CYSE 270: Linux System for Cybersecurity

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

Task A – Password Cracking

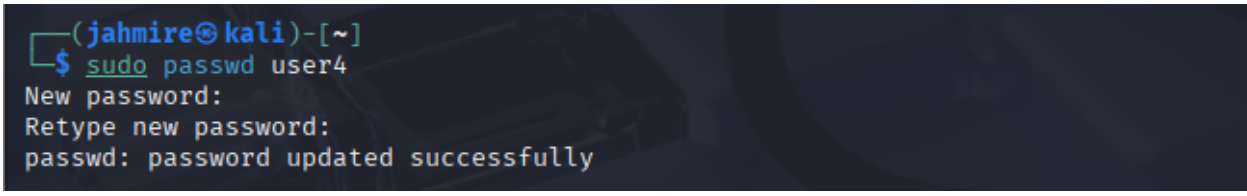
1. Create 6 users in your Linux Terminal, then set the password for each user that meets the following complexity requirement respectively. You should list the passwords created for each user. [6 * 5 = 30 points].
    a. For user1, the password should be a simple dictionary word (all lowercase)
    house

    b. For user2, the password should consist of 4 digits.
    1234

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

    house1234

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



    house1234@!

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

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

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

horns3892

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

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

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

HornS3892@!

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

2 passwords were successfully cracked.

```
┌──(jahmire㉿kali)-[~]
└─$ sudo john --format=crypt test.txt --wordlist=/home/jahmire/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 'q' or Ctrl-C to abort, almost any other key for status
1234             (user2)
house            (user1)
2g 0:00:13:59 0.09% (ETA: 2025-10-12 03:50) 0.002382g/s 18.98p/s 84.74c/s 84.74C/s 140290..jordie
Use the "--show" option to display all of the cracked passwords reliably
Session aborted
```

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