

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 ← Step 1.1  
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 ← Step 1.2  
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 ← Step 1.3  
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 ← Step 1.4  
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 ← Step 1.5  
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 ← Step 1.6  
New password:  
Retype new password:  
passwd: password updated successfully  
bburke@ubuntu-vm:~$
```

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

Step 3: Let john run for 10 minutes 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.

```
bburke@ubuntu-vm: ~  
bburke@ubuntu-vm:~$ sudo cat /etc/shadow | tail -6  
user1:$6$IrBFd/qa.k2Dt6$t/v8t8jKEoIG8c4hS6ke4JyFZ5e1vDpUzU69vB1ZAg/HS/pZjCHzmCz54UjSKLFK00m6XsZ8xRM1B1/ejJwrc1:19627:0:99999:7:::  
user2:$6$C3Jn3FWo4c/.KQt$3ocn1ToqvKFPpYGxKkHqIEQEY2IpkM1Zqat4VD743WT0mo8dnfwZxyVLDpG5Z.ZgdTd4uE5mbT30.8aRhoXco0:19627:0:99999:7:::  
user3:$6$2yUj1P33H5uAHPbZ74saJhK/PHD1XkP1WucffmTJ9N17K421n2tEHqcLmkHa6IM0l1QjVT5C/Z2sXBdUPuSB7HCxVzACu61:19627:0:99999:7:::  
user4:$6$eV8BH/Kjed0/ZN$vs3wMF6UwUG4VP3DpUGaT01BB0muPXNNjfqBZB3.G8p91zLNJHH7dEB5awTWIdFymcWEPwvXyV0qS/nzfdLy0:19627:0:99999:7:::  
user5:$6$G6QLS/pb2yY$W8wsZZIBnJ5cQ0ebvsdKLJLK8dELqzCbx2V2ESccZy/YperhyGjzL4bZqHFuZa0/LHL/8Q8xJGxHFumIHVDgP1:19627:0:99999:7:::  
user6:$6$wCK3./hSk9s9f8$kyMgKmBB5AIsXoAebB2M1mgVZF7XLDxdaSTIN3.LS1cXkYx0IDteL6Sg1YSquWsm0lBeRBxrZXscXcdhpJnSX.:19627:0:99999:7:::  
bburke@ubuntu-vm:~$  
bburke@ubuntu-vm:~$ sudo cat /etc/shadow | tail -6 > bburk002.hash  
bburke@ubuntu-vm:~$ ls  
bburk002.hash Desktop Documents Downloads Music Pictures Public rockyou.txt snap Templates Videos  
bburke@ubuntu-vm:~$  
bburke@ubuntu-vm:~$ john --wordlist=rockyou.txt bburk002.hash  
Using default input encoding: UTF-8  
Loaded 6 password hashes with 6 different salts (sha512crypt, crypt(3) $6$ [SHA512 128/128 ASIMD 2x])  
Cost 1 (iteration count) is 5000 for all loaded hashes  
Will run 4 OpenMP threads  
Press 'q' or Ctrl-C to abort, 'h' for help, almost any other key for status  
dictionary (user1)  
1235 (user2)  
2g 0:00:10:11 2.93% (ETA: 01:25:38) 0.003272g/s 796.7p/s 3734c/s 3734c/s may81997..matching  
Use the "--show" option to display all of the cracked passwords reliably  
Session aborted  
bburke@ubuntu-vm:~$ john --show bburk002.hash  
user1:dictionary:19627:0:99999:7:::  
user2:1235:19627:0:99999:7:::  
  
2 password hashes cracked, 4 left  
bburke@ubuntu-vm:~$
```

Extra Credit

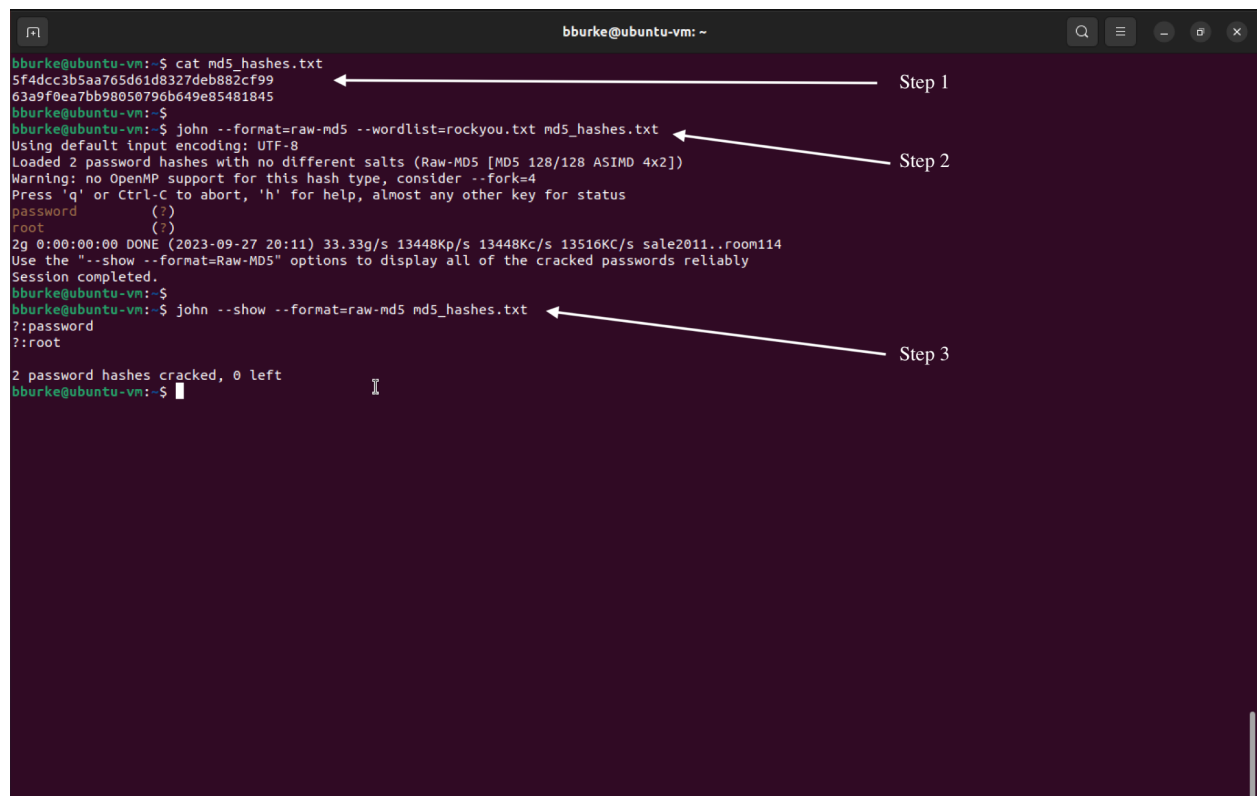
Step 1: Use john to find the provided MD5 hashes. First, create a text file with vim called “**md5_hashes.txt**” with the hashes stored inside.

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**



```
bburke@ubuntu-vm: ~  
bburke@ubuntu-vm:~$ cat md5_hashes.txt  
5f4dcc3b5aa765d61d8327deb882cf99  
63a9f0ea7bb98050796b649e85481845  
bburke@ubuntu-vm:~$ john --format=raw-md5 --wordlist=rockyou.txt md5_hashes.txt  
Using default input encoding: UTF-8  
Loaded 2 password hashes with no different salts (Raw-MD5 [MD5 128/128 ASIMD 4x2])  
Warning: no OpenMP support for this hash type, consider --fork=4  
Press 'q' or Ctrl-C to abort, 'h' for help, almost any other key for status  
password (?)  
root (?)  
2g 0:00:00:00 DONE (2023-09-27 20:11) 33.33g/s 13448Kp/s 13448Kc/s 13516Kc/s sale2011..room114  
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably  
Session completed.  
bburke@ubuntu-vm:~$ john --show --format=raw-md5 md5_hashes.txt  
?:password  
?:root  
2 password hashes cracked, 0 left  
bburke@ubuntu-vm:~$
```

The screenshot shows a terminal window with three steps annotated by arrows:

- Step 1:** Points to the command `cat md5_hashes.txt` which displays the two MD5 hashes.
- Step 2:** Points to the command `john --format=raw-md5 --wordlist=rockyou.txt md5_hashes.txt` which runs John the Ripper. The output shows it loaded 2 password hashes and cracked them to 'password' and 'root'.
- Step 3:** Points to the command `john --show --format=raw-md5 md5_hashes.txt` which shows the cracked passwords in a more readable format: '?:password' and '?:root'.