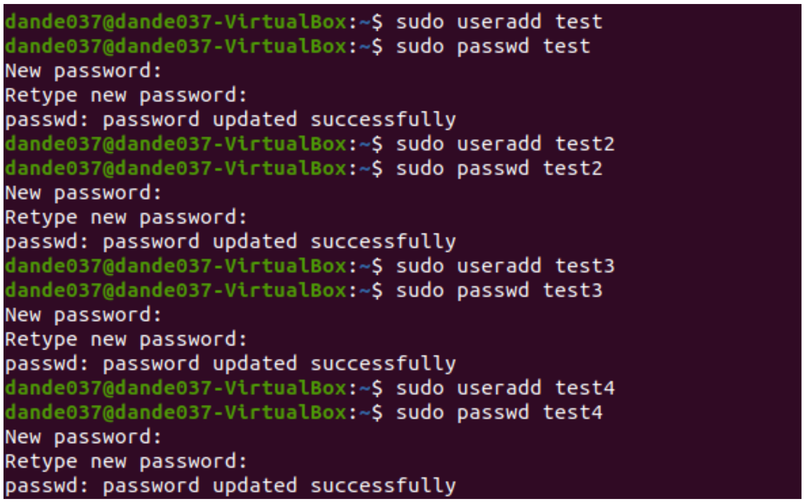
Assignment 5 - Password Cracking

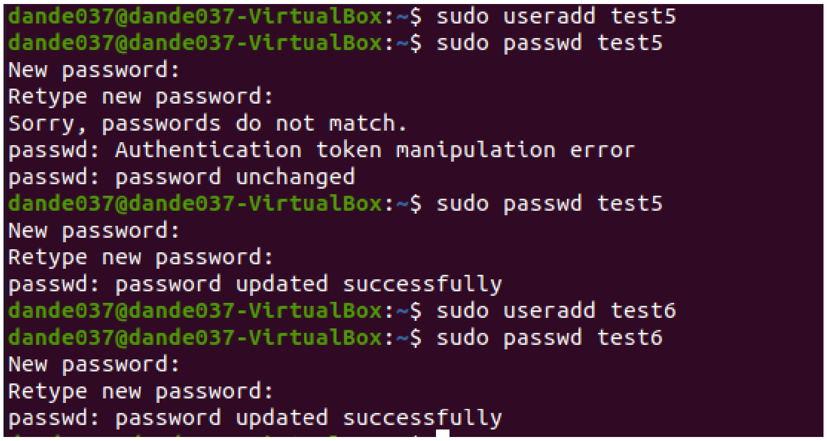
Dylan Anderson

01172654

Task A

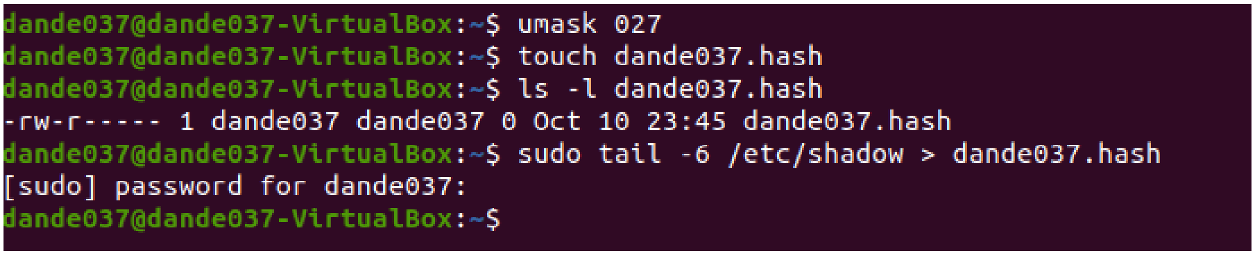


```
dande037@dande037-VirtualBox:~$ sudo useradd test
dande037@dande037-VirtualBox:~$ sudo passwd test
New password:
Retype new password:
passwd: password updated successfully
dande037@dande037-VirtualBox:~$ sudo useradd test2
dande037@dande037-VirtualBox:~$ sudo passwd test2
New password:
Retype new password:
passwd: password updated successfully
dande037@dande037-VirtualBox:~$ sudo useradd test3
dande037@dande037-VirtualBox:~$ sudo passwd test3
New password:
Retype new password:
passwd: password updated successfully
dande037@dande037-VirtualBox:~$ sudo useradd test4
dande037@dande037-VirtualBox:~$ sudo passwd test4
New password:
Retype new password:
passwd: password updated successfully
```



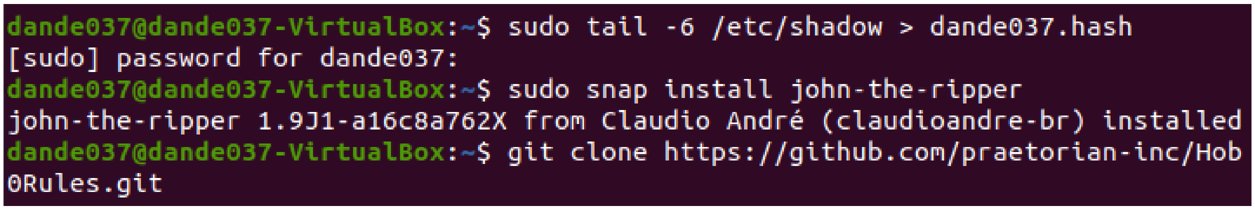
```
dande037@dande037-VirtualBox:~$ sudo useradd test5
dande037@dande037-VirtualBox:~$ sudo passwd test5
New password:
Retype new password:
Sorry, passwords do not match.
passwd: Authentication token manipulation error
passwd: password unchanged
dande037@dande037-VirtualBox:~$ sudo passwd test5
New password:
Retype new password:
passwd: password updated successfully
dande037@dande037-VirtualBox:~$ sudo useradd test6
dande037@dande037-VirtualBox:~$ sudo passwd test6
New password:
Retype new password:
passwd: password updated successfully
```

Six user accounts are created with the useradd command, test1-6, with the specified password requirements for each set with the passwd command. The following passwords for reference in order are tree, 1322, duck93, 1book%, 94smile, 83HelP#@. (A password was mistyped for test5, but was reentered correctly).

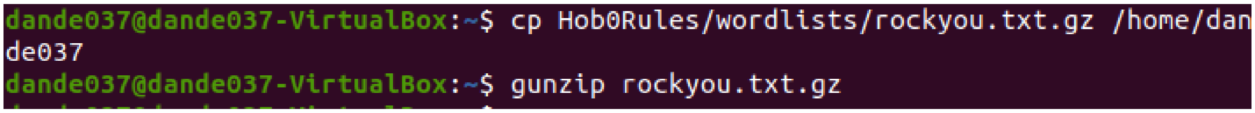


```
dande037@dande037-VirtualBox:~$ umask 027
dande037@dande037-VirtualBox:~$ touch dande037.hash
dande037@dande037-VirtualBox:~$ ls -l dande037.hash
-rw-r----- 1 dande037 dande037 0 Oct 10 23:45 dande037.hash
dande037@dande037-VirtualBox:~$ sudo tail -6 /etc/shadow > dande037.hash
[sudo] password for dande037:
dande037@dande037-VirtualBox:~$
```

A hash file is created with umask and the touch command, then all user passwords are stored into it through the tail command.

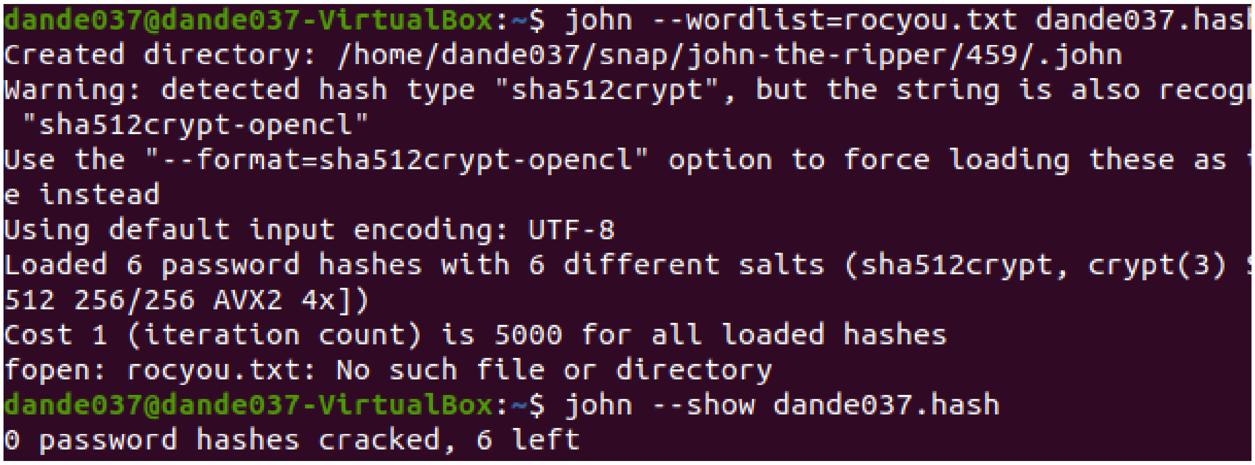


```
dande037@dande037-VirtualBox:~$ sudo tail -6 /etc/shadow > dande037.hash
[sudo] password for dande037:
dande037@dande037-VirtualBox:~$ sudo snap install john-the-ripper
john-the-ripper 1.9J1-a16c8a762X from Claudio André (claudioandre-br) installed
dande037@dande037-VirtualBox:~$ git clone https://github.com/praetorian-inc/Hob
0Rules.git
```



```
dande037@dande037-VirtualBox:~$ cp Hob0Rules/wordlists/rockyou.txt.gz /home/dan
de037
dande037@dande037-VirtualBox:~$ gunzip rockyou.txt.gz
```

John the ripper is installed, a dictionary file is then installed from github, the directory is then cloned to the main home directory using cp, then the rockyou file is unzipped.



```
dande037@dande037-VirtualBox:~$ john --wordlist=rocyou.txt dande037.has
Created directory: /home/dande037/snap/john-the-ripper/459/.john
Warning: detected hash type "sha512crypt", but the string is also recog
 "sha512crypt-opencl"
Use the "--format=sha512crypt-opencl" option to force loading these as
e instead
Using default input encoding: UTF-8
Loaded 6 password hashes with 6 different salts (sha512crypt, crypt(3)
512 256/256 AVX2 4x])
Cost 1 (iteration count) is 5000 for all loaded hashes
fopen: rocyou.txt: No such file or directory
dande037@dande037-VirtualBox:~$ john --show dande037.hash
0 password hashes cracked, 6 left
```

The john the ripper program is then used in wordlist mode and checked after 10 minutes to see how many passwords have been broken.