Jasmyn Wilhelm 11 October 2024

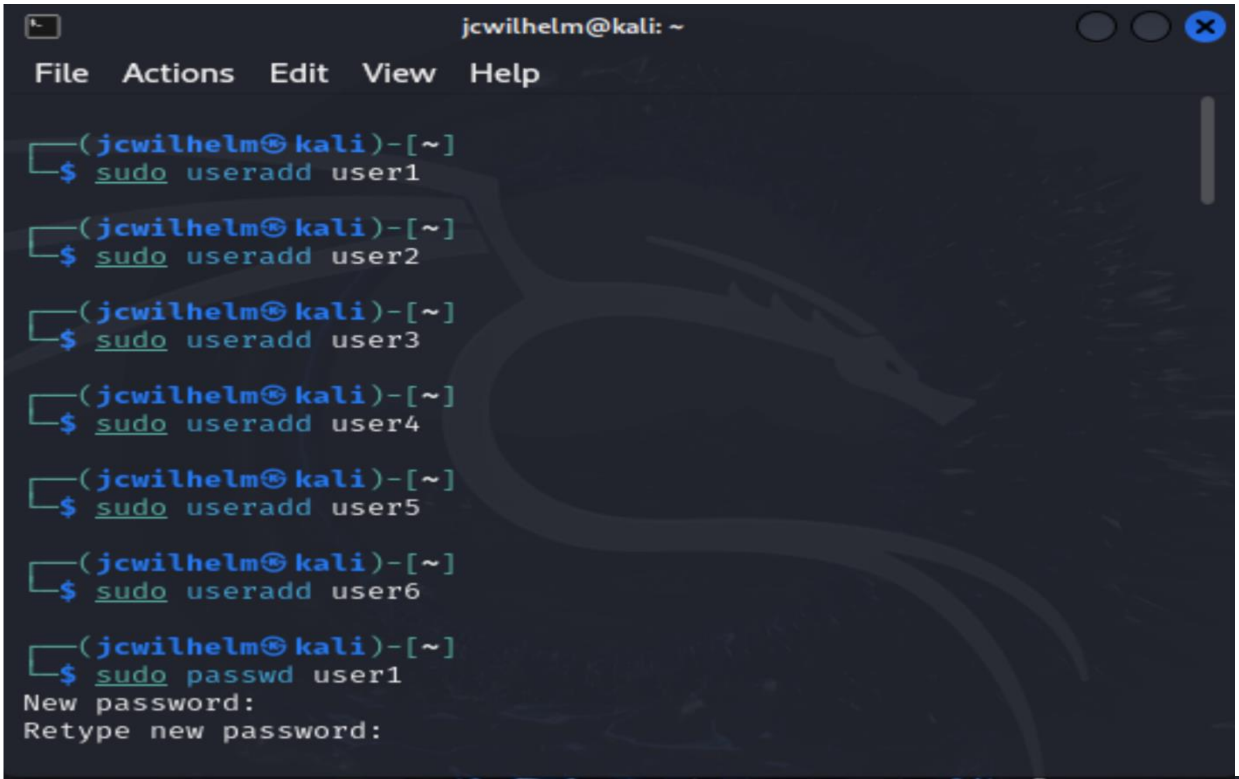
CYSE 270: Linux System for Cybersecurity

CYSE 270: Linux System for Cybersecurity

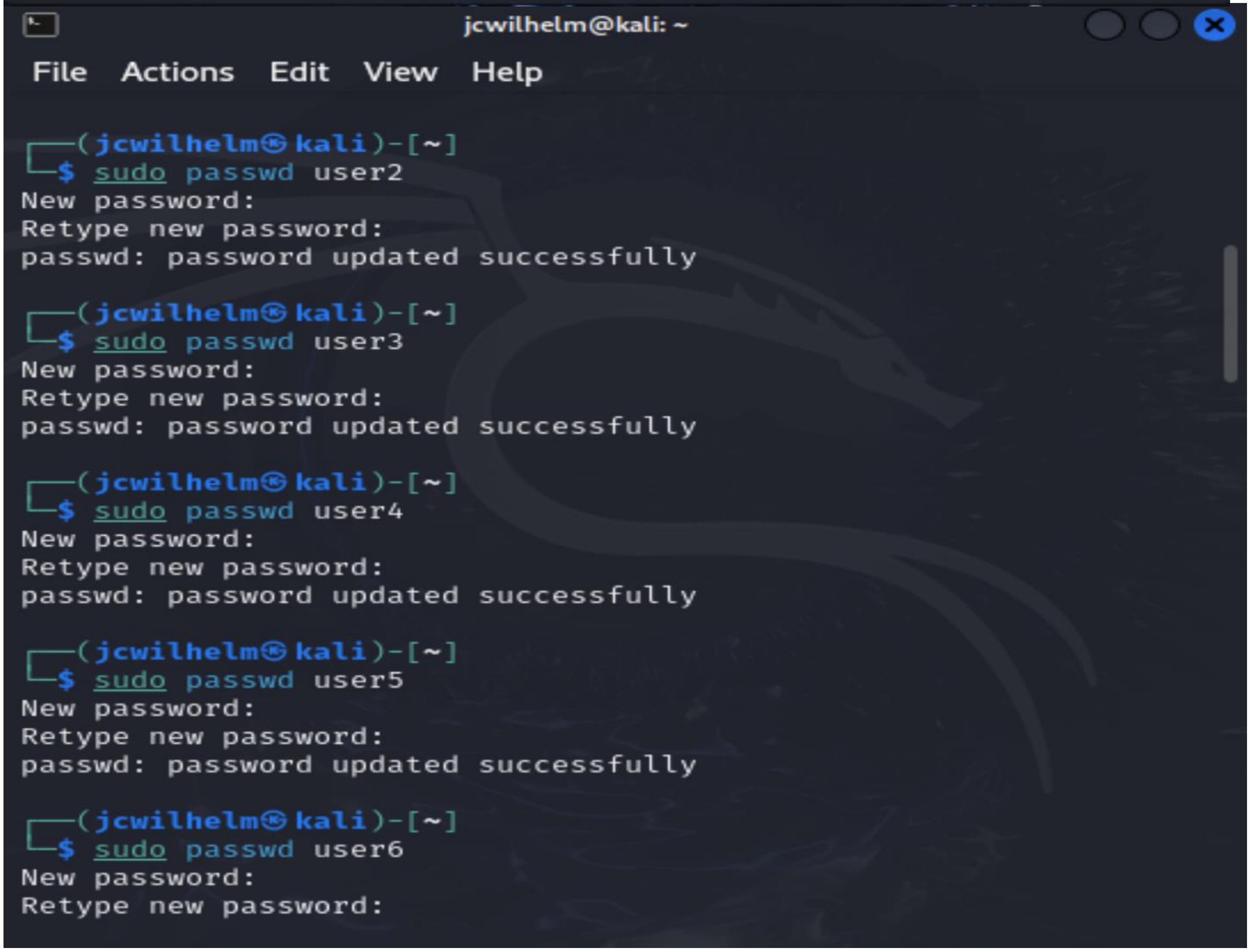
The goal of this lab is to test the strength of different passwords.

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)
        i password
    2. For user2, the password should consist of 4 digits.
        i 123456
    3. For user3, the password should consist of a simple dictionary word of any length characters (all lowercase) + digits.
        i password1234
    4. For user4, the password should consist of a simple dictionary word characters (all lowercase) + digits + symbols.
        i p@ssword1234
    5. For user5, the password should consist of a simple dictionary word (all lowercase) + digits.
        i 9a55w0rd
    6. For user6, the password should consist of a simple dictionary word (with a combination of lower and upper case) + digits + symbols.
        i #P@ssw0rd



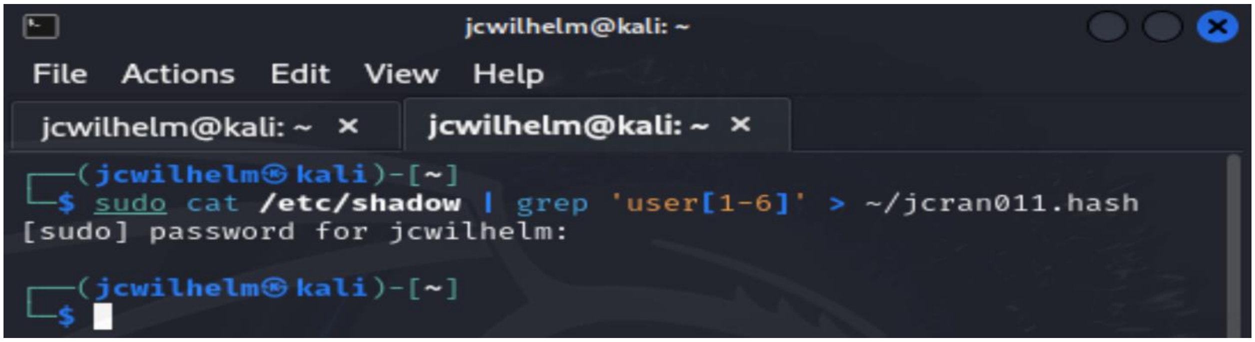
```
┌──(jcwilhelm㉿kali)-[~]
└─$ sudo useradd user1

┌──(jcwilhelm㉿kali)-[~]
└─$ sudo useradd user2

┌──(jcwilhelm㉿kali)-[~]
└─$ sudo useradd user3

┌──(jcwilhelm㉿kali)-[~]
└─$ sudo useradd user4

┌──(jcwilhelm㉿kali)-[~]
└─$ sudo useradd user5

┌──(jcwilhelm㉿kali)-[~]
└─$ sudo useradd user6

┌──(jcwilhelm㉿kali)-[~]
└─$ sudo passwd user1
New password:
Retype new password:
```



```
┌──(jcwilhelm㉿kali)-[~]
└─$ sudo passwd user2
New password:
Retype new password:
passwd: password updated successfully

┌──(jcwilhelm㉿kali)-[~]
└─$ sudo passwd user3
New password:
Retype new password:
passwd: password updated successfully

┌──(jcwilhelm㉿kali)-[~]
└─$ sudo passwd user4
New password:
Retype new password:
passwd: password updated successfully

┌──(jcwilhelm㉿kali)-[~]
└─$ sudo passwd user5
New password:
Retype new password:
passwd: password updated successfully

┌──(jcwilhelm㉿kali)-[~]
└─$ sudo passwd user6
New password:
Retype new password:
```

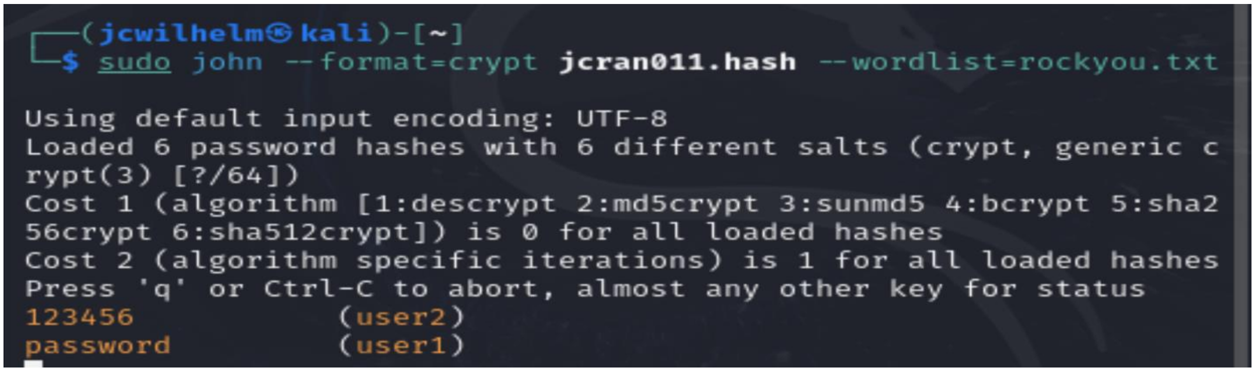
Remember, do not use the passwords for your real-world accounts.

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]**

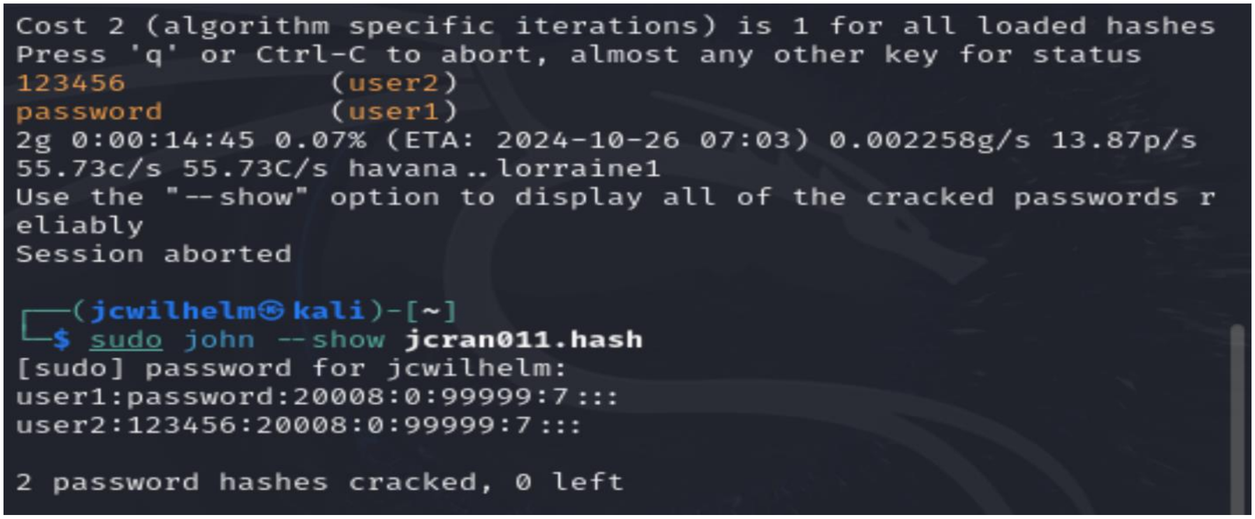


```
┌──(jcwilhelm㉿kali)-[~]
└─$ sudo cat /etc/shadow | grep 'user[1-6]' > ~/jcran011.hash
[sudo] password for jcwilhelm:

┌──(jcwilhelm㉿kali)-[~]
└─$ █
```

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



```
┌──(jcwilhelm㉿kali)-[~]
└─$ sudo john --format=crypt jcran011.hash --wordlist=rockyou.txt

Using default input encoding: UTF-8
Loaded 6 password hashes with 6 different salts (crypt, generic c
rypt(3) [?/64])
Cost 1 (algorithm [1:descrypt 2:md5crypt 3:sunmd5 4:bcrypt 5:sha2
56crypt 6:sha512crypt]) is 0 for all loaded hashes
Cost 2 (algorithm specific iterations) is 1 for all loaded hashes
Press 'q' or Ctrl-C to abort, almost any other key for status
123456           (user2)
password         (user1)
```



```
Cost 2 (algorithm specific iterations) is 1 for all loaded hashes
Press 'q' or Ctrl-C to abort, almost any other key for status
123456           (user2)
password         (user1)
2g 0:00:14:45 0.07% (ETA: 2024-10-26 07:03) 0.002258g/s 13.87p/s
55.73c/s 55.73C/s havana..lorraine1
Use the "--show" option to display all of the cracked passwords r
eliably
Session aborted

┌──(jcwilhelm㉿kali)-[~]
└─$ sudo john --show jcran011.hash
[sudo] password for jcwilhelm:
user1:password:20008:0:99999:7:::
user2:123456:20008:0:99999:7:::

2 password hashes cracked, 0 left
```

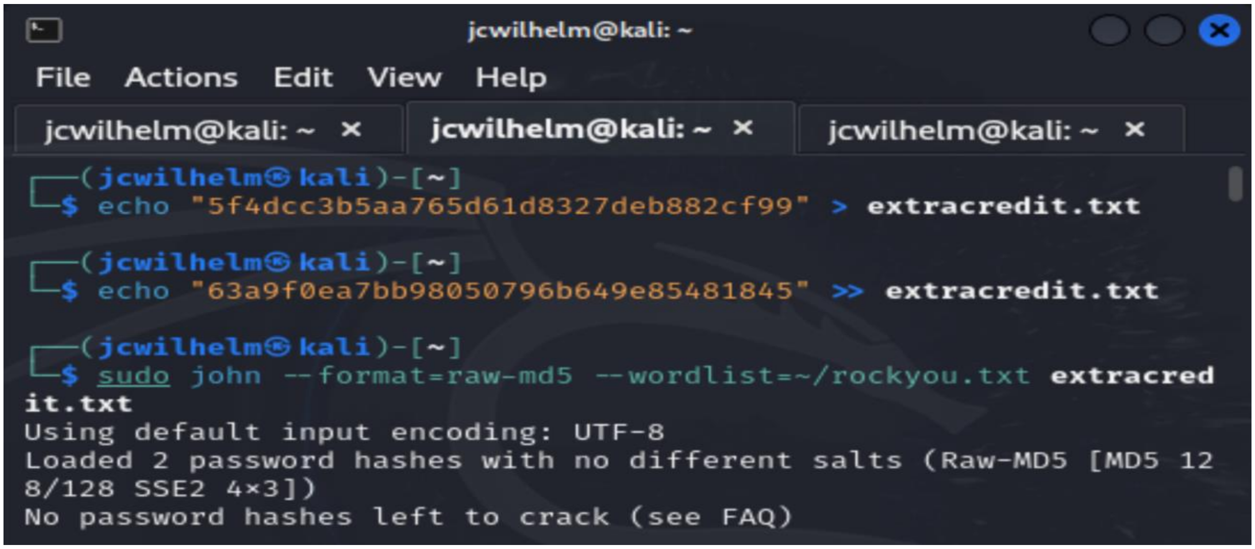
After 10 minutes, only users 1 & 2 were cracked.

Jasmyn Wilhelm 11 October 2024

CYSE 270: Linux System for Cybersecurity

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



```
┌──(jcwilhelm㉿kali)-[~]
└─$ echo "5f4dcc3b5aa765d61d8327deb882cf99" > extracredit.txt

┌──(jcwilhelm㉿kali)-[~]
└─$ echo "63a9f0ea7bb98050796b649e85481845" >> extracredit.txt

┌──(jcwilhelm㉿kali)-[~]
└─$ sudo john --format=raw-md5 --wordlist=~/rockyou.txt extracred
it.txt
Using default input encoding: UTF-8
Loaded 2 password hashes with no different salts (Raw-MD5 [MD5 12
8/128 SSE2 4×3])
No password hashes left to crack (see FAQ)
```

I was unable to crack the hashes, but these were the steps taken to attempt to do so.