CYSE 270: Linux System for Cybersecurity

Assignment: Lab 5 – Password cracking

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) user1 = apple

```
┌──(pmacm001㉿kali-270)-[~]
└─$ sudo useradd user1
[sudo] password for pmacm001:
```

```
┌──(pmacm001㉿kali-270)-[~]
└─$ sudo passwd user1
New password:
Retype new password:
passwd: password updated successfully
```

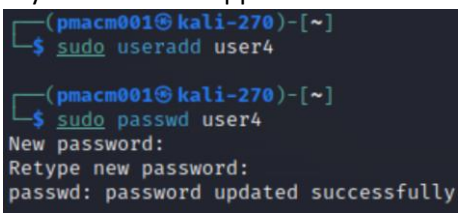
2. For user2, the password should consist of 4-character digits user2= 1998

```
┌──(pmacm001㉿kali-270)-[~]
└─$ sudo useradd user2

┌──(pmacm001㉿kali-270)-[~]
└─$ sudo passwd user2
New password:
Retype new password:
passwd: password updated successfully
```

3. For user3, the password should consist of a simple dictionary word of any length (all lowercase) + digits user3= apple98

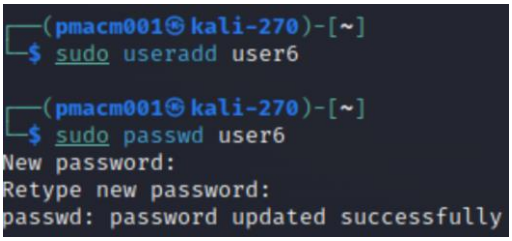
```
┌──(pmacm001㉿kali-270)-[~]
└─$ sudo useradd user3

┌──(pmacm001㉿kali-270)-[~]
└─$ sudo passwd user3
New password:
Retype new password:
passwd: password updated successfully
```

4. For user4, the password should consist of a simple dictionary word (all lowercase) + digits +symbols user4= apple14!



5. For user5, the password should consist of a simple dictionary word (all lowercase) + digits user5 = apple14

6. For user6, the password should consist of a simple dictionary word (with a combination of lower and upper case) + digits +symbols user6= Apple14!



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) 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]

```
┌──(pmacm001㉿kali-270)-[~]
└─$ sudo tail -6 /etc/shadow > pmacm001.hash
[sudo] password for pmacm001:

┌──(pmacm001㉿kali-270)-[~]
└─$ cat pmacm001.hash
user1:$y$j9T$Uf81YJgJMfhmkdfWMSZee1$L2PdulonlEmSBip25UEzv8sU/25nf2//5Z5NR5hvYo3:196
27:0:99999:7:::
user2:$y$j9T$B0PtlCdRxMYL8tQx3GoxF.$tmsB5I.3FQ7IjppjA8jKGp1SOtyoQBTnv0LnoET5n/C:196
27:0:99999:7:::
user3:$y$j9T$gxbLXMMVtheGTLpsD3ADJ0$TeqIn8SK2sC.8qv/uKbGGD3BImyw9UmiTeQr5IL4dD4:196
27:0:99999:7:::
user4:$y$j9T$dcbqZhrHm0VOit0h4ymk9/$L9CyOtFgApb7jnE4gYB9PVuvV1qNEec5zvYZQ8NWzx3:196
27:0:99999:7:::
user5:$y$j9T$QGalELQ06PR4dYGaWB/5X1$1fHxZYskkjseWiHrb.w9seMyuXhB1CUrowVqlFU1QH0:196
27:0:99999:7:::
user6:$y$j9T$rMp8EwIgnQLkRAcxKUfCR1$VNloKxpTVDE91BUkvvPKFAasL/B0QoUfQ3fVewBJg81:196
27:0:99999:7:::
```

```
┌──(pmacm001㉿kali-270)-[~]
└─$ sudo john --format=crypt pmacm001.hash --wordlist=rockyou.txt
Using default input encoding: UTF-8
Loaded 6 password hashes with 6 different salts (crypt, generic crypt(3) [?/64])
Remaining 5 password hashes with 5 different salts
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
0g 0:00:01:18 0.01% (ETA: 2023-10-14 17:20) 0g/s 11.01p/s 55.05c/s 55.05C/s chichi..sandy
```

```
┌──(pmacm001㉿kali-270)-[~]
└─$ sudo john --show /etc/shadow
user1:apple:19627:0:99999:7:::

1 password hash cracked, 0 left
```

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.

- 5f4dcc3b5aa765d61d8327deb882cf99
- 63a9f0ea7bb98050796b649e85481845