Frederick Gervacio

CYSE 270-17496: Linux System for Cybersecurity

Assignment 5

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

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].

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

a) bookcase

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

a) 6789

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

a) hotel1234

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

a) @pple12345

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

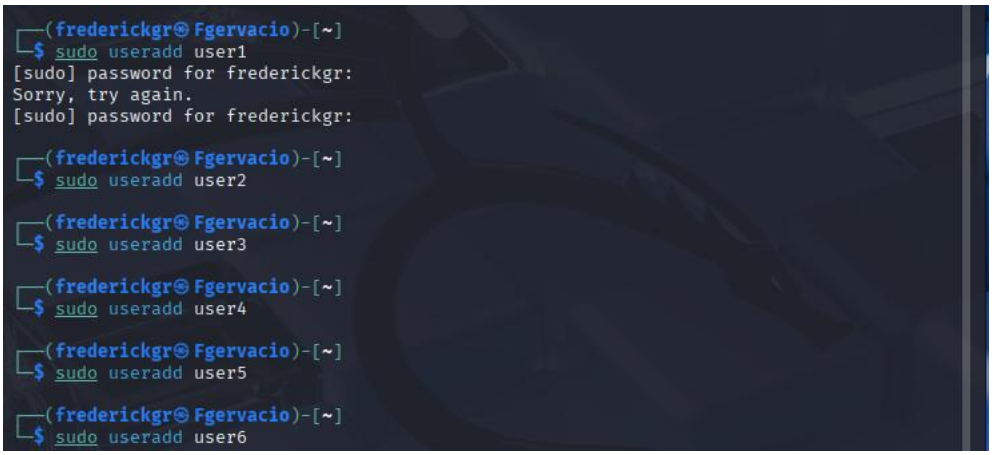
a) dictionary012345

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

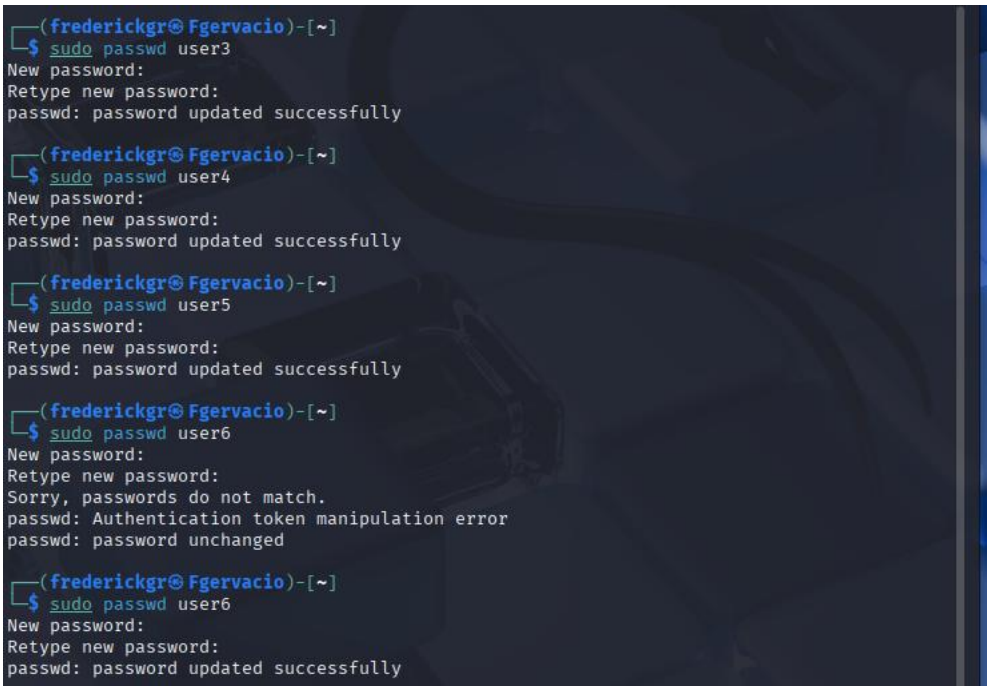
a) P@ssw0rd987654

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

I created the accounts using the command "sudo useradd (account name)"



Then assigned the password using the command "sudo password (username)"



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 the file using the command "sudo cat /etc/shadow | grep 'user[1-6]' and named it fgerv001.hash

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

```
┌──(frederickgr㉿Fgervacio)-[~]
└─$ sudo john --format=crypt fgerv001.hash --wordlist=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
Will run 8 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:51 0.02% (ETA: 2025-10-10 01:13) 0g/s 56.28p/s 341.4c/s 341.4C/s skater1..147
89632
0g 0:00:47:47 0.92% (ETA: 2025-10-10 02:37) 0g/s 54.84p/s 329.2c/s 329.2C/s muddy..monal
issa
0g 0:00:47:58 0.93% (ETA: 2025-10-10 02:31) 0g/s 54.90p/s 329.5c/s 329.5C/s love1020..li
vier
0g 0:00:49:31 0.96% (ETA: 2025-10-10 01:58) 0g/s 55.22p/s 331.4c/s 331.4C/s 1trumpet..19
861988
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.

a. 5f4dcc3b5aa765d61d8327deb882cf99

b. 63a9f0ea7bb98050796b649e85481845

```
┌──(frederickgr㉿Fgervacio)-[~]
└─$ sudo john --format=raw-md5 --wordlist=~/rockyou.txt extracredit1.txt
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-MD5 [MD5 256/256 AVX2 8×3])
Warning: no OpenMP support for this hash type, consider --fork=8
Press 'q' or Ctrl-C to abort, almost any other key for status
password         (?)
1g 0:00:00:00 DONE (2025-10-06 13:26) 25.00g/s 9600p/s 9600c/s 9600C/s 123456..michael1
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliab
ly
Session completed.

┌──(frederickgr㉿Fgervacio)-[~]
└─$ sudo john --format=raw-md5 --wordlist=~/rockyou.txt extracredit2.txt
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-MD5 [MD5 256/256 AVX2 8×3])
Warning: no OpenMP support for this hash type, consider --fork=8
Press 'q' or Ctrl-C to abort, almost any other key for status
root             (?)
1g 0:00:00:00 DONE (2025-10-06 13:27) 10.00g/s 8071Kp/s 8071Kc/s 8071KC/s rory17..ronald
918
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliab
ly
Session completed.

┌──(frederickgr㉿Fgervacio)-[~]
└─$ sudo john --show extracredit1.txt
0 password hashes cracked, 2 left

┌──(frederickgr㉿Fgervacio)-[~]
└─$ sudo john --show --format=Raw-MD5
Password files required, but none specified

┌──(frederickgr㉿Fgervacio)-[~]
└─$ sudo john --show --format=Raw-MD5 extracredit1.txt
?:password

1 password hash cracked, 0 left

┌──(frederickgr㉿Fgervacio)-[~]
└─$ sudo john --show --format=Raw-MD5 extracredit2.txt
?:root

1 password hash cracked, 0 left

┌──(frederickgr㉿Fgervacio)-[~]
└─$
```

I used the step above to complete the crack of the hash and had to use the “sudo john –-show –-format=Raw-MD5 (filename) command to see if the crack was completed successfully.