple that we see results almost instantly. To view the contents of the archive, all we would have to do is copy the password from the output, open the ZIP file in the Linux GUI, and paste it into the password field when prompted. Then voilà - we'd have our flag, attacker-encrypted data, or any other files we were trying to access. No spam - just thought-provoking articles and useful tidbits If this article resonated, feel free to share it with someone who might appreciate it too. If you have thoughts, opinions, or comments to share then I'd love to hear from you - feel free to send me a message on X or an email. In the intricate world of cybersecurity, where data protection is paramount, understanding how to crack password-protected ZIP files becomes a crucial skill. In this comprehensive guide, we'll delve into the powerful tool, fcrackzip, exploring its installation, usage, and strategies to crack encrypted ZIP files. Buckle up as we uncover the secrets of fcrackzip and its prowess in deciphering password-protected archives.In an era where digital security is of utmost importance, the ability to crack password-protected ZIP files is a valuable skill. Our journey begins with fcrackzip, a robust tool designed to decrypt zip files and unveil their concealed passwords. Whether through brute force or dictionary-based attacks, fcrackzip emerges as a reliable ally in the realm of cybersecurity.Installation of Fcrackzip ToolTo kickstart our exploration, let's first install fcrackzip. Open your terminal and execute the following command:sudo apt install fcrackzipOnce installed, access the tool's help menu using:fcrackzip — helpCreating a Password-Protected ZIP File:Before diving into the cracking process, let's generate a password-protected ZIP file. Execute the following commands:sudo touch secretinfo.txt sudo zip — password 12345678 secretinfo.zip secretinfo.txtThese commands create a text file, "secretinfo.txt," and generate a password-protected ZIP file, "secretinfo.zip," with the password "12345678."Cracking the Password with a Dictionary:Now, the real action begins. In dictionary mode, fcrackzip reads passwords from a text file. Execute the following command:sudo fcrackzip -D -p /home/frost/rockyou.txt -u secretinfo.zipBreaking down the command:- `-D`: Specifies the use of a dictionary or wordlist.- `-p`: Specifies the password file.- `/home/frost/rockyou.txt`: Path for the dictionary file (e.g., 'rockyou.txt').- `-u`: Uses unzip.- `secretinfo.zip`: The password-protected ZIP file.Press "Enter" to initiate the cracking process.Read here in detail: In the ever-evolving landscape of cybersecurity, the ability to crack ZIP file passwords is a skill that can't be underestimated. Fcrackzip, with its versatile capabilities, proves to be a formidable tool in this domain. While a strong, complex passphrase enhances security, fcrackzip efficiently handles weaker passwords, often delivering results within minutes.As we navigate the complexities of digital security, remember that responsible use of this knowledge is paramount. The power to crack passwords comes with ethical responsibilities. Stay curious, stay secure!Originally published at . We implement the password anywhere for security purpose, but if you forget the password then it becomes a super headache. You have put the password on rar or zip file and you didn't open for a long time. You forgot password when you tried to open again. Today I am going to share how to crack zip password by using Fcrackzip on both operating system windows as well as Kali Linux. You can crack zip password by running simple commands. some commands will give your a password in clear text formate. Sometimes we want to protect our important documents and put into zip archives. There is a feature into zipping to protect with a password. But forgetting is human nature. If we don't use this file along time and forget the password. The problem starts now. when you forget zip file password. and you are looking for a solution everywhere because you have an important document inside a zip archive. In this tutorial, I am going to give you the solution to this problem. after reading this article you become a zip password hunting person. fcrackzip windows is a very old tool and didn't update for a long time you can download from here Download fcrackzip windows and visit the home page: Follow the given steps to crack zip file password: Download fcrackzip and extract it on Desktop Open cmd and change directory to Desktop See Available options by using the command>fcrackzip.exe –help If you are using Kali Linux then, It was pre-installed in previous versions. In the latest version of Kali Linux fcrackzip is not installed by default so first you need to install on Kali Linux. It is similar and simple to install on Kali Linux, ubuntu, or debian based OS. Kali Linux is one of Debian based operating system. Basically we used the apt-get command to install any package, but package must be on repository. You can't install fcrackzip by apt-get command. I run the following command and get the following error vijay@kali:~$ sudo apt-get install frcackzip [sudo] password for vijay: Reading package lists... Done Building dependency tree Reading state information... Done E: Unable to locate package frcackzip vijay@kali:~$ I understood, the package doesn't exist on repository as i am looking for. So I decided to use another way to install package. I searched around the internet and find a useful link to download fcrackzip for Kali Linux. You can download from this link. I have used wget command to download this file as see example in below: vijay@kali:~$ wget --2020-06-18 12:48:16-- Resolving ftp.br.debian.org (ftp.br.debian.org)... 200.236.31.3, 2801:82:80ff:8000::4 Connecting to ftp.br.debian.org (ftp.br.debian.org)|200.236.31.3|:80... connected. HTTP request sent, awaiting response... 200 OK Length: 28824 (28K) [application/x-debian-package] Saving to: 'fcrackzip_1.0-10_amd64.deb' fcrackzip_1.0-10_a 100%[===============>] 28.15K 58.6KB/s in 0.5s 2020-06-18 12:48:23 (58.6 KB/s) - 'fcrackzip_1.0-10_amd64.deb' saved [28824/28824] vijay@kali:~$ It's comprehended for using ls command to check downloading done or not. You can install deb file on Kali Linux by using dpkg command the command will be as follows: $sudo dpkg -i fcrackzip_1.0-10_amd64.deb vijay@kali:~$ sudo dpkg -i fcrackzip_1.0-10_amd64.deb Selecting previously unselected package fcrackzip. (Reading database ... 297995 files and directories currently installed.) Preparing to unpack fcrackzip_1.0-10_amd64.deb ... Unpacking fcrackzip (1.0-10) ... Setting up fcrackzip (1.0-10) ... Processing triggers for kali-menu (2020.2.1) ... Processing triggers for man-db (2.9.1-1) ... vijay@kali:~$ You can follow the given steps: Open terminal and execute the following command#fcrackzip –help In this example I am going to show you about brute force attack and with fcrackzip -b switch can be used for the brute-force attack. If you want to use dictionary attack use -D switch.You can use the following command to crack zip password by fcrackzip tool in Kali Linux fcrackzip -b -c 'a1' -l 6-10 -v -u /root/Desktop/sssss.zip Here: -b = brute-force attack -c = Charset 'a1' (a for small alphabet and 1 for numeric value) -l = Length of password (min length-max length) -v = verbose (no compulsory) -u = Use unzip and path of password protected file Hit Enter and wait for the password! The fcrackzip utility and wordlists are included by default in Kali to crack passwords for these compressed files. Because of their compact size and encryption algorithm, we frequently use zipped files. These zipped files have a password protection feature that ensures the files' confidentiality. When you've forgotten your password and are stuck trying to figure out how to hack it, fcrack comes to your rescue to save the day and show you how to encrypt your papers. With the support of fcrackzip, which is available in Linux, you can easily crack a secure zip file. Installation: fcrackzip is a tool that can be used to decrypt zip files and determine their passwords. The brute-force method is used in this tool. Fcrackzip can be installed in a few basic steps: Step 1: $ sudo apt update Step 2: $ sudo apt-get install fcrackzipVerify Installation: Since we're using Kali Linux, the fcrackzip utility is already installed; all we have to do now is open the terminal and type "fcrackzip --help" and the tool's help command will run. fcrackzip --helpCreating a zip file that is password-protected: To begin, we must generate a password-protected file. To do so, we must first pick the file that we want to secure with that format, and then we must execute the instruction. sudo zip --password abc123 file.zip luv.txtUsing fcrackzip, you can crack zip passwords: To use a brute force attack, fcrackzip is a powerful and simple method for performing a brute force attack on any zip file. To do so, we would use various formats to break the zip file's password. To do so, we'll use (-b) to enable us to brute force the zip file, (-c) to describe the dictionary's charset, and (-u), which allows us to see only the right outcome in the result. sudo fcrackzip -b -c 'a1' -u file.zipGetting the zip file's password with Verbose mode: Verbose is a mode in fcrackzip that can be enabled with the (-v) parameter. Now that you're in verbose mode, you'll get a lot more stuff. In our case, the verbose mode allows us to obtain information about the file in the password-protected zip file, such as its height, name, and the current dictionary combination that is added to that zip file. sudo fcrackzip -b -c 'a1' -v -u file.zipCracking a password of a certain length: To do so, we used the same command we used to build a password-protected zip file to create a password-protected zip file. In this case, we use two different parameters, such as (-c 'a'), which we formerly used for a different function but are now using for adding numeric charset. The second variable is (-l). The length of the password is defined by this parameter (minimum length – maximum length). sudo fcrackzip -b -v -c 'a' -l 1-5 -u file.zipCracking a password with supplying the initial password: We have a set initial password for brute force with the name string to provide keys for dictionary matching, and we can provide them with a set of strings to apply certain keywords to their dictionary with this parameter. sudo fcrackzip -b -v -c 'a' -p rishu file.zipCracking a password with Dictionary: In this mode, fcrackzip can read passwords from a file that we provide; the file must contain one password per line and be alphabetically ordered for fcrackzip to function properly. Using the command syntax below to use fcrackzip for the rockyou.txt wordlist. It's not necessary to create a hash file. sudo fcrackzip -u -D -p /usr/share/wordlists/rockyou.txt file.zip praise munene Posted on Mar 14, 2022   Hello,today am going to show you how to crack password protected zip files in kali linux. Kali linux is pre installed with password cracking tools namely: 1.John the ripper 2.Fcrackzip utility 3.Wordlists We'll focus more on john the ripper which is pre-installed in most unix operating systems. However if your linux operating system lacks this tools,you can install or update the necessary packages with the following commands: $sudo apt update $sudo apt install john fcrackzip wordlists John the ripper will use its own wordlist located in the /user/share/john/password.lst to crack the password.you can also locate all the wordlists in your system by typing the following command: $locate wordlist Step 1:create a password protected zip file The only other thing needed to start is a password protected zip file. Follow the steps: Create a text file add some text and name it say hacker.txt. Open the terminal in the directory and type the following command $zip -password 12345678 hacker.zip hacker.txt The command creates a zip file with the password of your choosing after the word password in the shell command above. Replace the file names and paths to your own. Step 2:get the password hash To get the password hash to be cracked, we need to enter the command: $zip2john hacker.zip Step 3:put the password hash in a text file Type the following command : $zip2john hacker.zip > hash3.txt Followed by: $John hash.txt Sometimes you may need to customize or create your own wordlist or use a different wordlist the command follows the following format $john –wordlist= the wordlist path saved hashes I.e $john --wordlist= /usr/share/wordlists/rockyou.txt hacker.txt The time taken to crack each password varies with the strength of the password