Assignment: Lab 5

Task A

Step 1: Create 6 users that meet the password complexity requirements

- 1.1: Execute "sudo useradd -m user1 && sudo passwd user1"

  User1 = dictionary (cracked)

- 1.2: Execute "sudo useradd -m user2 && sudo passwd use2"

  User2 = 1235 (cracked)

- 1.3: Execute "sudo useradd -m user3 && sudo passwd user3"

  User3 = dogs124

- 1.4: Execute "sudo useradd -m user4 && sudo passwd user4"

  User4 = cats78*!

- 1.5: Execute "sudo useradd -m user5 && sudo passwd user5"

  User5 = curtain27

- 1.6: Execute "sudo useradd -m user6 && sudo passwd user6"

  User6 = PiLl0w13*!

bburke@ubuntu-vm: ~

```
bburke@ubuntu-vm:~$ sudo useradd -m user1 && sudo passwd user1
New password:
BAD PASSWORD: The password fails the dictionary check - it is based on a dictionary word
Retype new password:
passwd: password updated successfully
bburke@ubuntu-vm:~$
bburke@ubuntu-vm:~$ sudo useradd -m user2 && sudo passwd user2
New password:
BAD PASSWORD: The password is shorter than 8 characters
Retype new password:
passwd: password updated successfully
bburke@ubuntu-vm:~$
bburke@ubuntu-vm:~$ sudo useradd -m user3 && sudo passwd user3
New password:
BAD PASSWORD: The password fails the dictionary check - it is based on a dictionary word
Retype new password:
passwd: password updated successfully
bburke@ubuntu-vm:~$
bburke@ubuntu-vm:~$ sudo useradd -m user4 && sudo passwd user4
New password:
BAD PASSWORD: The password is shorter than 8 characters
Retype new password:
passwd: password updated successfully
bburke@ubuntu-vm:~$
bburke@ubuntu-vm:~$ sudo useradd -m user5 && sudo passwd user5
New password:
BAD PASSWORD: The password fails the dictionary check - it is based on a dictionary word
Retype new password:
passwd: password updated successfully
bburke@ubuntu-vm:~$
bburke@ubuntu-vm:~$ sudo useradd -m user6 && sudo passwd user6
New password:
Retype new password:
passwd: password updated successfully
bburke@ubuntu-vm:~$
```

Step 1.1

Step 1.2

Step 1.3

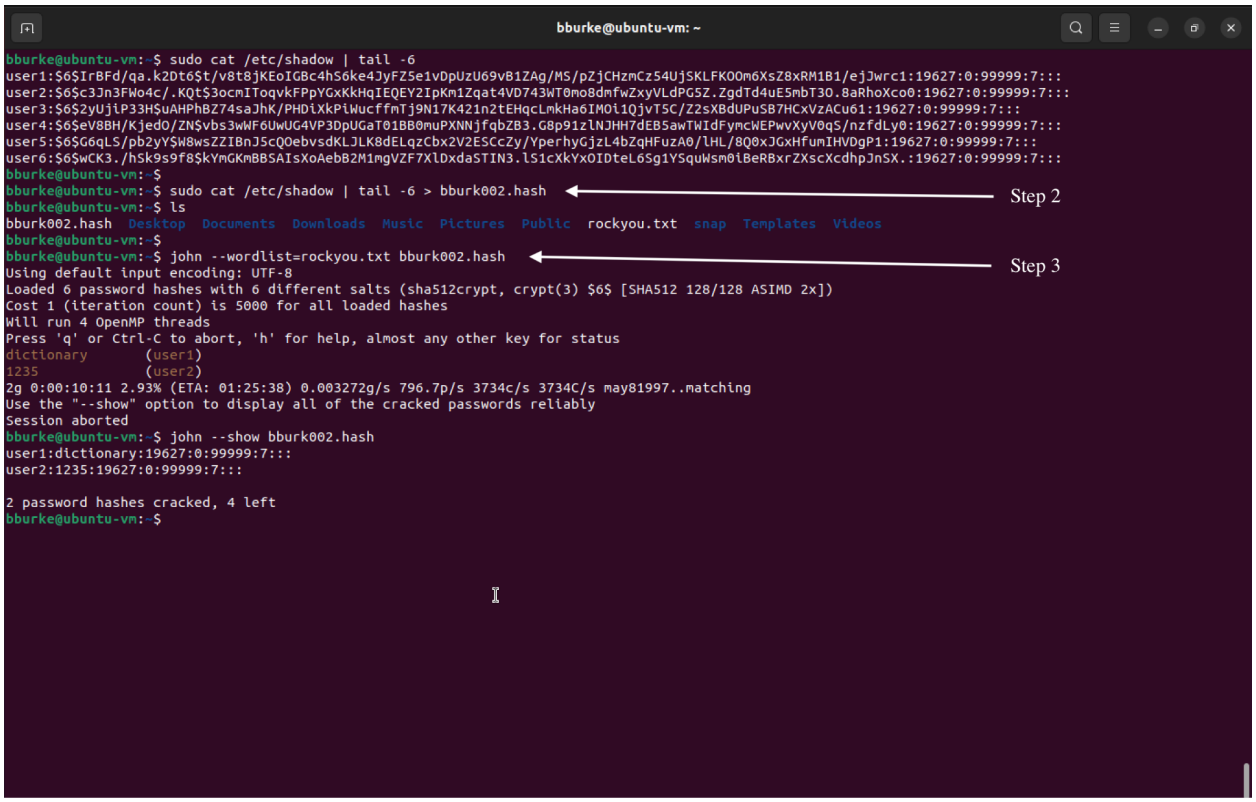
Step 1.4

Step 1.5

Step 1.6

Step 2: Export user hashes with “sudo cat /etc/shadow | tail -6 > bburk002.hash”

Step 3: Let john run for <u>10 minutes</u> with the command “john --wordlist=rockyou.txt bburk002.hash”. A total of 2 out of 6 passwords were cracked. User1’s password and User2’s password were cracked.



Extra Credit

Step 1: Use john to find the provided MD5 hashes. First, create a text file with vim called "md5_hashes.txt" with the hashes stored inside.

Step 2: Execute "john --format=raw-md5 --wordlist=rockyou.txt md5_hashes.txt"

Step 3: Execute "john --format=raw-md5 --show md5_hashes.txt" and get the following result:

5f4dcc3b5aa765d61d8327deb882cf99 = password

63a9f0ea7bb98050796b649e85481845 = root