Lab 5 Password Cracking

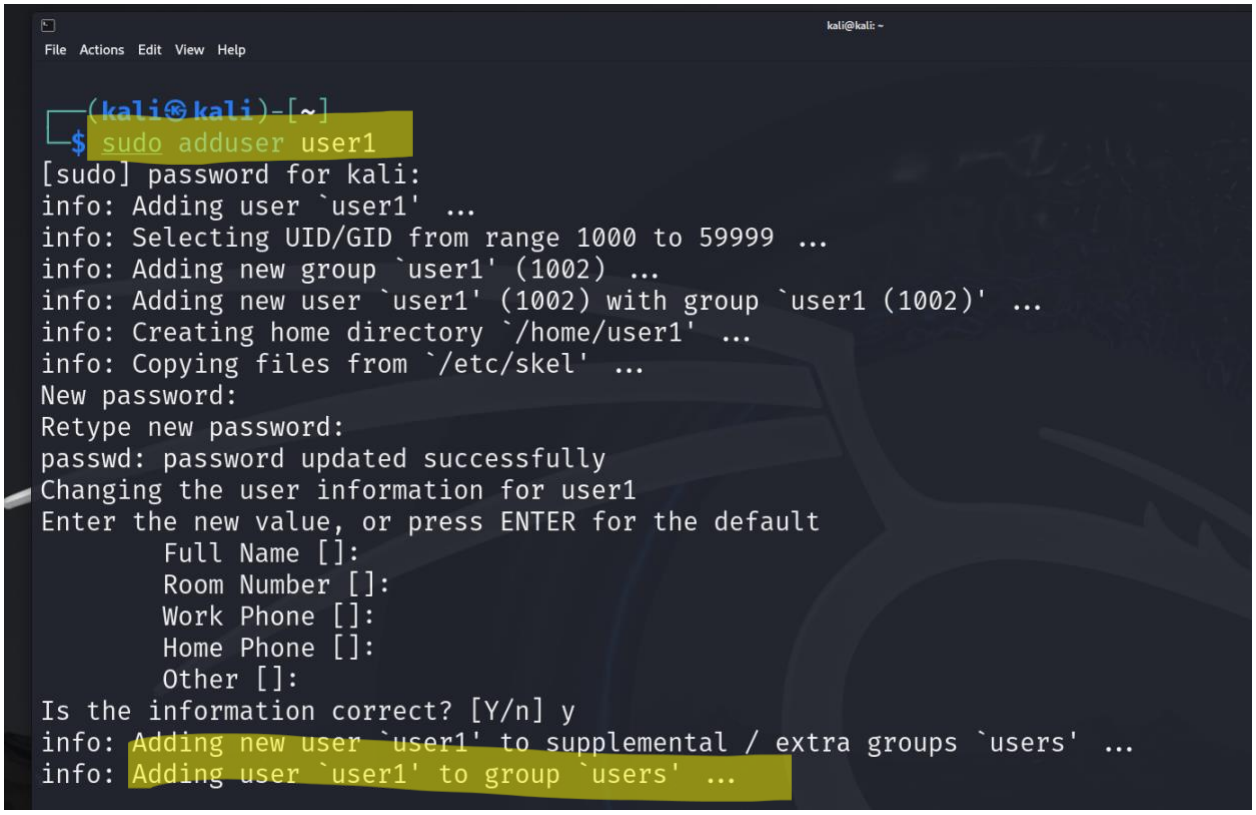
Task A

1. Create 6 users in your Linux Terminal, then set the password for each user that meets the following complexity requirement respectively. You should list the passwords created for each user.

1. For user1, the password should be a simple dictionary word (all lowercase)

Explanation: I set the password to ate and created user 1 with the command **sudo adduser** followed by what I wanted the user name to be, which is user1. Alteranively I can edit thins password later with the command **sudo passwd user1**. User1 will change depending on which user I want to edit. I do this later because I mistyped a password.

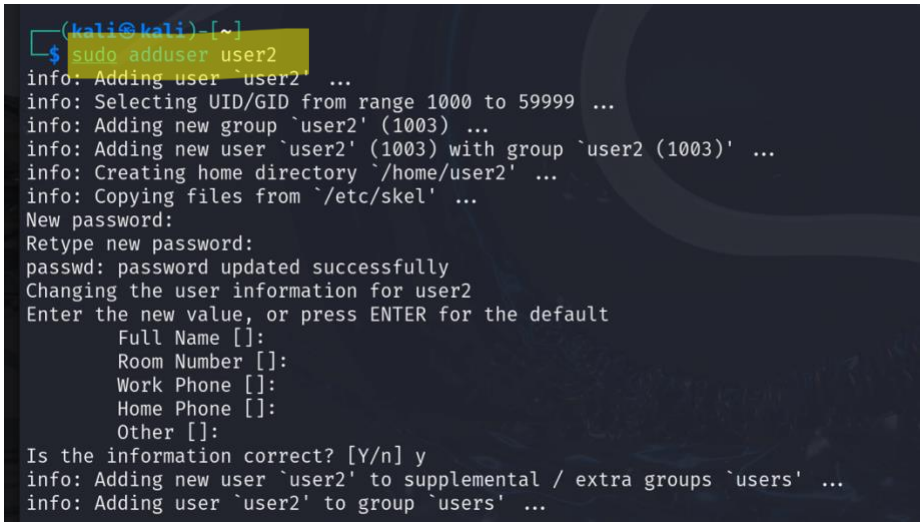
Screenshot:



2. For user2, the password should consist of 4 digits.

Explanation: Password is 1234 and I used the same commands in step 1 but changing user1 to user2.

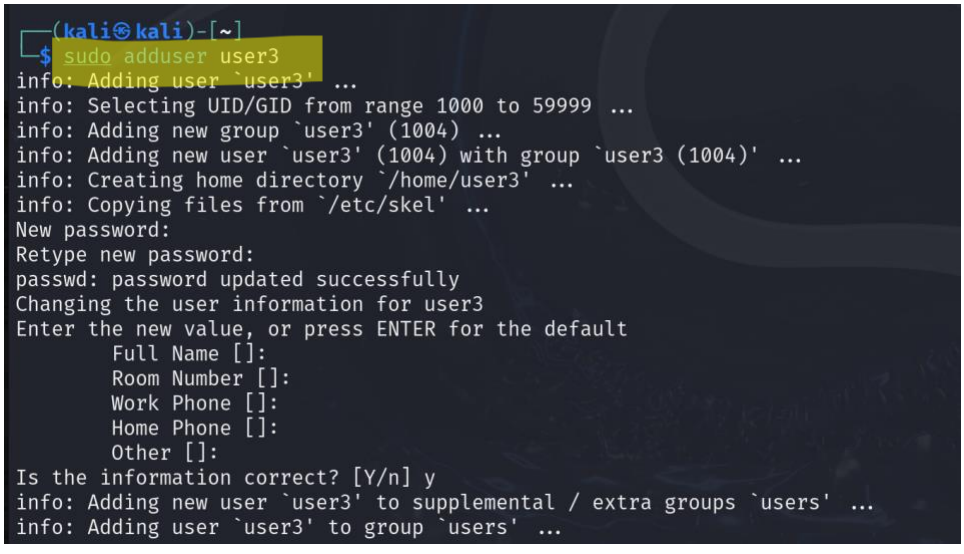
Screenshot:



3. For user3, the password should consist of a simple dictionary word of any length characters (all lowercase) + digits.

Explanation: Password is apple123 and I used the same commands in step 1 but changing user1 to user3.

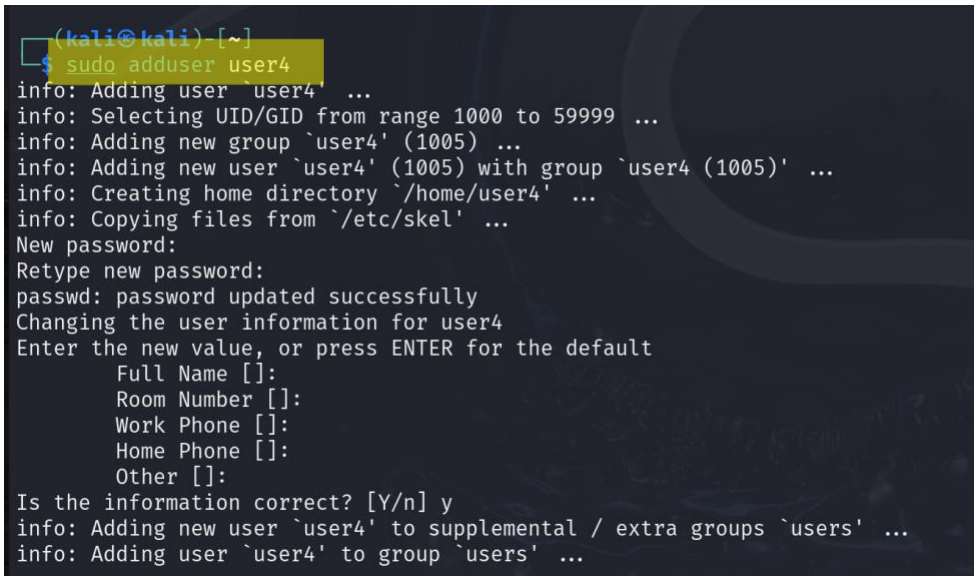
Screenshot:



4. For user4, the password should consist of a simple dictionary word characters (all lowercase) + digits + symbols.

Explanation: Password is pass123! and I used the same commands in step 1 but changing user1 to user4.

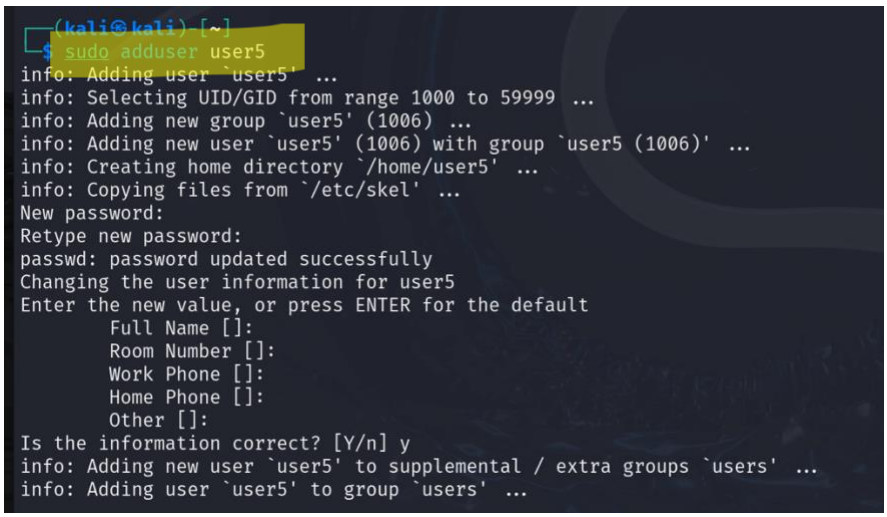
Screenshot:



5. For user5, the password should consist of a simple dictionary word (all lowercase) + digits.

Explanation: Password is orange123 and I used the same commands in step 1 but changing user1 to user5.

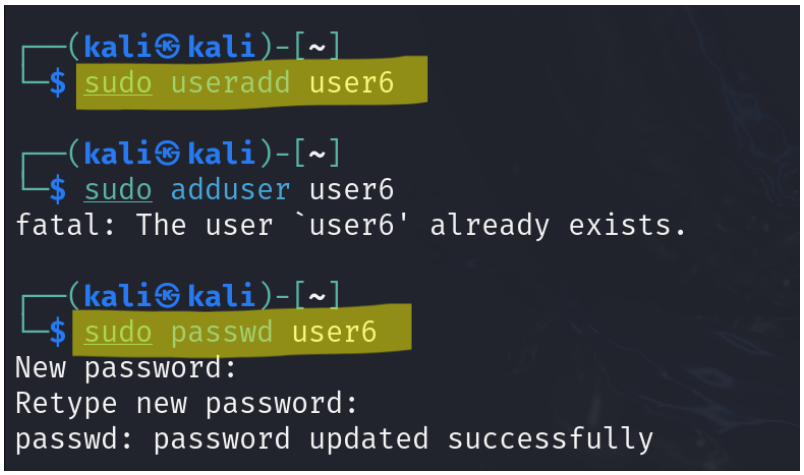
Screenshot:



6. For user6, the password should consist of a simple dictionary word (with a combination of lower and upper case) + digits + symbols.

Explanation: Password is Champ123! and I used the same commands in step 1 but changing user1 to user6. This is where I mess up and mistyped user6's password, I also used a different command **useradd** . I correct my mistake by using **sudo passwd** command followed by the user I want to edit. The command **sudo useradd** will add the user w/o letting me create a password and edit details right away. As seen in the previous steps.

Screenshot:



2. Export above users' hashes into a file named xxx.hash (replace xxx with your MIDAS name) and use John the Ripper tool to crack their passwords in wordlist mode (use rockyou.txt).

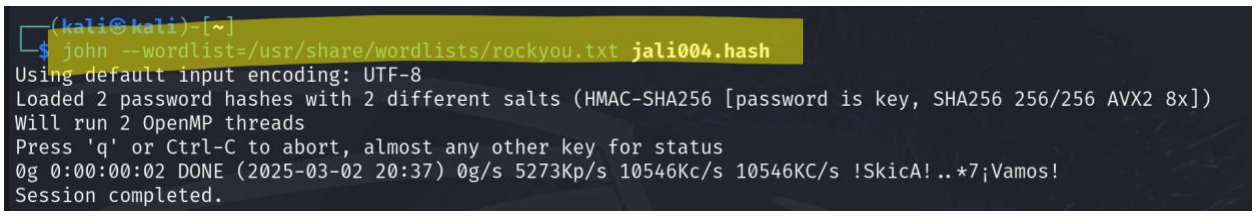
Explanation: To download rockyou.txt I use the following commands:

sudo apt update && sudo apt install wordlists -y

sudo gunzip /usr/share/wordlists/rockyou.txt.gz

john --wordlist=/usr/share/wordlists/rockyou.txt jali004.hash

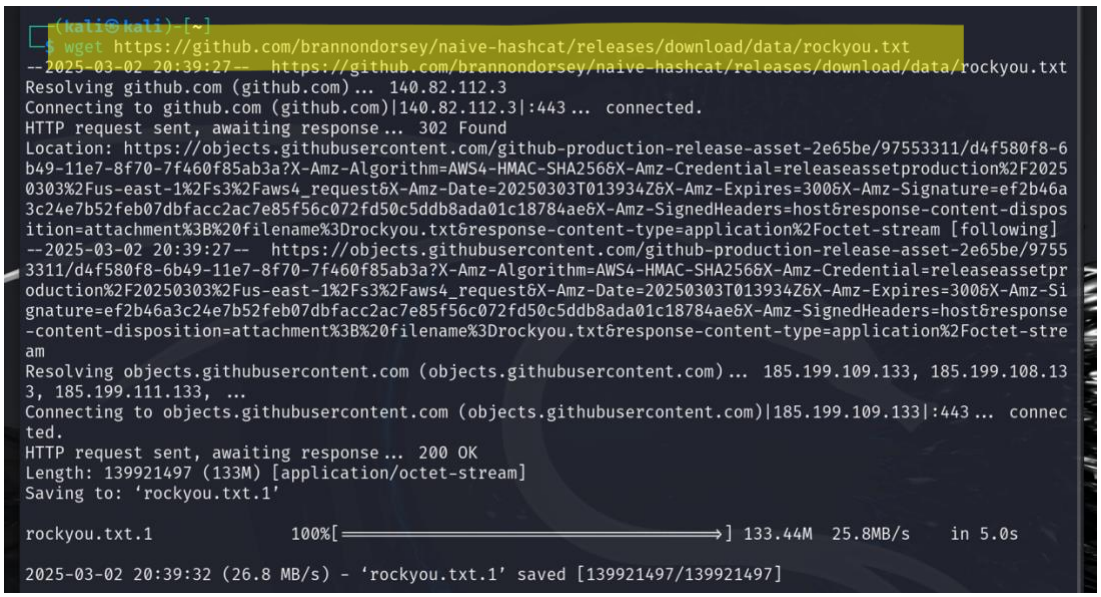
Screenshot:



Further Explanation: Also tried this way using command because why not:

wgethttps://github.com/brannondorsey/naïve-hashcat/releases/download/data/rockyou.txt

Screenshot:



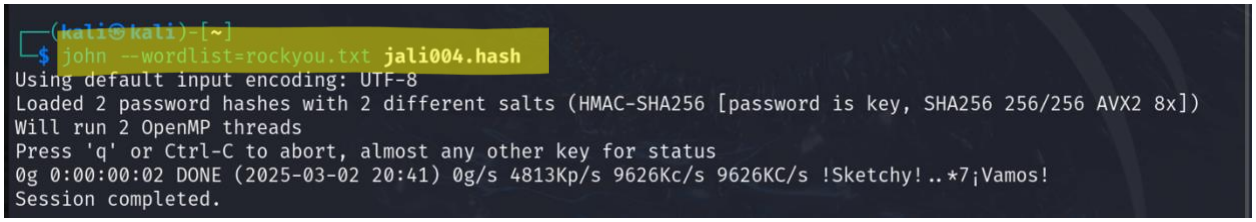
Further Explanation:

I then use the command **sudo grep** followed by what I'm trying to grab and where it is located and then defining where it is going, or to put another way… I am taking the passwords from a file and exporting them to another so I can manipulate this file.

Screenshot:

Further Explanation: I then use the **john** command and define what word list I will be using in what file. Notice the argument syntax, **john** what wordlist followed by file name.

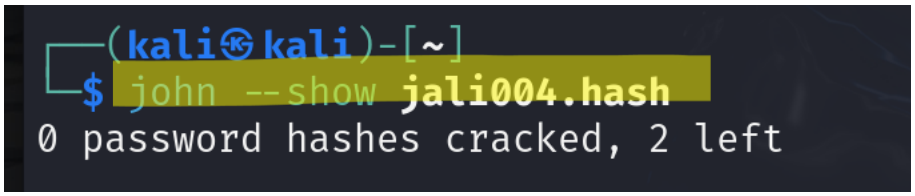
Screenshot:



3. Keep your john the ripper cracking for 10 minutes. How many passwords have been successfully cracked?

Explanation: My passwords were not in the wordlist file I downloaded, I was able to check this using the **cat** command and calling the word list file rock you to display. So it makes sense that 0 passwords were cracked and two were left. I use the command **john –show** followed by the file. So I can display the required information.

Screenshot:



Extra Credit on Next Page

1. Find and use the proper format in John the ripper to crack the following MD5 hash. Show your steps and results.

5f4dcc3b5aa765d61d8327deb882cf99
63a9f0ea7bb98050796b649e85481845

Explanation: I use the command **echo** to create a file containing the above MD5 hashes. I use the **cat** command followed by the file I created to verify I did this correctly. I then run **john** followed by the correct formatting of the hashes, followed by the wordlist I am using, followed by what file I need **john** to sift through. Once John has given me session complete I then complete the task with the command **john show** followed by the format because I want to be able to read it, and closing with what file I am looking in. The passwords are as follows:

password

root

Screenshot: