

Carl Lochstampfor

CYSE 270: Linux System for Cybersecurity

Assignment: Lab 5 – Cracking Passwords

June 22, 2025

Goal:

The goal of this lab is to test the strength of different passwords.

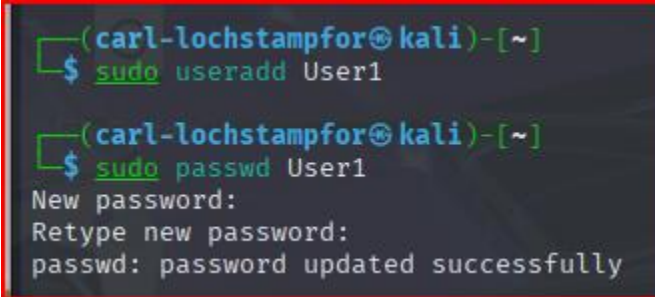
Submission Instructions:

1. Complete all tasks in **Task A** your chosen Ubuntu/Kali VM.
2. Take screenshots for each step as evidence of successful Command execution.
3. Save all your screenshots and results in a single PDF or Word document.
4. Ensure that all **Commands are executed** correctly for each step taken.

In this assignment, you should replace xxxxx (cloch001) with your MIDAS ID in all occurrences.

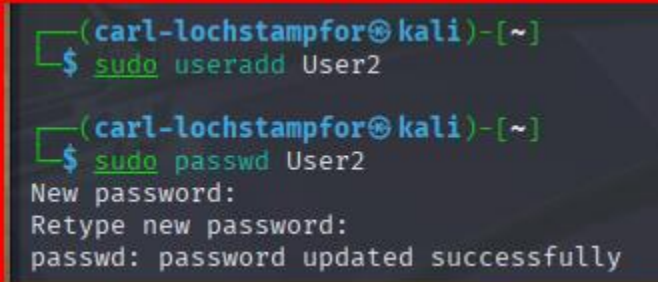
Task A — Password Cracking

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. [**6 * 5 = 30 points**].
 - a. For user1, the password should be a simple dictionary word (all lowercase)
 - i. User1: password



```
(carl-lochstampfor@kali)-[~]  
$ sudo useradd User1  
  
(carl-lochstampfor@kali)-[~]  
$ sudo passwd User1  
New password:  
Retype new password:  
passwd: password updated successfully
```

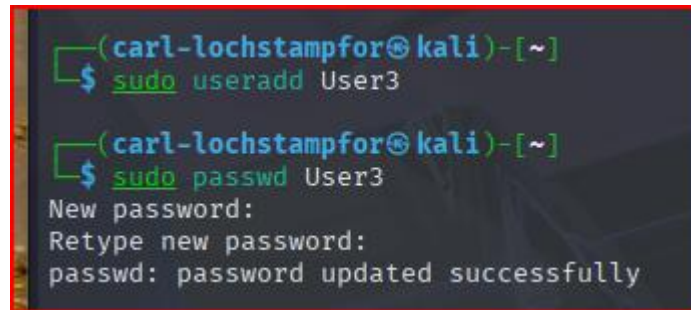
- b. For user2, the password should consist of 4 digits.
 - i. User2: 1234



```
(carl-lochstampfor@kali)-[~]  
$ sudo useradd User2  
  
(carl-lochstampfor@kali)-[~]  
$ sudo passwd User2  
New password:  
Retype new password:  
passwd: password updated successfully
```

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

i. User3: superman1234



```
(carl-lochstampfor@kali)~$ sudo useradd User3
(carl-lochstampfor@kali)~$ sudo passwd User3
New password:
Retype new password:
passwd: password updated successfully
```

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

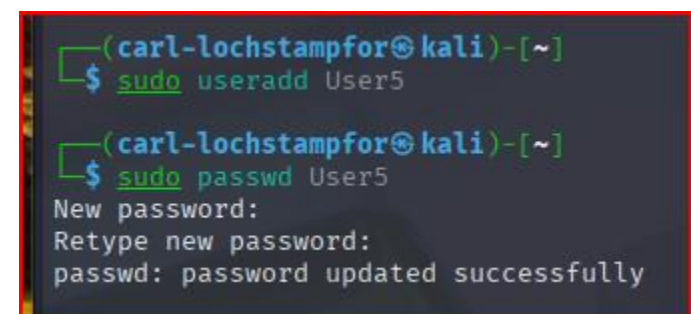
i. User4: password1234&*()



```
(carl-lochstampfor@kali)~$ sudo useradd User4
(carl-lochstampfor@kali)~$ sudo passwd User4
New password:
Retype new password:
passwd: password updated successfully
```

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

i. User5: password78910



```
(carl-lochstampfor@kali)~$ sudo useradd User5
(carl-lochstampfor@kali)~$ sudo passwd User5
New password:
Retype new password:
passwd: password updated successfully
```

- f. For user6, the password should consist of a simple dictionary word (with a combination of lower and upper case) + digits + symbols.
 i. User6: p4S\$W0r4!#

```
(carl-lochstampfor@kali)-[~]
$ sudo useradd User6

(carl-lochstampfor@kali)-[~]
$ sudo passwd User6
New password:
Retype new password:
passwd: password updated successfully
```

Remember, do not use the passwords for your real-world accounts.

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). [40 points]

Exported only the six specific users to a separate file, cloch001.hash.

Command >>

sudo grep -E 'User1| User2| User3| User4| User5| User6' /etc/shadow > cloch001.hash

```
(carl-lochstampfor@kali)-[~]
$ sudo grep -E 'User1|User2|User3|User4|User5|User6' /etc/shadow > cloch001.hash

(carl-lochstampfor@kali)-[~]
$ ls -l
total 136704
-rw-rw-r-- 1 carl-lochstampfor carl-lochstampfor 594 Jun 19 13:06 cloch001.hash
drwxrwxr-x 2 carl-lochstampfor carl-lochstampfor 4096 Jun 7 10:16 cyse270
drwxrwxr-x 2 carl-lochstampfor carl-lochstampfor 4096 Jun 6 12:28 data
drwxr-xr-x 2 carl-lochstampfor carl-lochstampfor 4096 May 21 18:56 Desktop
drwxr-xr-x 2 carl-lochstampfor carl-lochstampfor 4096 May 21 18:56 Documents
drwxr-xr-x 2 carl-lochstampfor carl-lochstampfor 4096 May 21 18:56 Downloads
-rw-rw-r-- 1 carl-lochstampfor games 0 Jun 10 09:46 fruit.txt
drwxr-xr-x 2 carl-lochstampfor carl-lochstampfor 4096 May 21 18:56 Music
-rw-rw-r-- 1 carl-lochstampfor carl-lochstampfor 47 Jun 6 16:06 notes.txt
drwxr-xr-x 2 carl-lochstampfor carl-lochstampfor 4096 May 21 18:56 Pictures
drwxr-xr-x 2 carl-lochstampfor carl-lochstampfor 4096 May 21 18:56 Public
-rw-r--r-- 1 carl-lochstampfor carl-lochstampfor 139921507 Jun 19 12:58 rockyou.txt
-rw-r----- 1 root root 2004 Jun 19 13:01 shadow
drwxr-xr-x 2 carl-lochstampfor carl-lochstampfor 4096 May 21 18:56 Templates
-rw-rw-r-- 1 carl-lochstampfor carl-lochstampfor 2004 Jun 19 12:59 test.txt
drwxr-xr-x 2 carl-lochstampfor carl-lochstampfor 4096 May 21 18:56 Videos

(carl-lochstampfor@kali)-[~]
$ cat cloch001.hash
User1:$y$j9T$n2z0L/4qsZDdV6gcScPz01$.U1EHDkmfzW5galaLLKdmmOyqiVEvX6dVy4rIjo0JA.:20258:0:99999:7:::
User2:$y$j9T$GaDxafHkipMN1BNCTdqY/1$ZntEuV.YNPv9PJFLIjnl1JkUM/p4isAYA92ZMG5.vz1:20258:0:99999:7:::
User3:$y$j9T$5uvLf/cDR2NzcYiKp3RYg.$yAwz54wRaRWktexqrbIzDcw9iZmt.MJ3r8ZWtBBlqrD:20258:0:99999:7:::
User4:$y$j9T$ouHXMubfvK4l8q29XN/5m/$IpuXtHJpdd0UA9bTbNr0H9TyBOXFM/PEaQ6zjQ06T5.:20258:0:99999:7:::
User5:$y$j9T$06SjuzsGfMSSQuWvLZ/2t1$mi1bvvyvU0TJVluIlg.Hi4z3/aja04qs4sXxcF6G2sb1:20258:0:99999:7:::
User6:$y$j9T$stBB8yWDLjGF7/VbF1Pz/.$8hUyBP3vGS94oMSC3z6TW/AnVWBP5GB/QFnqEm..o0A:20258:0:99999:7:::
```

Started Running Jack the Ripper tool to crack the passwords

Command >>

```
sudo timeout 10m john --format=crypt cloch001.hash --wordlist=/home/carl-lochstampfor/rockyou.txt
```

```
(carl-lochstampfor@kali)-[~]
$ sudo timeout 10m john --format=crypt cloch001.hash --wordlist=/home/carl-lochstampfor/rockyou.txt
Using default input encoding: UTF-8
Loaded 6 password hashes with 6 different salts (crypt, generic crypt(3) [?/64])
Cost 1 (algorithm [1:descrypt 2:md5crypt 3:sunmd5 4:bcrypt 5:sha256crypt 6:sha512crypt]) is 0 for all loaded hashes
Cost 2 (algorithm specific iterations) is 1 for all loaded hashes
Press Ctrl-C to abort, or send SIGUSR1 to john process for status
password      (User1)
```

3. Keep your john the ripper cracking for 10 minutes. How many passwords have been successfully cracked? **[30 points]**

Only two passwords were cracked: **User1** and **User1**.

```
(carl-lochstampfor@kali)-[~]
$ sudo timeout 10m john --format=crypt cloch001.hash --wordlist=/home/carl-lochstampfor/rockyou.txt
Using default input encoding: UTF-8
Loaded 6 password hashes with 6 different salts (crypt, generic crypt(3) [?/64])
Cost 1 (algorithm [1:descrypt 2:md5crypt 3:sunmd5 4:bcrypt 5:sha256crypt 6:sha512crypt]) is 0 for all loaded hashes
Cost 2 (algorithm specific iterations) is 1 for all loaded hashes
Press Ctrl-C to abort, or send SIGUSR1 to john process for status
password      (User1) ✖
1234          (User2)
2g 0:00:10:00 0.12% (ETA: 2025-06-25 10:45) 0.003330g/s 33.73p/s 137.4c/s 137.4C/s kirsten1..ailyn
Use the "--show" option to display all of the cracked passwords reliably
Session aborted
```

Extra credit (10 points)

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

Step 1: Printed the hashes to the terminal and wrote/exported them into a new file called **md5hashes.txt**. Then confirmed the hashes were saved in the file.

- a. Hashes:
 - i. 5f4dcc3b5aa765d61d8327deb882cf99
 - ii. 63a9f0ea7bb98050796b649e85481845
- b. Command >> **echo "5f4dcc3b5aa765d61d8327deb882cf99" > md5hashes.txt**
- c. Command >> **echo "63a9f0ea7bb98050796b649e85481845" >> md5hashes.txt**

```
(carl-lochstampfor@kali)-[~]  
$ echo "5f4dcc3b5aa765d61d8327deb882cf99" > md5hashes.txt  
dquote>  
  
(carl-lochstampfor@kali)-[~]  
$ echo "5f4dcc3b5aa765d61d8327deb882cf99" > md5hashes.txt
```

```
(carl-lochstampfor@kali)-[~]  
$ cat md5hashes.txt  
5f4dcc3b5aa765d61d8327deb882cf99  
  
(carl-lochstampfor@kali)-[~]  
$ echo "63a9f0ea7bb98050796b649e85481845" >> md5hashes.txt
```


Command >> **ls -l** (displays the file was created)

```
(carl-lochstampfor@kali)-[~]
$ ls -l
total 136708
-rw-rw-r-- 1 carl-lochstampfor carl-lochstampfor 594 Jun 19 13:06 cloch001.hash
drwxrwxr-x 2 carl-lochstampfor carl-lochstampfor 4096 Jun 7 10:16 cyse270
drwxrwxr-x 2 carl-lochstampfor carl-lochstampfor 4096 Jun 6 12:28 data
drwxr-xr-x 2 carl-lochstampfor carl-lochstampfor 4096 May 21 18:56 Desktop
drwxr-xr-x 2 carl-lochstampfor carl-lochstampfor 4096 May 21 18:56 Documents
drwxr-xr-x 2 carl-lochstampfor carl-lochstampfor 4096 May 21 18:56 Downloads
-rw-rw-r-- 1 carl-lochstampfor games 0 Jun 10 09:46 fruit.txt
-rw-rw-r-- 1 carl-lochstampfor carl-lochstampfor 66 Jun 19 13:43 md5hashes.txt
drwxr-xr-x 2 carl-lochstampfor carl-lochstampfor 4096 May 21 18:56 Music
-rw-rw-r-- 1 carl-lochstampfor carl-lochstampfor 47 Jun 6 16:06 notes.txt
drwxr-xr-x 2 carl-lochstampfor carl-lochstampfor 4096 May 21 18:56 Pictures
drwxr-xr-x 2 carl-lochstampfor carl-lochstampfor 4096 May 21 18:56 Public
-rw-r--r-- 1 carl-lochstampfor carl-lochstampfor 139921507 Jun 19 12:58 rockyou.txt
-rw-r----- 1 root root 2004 Jun 19 13:01 shadow
drwxr-xr-x 2 carl-lochstampfor carl-lochstampfor 4096 May 21 18:56 Templates
-rw-rw-r-- 1 carl-lochstampfor carl-lochstampfor 2004 Jun 19 12:59 test.txt
drwxr-xr-x 2 carl-lochstampfor carl-lochstampfor 4096 May 21 18:56 Videos
```

Command >> **cat md5hashes.txt** (displays the contents of the file, which are the hashes)

```
(carl-lochstampfor@kali)-[~]
$ cat md5hashes.txt
5f4dcc3b5aa765d61d8327deb882cf99
63a9f0ea7bb98050796b649e85481845
```

Step 2: Run the proper format of John the Ripper to crack the above MD5 hashes (readded the 10-minute timeout as a preference).

- d. Command >> **sudo timeout 10m john --format=raw-md5 md5hashes.txt --wordlist=/home/carl-lochstampfor/rockyou.txt**
 - i. The difference between the first test with Jack and this second test is the format changing from **'format=crypt'** to **'format=raw-md5'**.
- e. Results: Jack the Ripper cracked the hashes almost instantaneously. The hashes were **'password'** and **'root'**.

```
(carl-lochstampfor@kali)-[~]
$ sudo timeout 10m john --format=raw-md5 md5hashes.txt --wordlist=/home/carl-lochstampfor/rockyou.txt
[sudo] password for carl-lochstampfor:
Using default input encoding: UTF-8
Loaded 2 password hashes with no different salts (Raw-MD5 [MD5 128/128 SSE2 4x3])
Press Ctrl-C to abort, or send SIGUSR1 to john process for status
password (7)
root (7)
2g 0:00:00:00 DONE (2025-06-19 13:57) 50.00g/s 20174Kp/s 20174Kc/s 20179Kc/s rory17..ronron2008
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed.
```