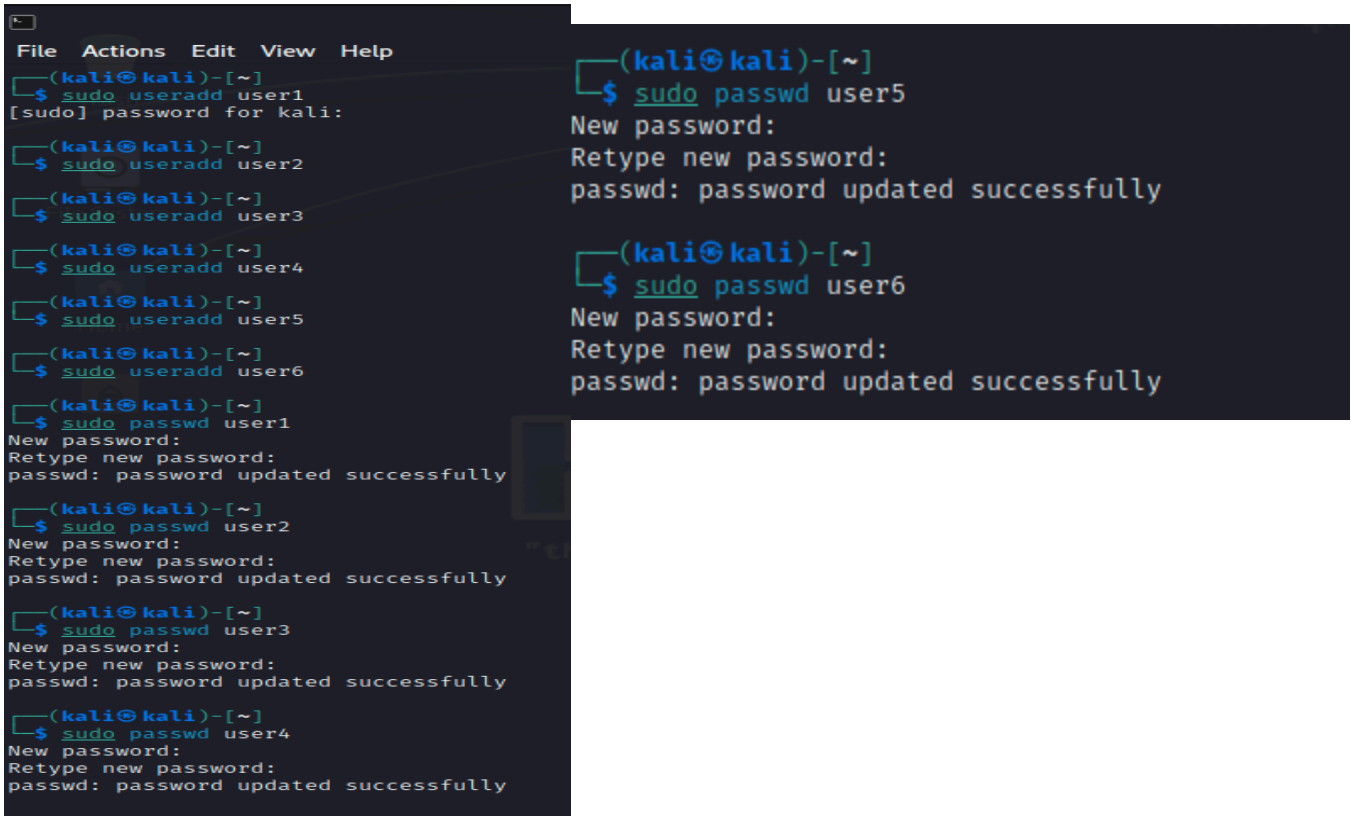
Zyron James M. Sumulong
CYSE 270
Assignment 5

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)
    Password: cyber
2. For user2, the password should consist of 4 digits.
    Password: 2498
3. For user3, the password should consist of a simple dictionary word of any length characters (all lowercase) + digits.
    Password: dominion26
4. For user4, the password should consist of a simple dictionary word characters (all lowercase) + digits + symbols.
    Password: old7!
5. For user5, the password should consist of a simple dictionary word (all lowercase) + digits.
    Password: university3
6. For user6, the password should consist of a simple dictionary word (with a combination of lower and upper case) + digits + symbols.
    Password: College1!

Commands:
- Sudo useradd xxx
- Sudo passwd



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]

Commands:

- sudo tail -n6 /etc/shadow (shows the last 6 lines of /etc/shadow which would be the hashes
- sudo tail -n6 /etc/shadow > zsumu001.hash (saved as a file called zsumu001.hash)
- Cat ~/zsumu001.hash (shows the contents of the file)

```
File  Actions  Edit  View  Help
┌──(kali㉿kali)-[~]
└─$ sudo tail -n6 /etc/shadow
user1:$y$j9T$03HGHE0UB2wHnHTqbhOKj0$60LqTZTTrNAMf5ZuUVkEdNW.5bqTsNBo/Wv943Hk9l7:20366:0:99999:7:::
user2:$y$j9T$ui/s4I7LztdhMTWKkRT.f1$tFRAcmrIJHIIOjrIr2Ara/jwTGw2ooZVuTPGgYkrlpC:20366:0:99999:7:::
user3:$y$j9T$eXIQnAZtvfUxrGYEOw8UX/$upQXMzVp/weJVLjRB5UKu6YmP2GwuObBnT9KASe5HfD:20366:0:99999:7:::
user4:$y$j9T$eLp0.1QXXpwZ7Hxb1nrQm1$h.DX2sj3pNiEfUYEsZzvWYPvhFVz20Tf2gMltu3Ozx.:20366:0:99999:7:::
user5:$y$j9T$weiUaZgsDaaEwaOqglCyi.$Z23SnJIm/tBUJWDETqkQdfvO8/VLsM4WQnj5aTJIZH7:20366:0:99999:7:::
user6:$y$j9T$DUzMTnUCddk8LoN7Hgqwl1$EQ4PsTjQ/jfW3xSwUH8Bjkad90HQv/0FYYCU.fiU./4:20366:0:99999:7:::

┌──(kali㉿kali)-[~]
└─$ sudo tail -n6 /etc/shadow > zsumu001.hash

┌──(kali㉿kali)-[~]
└─$ cat ~/zsumu001.hash
user1:$y$j9T$03HGHE0UB2wHnHTqbhOKj0$60LqTZTTrNAMf5ZuUVkEdNW.5bqTsNBo/Wv943Hk9l7:20366:0:99999:7:::
user2:$y$j9T$ui/s4I7LztdhMTWKkRT.f1$tFRAcmrIJHIIOjrIr2Ara/jwTGw2ooZVuTPGgYkrlpC:20366:0:99999:7:::
user3:$y$j9T$eXIQnAZtvfUxrGYEOw8UX/$upQXMzVp/weJVLjRB5UKu6YmP2GwuObBnT9KASe5HfD:20366:0:99999:7:::
user4:$y$j9T$eLp0.1QXXpwZ7Hxb1nrQm1$h.DX2sj3pNiEfUYEsZzvWYPvhFVz20Tf2gMltu3Ozx.:20366:0:99999:7:::
user5:$y$j9T$weiUaZgsDaaEwaOqglCyi.$Z23SnJIm/tBUJWDETqkQdfvO8/VLsM4WQnj5aTJIZH7:20366:0:99999:7:::
user6:$y$j9T$DUzMTnUCddk8LoN7Hgqwl1$EQ4PsTjQ/jfW3xSwUH8Bjkad90HQv/0FYYCU.fiU./4:20366:0:99999:7:::
```

3. Keep your john the ripper cracking for 10 minutes. How many passwords have been successfully cracked? [30 points]
1 password has been cracked and it was user1
Commands:

- cd/ /usr/share/wordlist (changed my current directory)
- Ls (list the files in the directory I am in, used to verify the rockyou.txt.gz was in)
- Sudo gunzip rockyou.txt.gz (unzips rockyou.txt.gz)
- Cp rockyou.txt ~ (copies file to my home directory)
- Cd (changes back to home folder)
- Ls (used to verify zsumu001.hash and rockyou.txt)
- John zsumu001.hash –wordlist=rockyou.txt (runs John the Ripper on the zsumu001.hash)
- John zsumu001.hash –format=crypt (Treats the hashes in file as crypt(3) format)

```
┌──(kali㉿kali)-[~]
└─$ cd /usr/share/wordlists/

┌──(kali㉿kali)-[/usr/share/wordlists]
└─$ ls
amass  dirb  dirbuster  fasttrack.txt  fern-wifi  john.lst  legion  metasploit  nmap.lst  rockyou.txt.gz  sqlmap.txt  wfuzz  wifite.txt

┌──(kali㉿kali)-[/usr/share/wordlists]
└─$ gunzip rockyou.txt.gz
gzip: rockyou.txt: Permission denied

┌──(kali㉿kali)-[/usr/share/wordlists]
└─$ sudo gunzip rockyou.txt.gz
```

```
┌──(kali㉿kali)-[/usr/share/wordlists]
└─$ cp rockyou.txt ~

┌──(kali㉿kali)-[/usr/share/wordlists]
└─$ cd

┌──(kali㉿kali)-[~]
└─$ ls
Desktop  Documents  Downloads  Music  Pictures  Public  Templates  Videos  copyright_cyse270  data  rockyou.txt  testfile  zsumu001.hash

┌──(kali㉿kali)-[~]
└─$ john zsumu001.hash --wordlist=rockyou.txt
Using default input encoding: UTF-8
No password hashes loaded (see FAQ)

┌──(kali㉿kali)-[~]
└─$ john zsumu001.hash --format=crypt
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
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
cyber            (user1)
```