Guardian of The Digital Realm: A Journey with John the Ripper

Alisha Mungro & Jaiven Harris

Lenoir-Rhyne University

CSC 120: Survey of Computing

Dr. Ajay Kumara

November 29, 2023

Guardian of The Digital Realm: A Journey with John the Ripper

About 38% of Americans reports of having their password word cracked or guessed and many people get easily hacked with just either a weak password or just using the same passwords for different websites can really be bad for you. With technology quickly advancing, hackers are learning new ways to infiltrate systems and gain access to individuals and organizations sensitive information; this is called cybercrime. According to Kaspersky website, cybercrime is defined as criminal activity that targets a computer, computer network or device and this can include obtaining the passwords of those devices. In order to mitigate this, we must fight hackers with the same hacking/cracking tools and techniques. One password cracking tool that helps mitigate cybercrime is called John the Ripper. First released in 1996, John the Ripper is a password cracking tool designed to test the strengths of passwords, encrypted (hashed) passwords, and crack passwords (Sharma, 2020). The tool incorporates several key characteristics, such as providing diverse modes for accelerating password cracking, automatically identifying the hashing algorithm utilized in encrypted passwords, and offering straightforward operation and configuration. These attributes contribute to making the tool a preferred choice for both beginners and experienced professionals in the realm of password cracking.

John the Ripper offers numerous methods for password cracking. In this project, our emphasis on cracking passwords is centered around utilizing wordlist mode, commonly known as dictionary attacks, single crack mode, and generating text documents containing hashed passwords, which were then supplied to John the Ripper. Hashing involves transforming an alphanumeric string into a fixed-size string through a hash function, a mathematical process that takes an input string and produces another alphanumeric string; our passwords are never stored in the format that we type it in. When registering on a website for example, the password undergoes hashing before storage. During login attempts, the same hashing algorithm generates a hash for the input, which is then compared with the original hash stored in the database. This ensures that passwords are not stored in plain text, with the algorithm consistently producing the same results for identical data inputs. With John the Ripper, the tool will recognize the hashed text, begin to generate hashes on the fly, and stop when a generated hash matches the given hash. Given the principles outlined and the comprehension of password storage and hashing, this project seeks to offer valuable insights into the processes of cracking password-protected zip files, Kali Linux passwords, and hashed passwords using wordlist and single crack mode. For simplicity, John the Ripper will be abbreviated as John throughout the project.

Installation

John can be installed onto many different operating systems. However, this project utilizes Kali Linux as the preferred operating system to perform the different cracking techniques. On Kali Linux, John is pre-installed into the operating system. To begin this project, you need to open up a terminal on Kali Linux (utilizing a terminal will be used for the entire project) and ensure that John is indeed pre-installed. You can check this by typing in the following command:

The output of this command will showcase that John is installed into Kali Linux. Here is the output for this command:

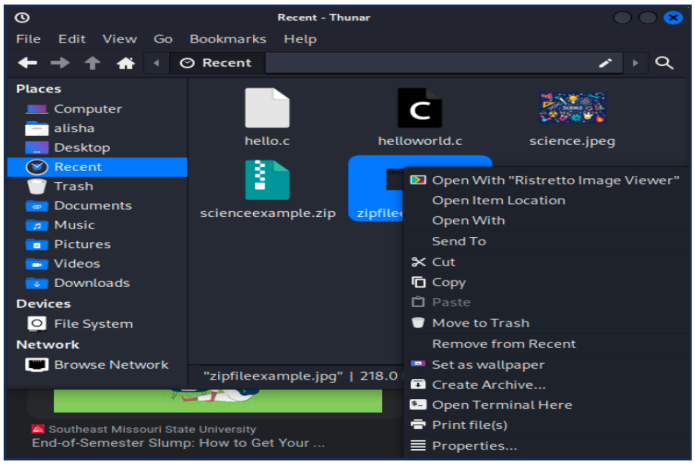
```
John the Ripper 1.9.0-jumbo-1+bleeding-aec1328d6c 2021-11-02 10:45:52 +0100 OMP [linux-gnu 64-bit aarch64 ASIM
D AC]
Copyright (c) 1996-2021 by Solar Designer and others
Homepage: https://www.openwall.com/john/

Usage: john [OPTIONS] [PASSWORD-FILES]

Use --help to list all available options.
```

Once completing this verfication step, we are now ready to begin cracking hashed passwords.It is crucial to note that the terminal is case sensitive. Therefore, you must type in things exaclty as they appear.

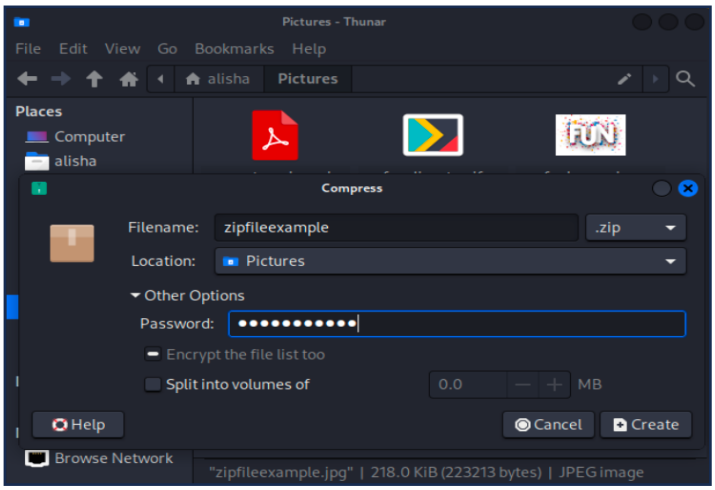
Cracking a Password Protected Zip File

Cracking the password for a password protected zip file is fairly simple. To begin, you need to search the web for a picture (can be any picture desired), download the image, and then save it as a file onto the Kali Linux Desktop. For this example, we have named the file “zipfileexample’. The following steps are as followed:

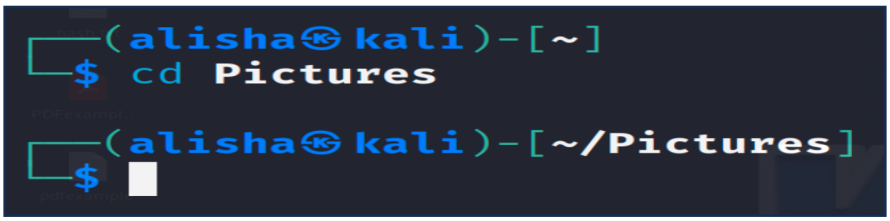
1. Click on the ‘Home’ icon on the desktop
2. Click Recent Folder
3. Locate the recently saved image. Right-click the image and select ‘Create Archive’



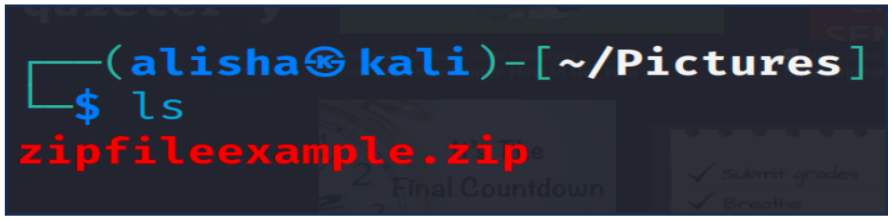
4. Ensure the file is formated to ‘zip’ and click the ‘Other Options’ and input a password for the image. For this example, we are going to input ‘12345 as the password. Ensure the location is ‘Pictures’. Hit ‘Create’ once password is keyed in.



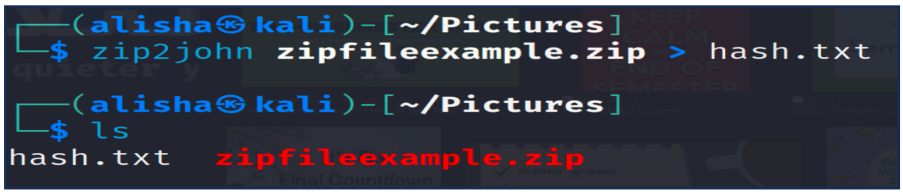
5. Open a terminal and type the command ‘cd Pictures’. ‘cd’ is a command that stands for ‘Change Directory’. We want to change the directory because we have saved our image into the ‘Pictures’ directory. The output of this command should should that instead of being in the home directory (~) we are now in the ‘Pictures’ directory.



6. Type the command ‘ls’ to have the terminal list all the files in the current directory (Pictures). This will ensure that the image we saved is in the directory that we are in. The output of this command will list all the current files inside the current directory. We see that the ‘zipfileexample’ saved into the current directory.

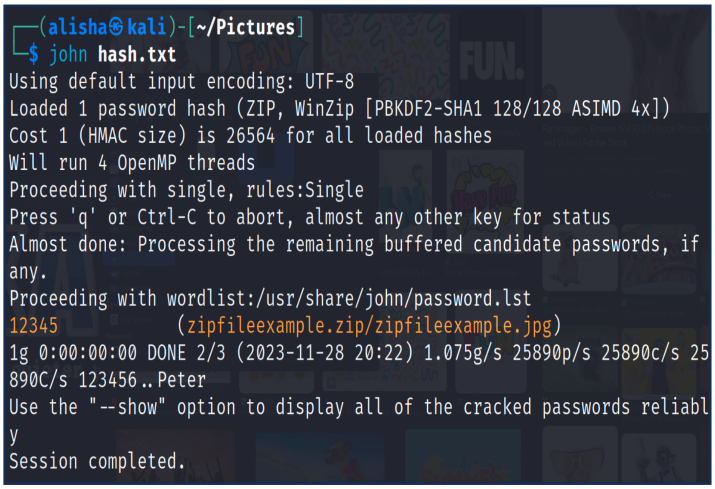


7. Next, we are going to create a text file that contains the hashed format of the password protected zip file. Remember that in order for John to crack passwords, the tool must be given the hashed format of the password in question. To do this, we are going to type the command ‘zip2john zipfileexample.zip > hash.txt’. We are going to then confirm that the text file was created by typing the command ‘ls’ to listen the files in the current directory.
    a. ‘zip2john’ finds the hashed password for the zip file on question and extracts it
    b. ‘> hash.txt’ tells john to save the results of the extraction into a text file called ‘hash.txt’.



8. Now we can begin to crack the hashed password for the zip file. The command we are using is ‘john hash.txt’.
    a. ‘john hash.txt’ tells John to crack the text file ‘hash.txt’ that contains the hashed password.
    b. We see in the orange text that John found the password for the zip file to be ‘12345’.

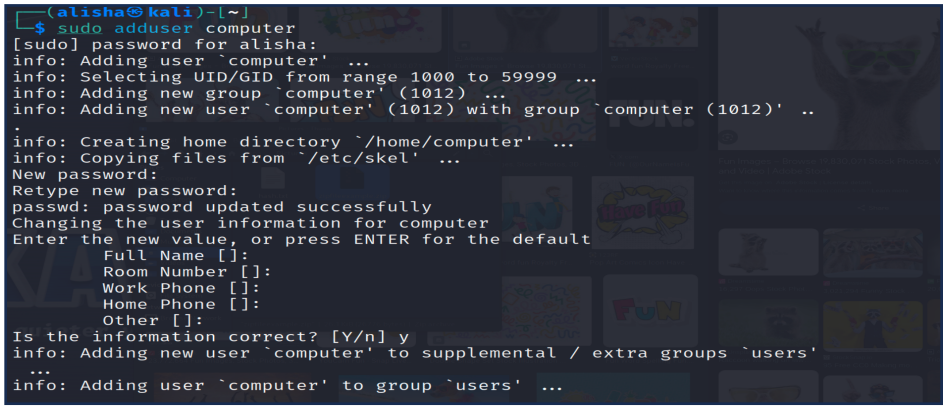
c. The password for the zip file has successfullt been cracked.



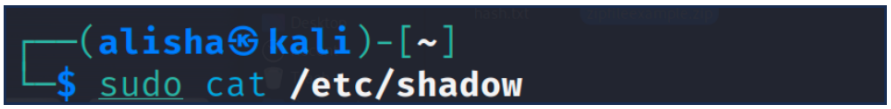
Cracking a Kali Linux Password

In this example, we are going to add a new user to Kali Linux, create a password for that user, and then have John crack the passsword for the user. The steps are as followed:

1. To begin, we need to add a new user to Kali Linux. Open a terminal inside the operating system and type the command ‘sudo adduser science’. You will be prompted to input in your password for Kali Linux.
    a. sudo is an abbreviation for '**S**uper **U**ser **DO**.' When you prepend any command with 'sudo,' it executes that command with superuser or elevated privileges. This is comparable to the "run as administrator" feature in Windows. You will be prompted to put in your Kali Linux password in order to continue with executing the command.
    b. The adduser command informs the operating system about the objective we intend to achieve, which is adding a new user to Kali Linux.
    c. The word ‘science is the name for the user we are create.
2. After inputting in your Kali Linux password, the next command line syntax will prompt you to put in a new password for the user ‘science’. For this example, we have made the password ‘hacker’.
    a. Kali Linux will then ask you if the information inputted is correct. Type ‘Y’ to confirm yes.

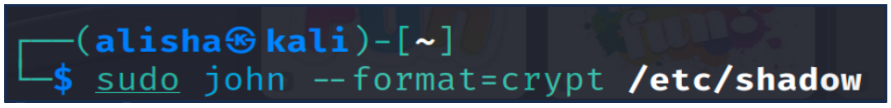


3. In Linux, there are two important files saved in the /etc folder: passwd and shadow.
    a. /etc/passwd: This file retains details such as the username, user ID, login shell, and more.
    b. /etc/shadow: This file encompasses the password hash, password expiry information, and other relevant data.
4. Type the command 'sudo cat /etc/shadow'.
    a. To view this file, we need super user privileges. The command sudo allows us to be able to execute this command.
    b. The command 'cat' reads out the data from a file and gives its contents as an output.
    c. /etc/shadow tells the 'cat' command that we want to view the content within this file.

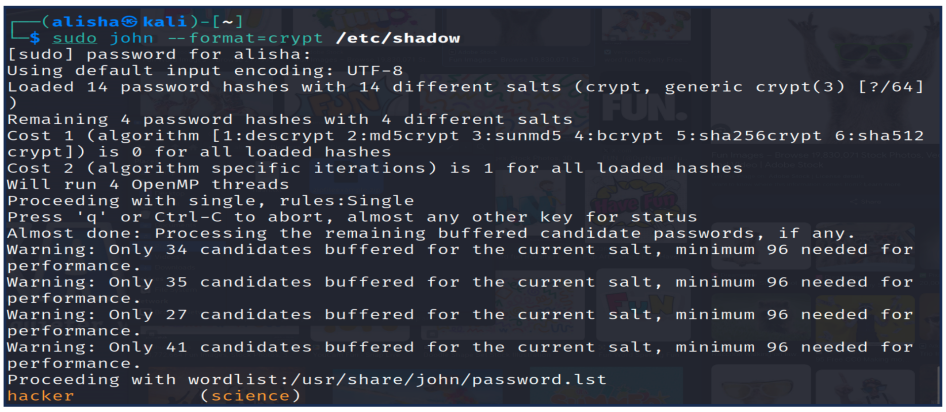


5. Scroll to the bottom of the output and you will see the hashed password for the user science.

6. Now we are going to crack file /etc/shadow that contains the password for the user science. Type in the command 'sudo john --format=crypt /etc/shadow' and then you will be prompted to put in your Kali Linux password in order to execute this command.
    a. To execute this command, we need super user privileges. The command sudo allows us to be able to execute this command.
    b. '—format=' tells John that we are going to tell it the hash format that we want it to use in order to crack the file. 'crypt' tells John that we want it to use the hash format that the Kali Linux operating system uses.
    c. '/etc/shadow' is the file that we want to crack.



7. After running this command, in the orange text, we see that John successfully found the password for the user science to be 'hacker'.

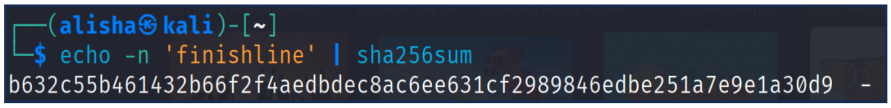


Wordlist Mode

In Wordlist Mode, John the Ripper employs a predetermined list of words, commonly referred to as a wordlist or dictionary, to systematically attempt various password combinations. This mode is recognized as the simplest cracking method supported by John. To utilize it, you only need to specify a wordlist, typically a text file with one word per line, along with the relevant password files. The tool then systematically checks each word in the list to identify a match with the hashed passwords contained in the specified files.

To illustrate this mode, we will select a specific word and instruct John to convert it into the sha256 hash format. Subsequently, we will link that word with a new user, compiling all the associated details, and generate a new text file containing this information. We will then use one of the pre-installed Wordlist contained in Kali Linux to crack the text file. The steps are as followed:

1. Open a terminal and type the command ‘echo -n ‘finishline’ | sha256sum’.
    a. The command ‘echo -n’ tells the operating system to print the word ‘finishline’ exactly as it appears in the hashed format desired.
    b. The command ‘sha256sum’ tells the operating system to convert the word ‘finishline’ into the Sha-256 hashed format. Sha-256 is a patented cryptographic hash function that outputs a value that is 256 bits long.
2. The output of this command showcases the hashed format for the word ‘finishline’.



3. Now we must take this output and compile it into a text file with the user that we want the hashed word to be associated with. In order to complete this, type the command ‘echo user01: b632c55b461432b66f2f4aedbdec8ac6ee631cf2989846edbe251a7e9e1a30d9 > wordlistmode.txt’.
    a. The command ‘echo’ tells the operating system to print the preceding information exactly as it appears as into the text file ‘wordlistmode.txt’.
    b. The information before the semicolon tells the system that we want the username to be ‘user01’. The information after the semicolon tells that system that we want the given hashed text associated with user01.

4. Let’s confirm that the hashed password has been compiled into the file name 'wordlistmode.txt'. Type the command 'cat wordlistmode.txt'.
    a. The command ‘cat’ reads out the data from a file and gives its contents as an output.
    b. We see below that the file contains the content that we created in Step 3.

```
┌──(alisha㉿kali)-[~]
└─$ cat wordlistmode.txt
user01:b632c55b461432b66f2f4aedbdec8ac6ee631cf2989846edbe251a7e9e1a30d9
```

5. Next, we can begin the process of cracking the hashed password for user01 with Wordlist Mode. To being, enter this command as follows:
    a. 'john --wordlist=/usr/share/wordlists/rockyou.txt --format=raw-sha256 wordlistmode.txt'.
    b. The command '--wordlist=/usr/share/wordlists/rockyou.txt' tells John that we want to use Wordlist Mode. Furthermore, it contains the location for the wordlist rockyou.txt that we want to use in order to crack the wordlistmode.txt file.
    c. The command '- -format=raw-sha256' tells John that we want to use the Sha-256 hashed format.
    d. 'wordlistmode.txt' is the file we are wanting to crack that contains the hashed password.
6. After running this command, in the orange text, we see that John successfully found the password for user01 to be 'finishline'.

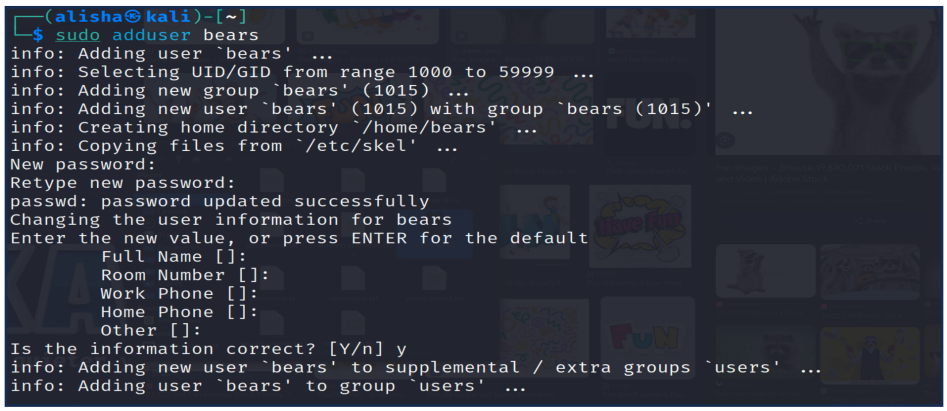
```
┌──(alisha㉿kali)-[~]
└─$ john --wordlist=/usr/share/wordlists/rockyou.txt --format=raw-sha256 wordlist
mode.txt
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-SHA256 [SHA256 128/128 ASIMD 4x])
Warning: poor OpenMP scalability for this hash type, consider --fork=4
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
finishline       (user01)
1g 0:00:00:00 DONE (2023-11-28 22:50) 20.00g/s 9175Kp/s 9175Kc/s 9175KC/s remmer.
.tungalag
Use the "--show --format=Raw-SHA256" options to display all of the cracked passwo
rds reliably
Session completed.
```

Single Crack Mode

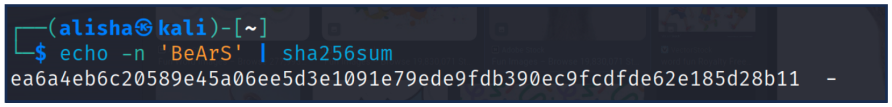
Single Crack mode within John the Ripper is a specialized approach to password cracking that differs significantly from the systematic use of the entire wordlist in Wordlist mode. In this mode, the software selects a single dictionary word and applies diverse transformations to it before initiating the password cracking process. These transformations encompass changes in capitalization, the addition or removal of numbers, incorporation of special characters, and exploration of common variations. The primary objective is to enhance the likelihood of discovering a match with the hashed password, even if the original dictionary word does not precisely align. Unlike the systematic examination of an entire wordlist, Single Crack mode hones in on manipulating a singular word to generate multiple potential password variations. Its efficiency shines in scenarios involving passwords subjected to straightforward modifications or variations from standard dictionary words.

To exemplify this, we'll create a new user in Kali Linux with a password derived as a variation of the user's name. Subsequently, we'll instruct the operating system to convert this password into Sha-256 hashed format for password cracking purposes. The steps are as followed:

1. Open a terminal and type the command ‘sudo adduser bears’.
    a. To execute this command, we need super user privileges. The command sudo allows us to be able to execute this command.
    b. The adduser command informs the operating system about the objective we intend to achieve, which is adding a new user to Kali Linux.
    c. The word ‘bears’ is the name for the user we are create.
2. After inputting in your Kali Linux password, the next command line syntax will prompt you to put in a new password for the user ‘science’. For this example, we have made the password a variation of the user’s name. The password we will be using is ‘BeArS’.
    a. Kali Linux will then ask you if the information inputted is correct. Type ‘Y’ to confirm yes.

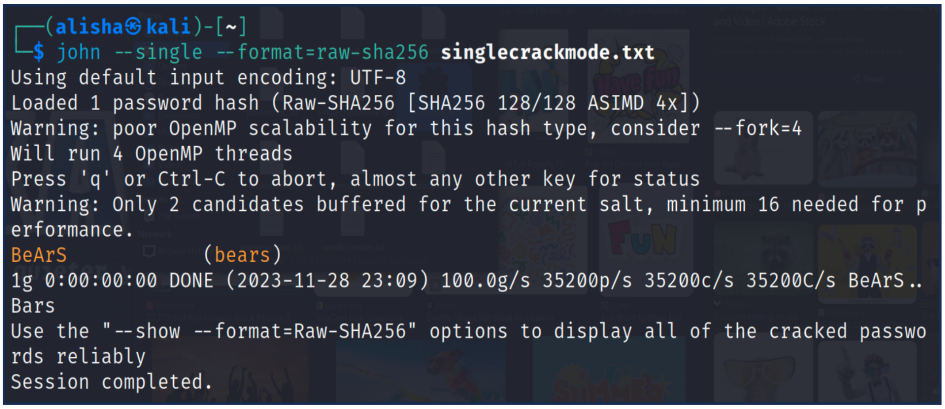


3. Next, we need to tell the operating system to take the password for the user bear and convert the password into Sha-256 hash format. We will then tell the operating system to take the hashed password and save it into a new text file. To begin, type the command ‘echo -n ‘BeArS’ | sha256sum’.
    a. The command ‘echo -n’ tells the operating system to print the word ‘BeArS’, which is the password we created for the user bears and print it exactly as it appears in the hashed format desired.
    b. The command ‘sha256sum’ tells the operating system to convert the word ‘BeArS’ into the Sha-256 hashed format. Sha-256 is a patented cryptographic hash function that outputs a value that is 256 bits long.
    c. The output of this command showcases the hashed format for the word ‘BeArS’.



4. Now we must take this output and compile it into a text file for the user bear. To do this, type the command ‘echo -n bears:ea6a4eb6c20589e45a06ee5d3e1091e79ede9fdb390ec9fcdfde62e185d28b11 > singlecrackmode.txt’.
    a. The command ‘echo’ tells the operating system to print the preceding information exactly as it appears as into the text file ‘singlecrackmode.txt’.
    b. The information before the semicolon tells the system that we want the user ‘bears. The information after the semicolon tells that system that we want the given hashed text associated with the user bears.

5. After completing the previous steps, we are able to crack the hashed password using single crack mode. To begin the password cracking, we need to type the following command: ‘john --single --format=raw-sha256 singlecrackmode.txt’.
    a. The command ‘ --single’ tells John that we want to utilize single crack mode to crack the password.
    b. The command ‘- -format=raw-sha256’ tells John that we want to use the Sha-256 hashed format.
    c. ‘singlecrackmode.txt’ is the file that we want to crack.
6. After running this command, we see that in the orange text, that John has found the password bears to be ‘BeArS’, which is a variation of the user’s name.



References

- *What is cybercrime? How to protect yourself from cybercrime.* (n.d). Kaspersky. Retrieved November 27, 2023, from https://usa.kaspersky.com/resource-center/threats/what-is-cybercrime
- Sharma, A. (2020, July 01). *John the Ripper explained: An essential password cracker for your hacker toolkit.* CSO Online. https://www.csoonline.com/article/569533/john-the-ripper-explained-an-essential-password-cracker-for-your-hacker-toolkit.html
- Shivanandhan, M. (2022, November 17). *How to Crack Passwords using John The Ripper – Pentesting Tutorial.* FreeCodeCamp. https://www.freecodecamp.org/news/crack-passwords-using-john-the-ripper-pentesting-tutorial/
- *John the Ripper's cracking modes.* (n.d.). Open Wall. Retrieved November 28, 2023, from https://www.openwall.com/john/doc/MODES.shtml
- *security.org team. (2023, August 25). America's password habits 2021. Security.org.* https://www.security.org/resources/online-password-strategies/