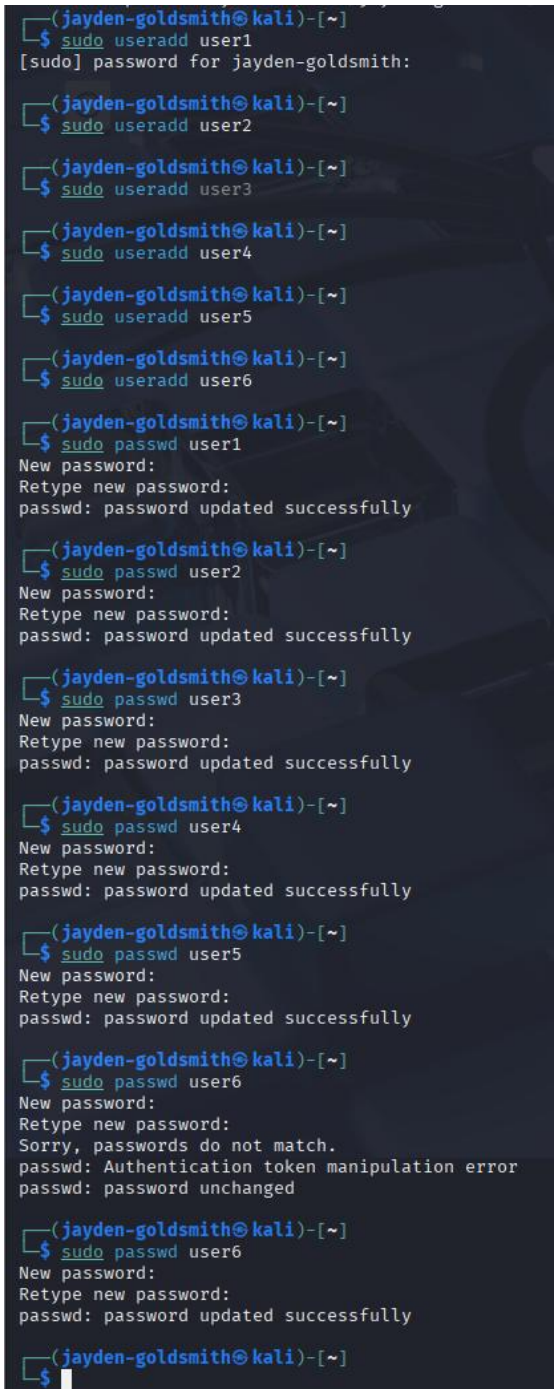
Jayden Goldsmith

Assignment 5 – Password Cracking

1.

Used “sudo” for superuser access to add each user with the “useradd” command. Did the same for setting each user with a password with “passwd”. Used the up arrow on the keyboard to quickly autofill with the previous command and replace the number at the end of each user to change their settings.



Passwords:

user1 = cloud

user2 = 9999

user3 = orange42

user4 = flower100?

user5 = pink123

user6 = BreaD69?

Jayden Goldsmith

2.

Now that all the users I can save the shadow file's content into this new file that uses my MIDAS ID.

```
┌──(jayden-goldsmith㉿kali)-[~]
└─$ sudo cat shadow > jgold033.hash
```

I then checked to see if the users' hashes were in the jgold033.hash, which they were.

```
user1:$y$j9T$GYDB3OJPCiAf3UcAq5/1t0$.NPFfERh3hA5Gl0iOxIcWtYe25tihYm5VtJ1aq7y4A6:20366:0:99999:7:::
user2:$y$j9T$IokDbLNwJndvwlXCqp0lx.$xdsjmf0wJdsvCgKzeQKN6fDRPSFdnQh61IY5bVkXy0C:20366:0:99999:7:::
user3:$y$j9T$/Q5KLWpzaxb8RL2lAnX8u0$sYdRScfxvnyRJtWsxLmAXdCe5CPlSgmsGT6iVDCnY.9:20366:0:99999:7:::
user4:$y$j9T$G8eYl18wkGg7HteE.Qb.V1$fJIZg8DY/h7YTvFJKX6CuB2/1O/oSWFKjPsSedj91g4:20366:0:99999:7:::
user5:$y$j9T$Kgv2vVMCq7CNAryBmP0Rp/$lCEaG1j75nvXQs/aV4z57SlpyYJ.H/cUUv6d.FYGG/D:20366:0:99999:7:::
user6:$y$j9T$idzqE1dG8.Eg1HCaifM7f1$IkBlRc0wT0N9BPK.KkEfzOTQDnDrGCCbkvauAIC6sAA:20366:0:99999:7:::
```

Then used the following command to start John the Ripper and put it in wordlist mode.

```
┌──(jayden-goldsmith㉿kali)-[~]
└─$ sudo john --format=crypt jgold033.hash --wordlist=/home/jayden-goldsmith/rockyou.txt
Using default input encoding: UTF-8
Loaded 10 password hashes with 10 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
Press 'q' or Ctrl-C to abort, almost any other key for status
```

Jayden Goldsmith

3.

~~I have cracked 1 password.~~

I have cracked 2 passwords.

After 10 minutes, user5 is the only password to be cracked, the password being “pink123”. After waiting an additional 10 minutes it is still the only password to be cracked.

```
┌──(jayden-goldsmith㉿kali)-[~]
└─$ sudo john --format=crypt jgold033.hash --wordlist=/home/jayden-goldsmith/rockyou.txt
Using default input encoding: UTF-8
Loaded 14 password hashes with 14 different salts (crypt, generic crypt(3) [?/64])
Remaining 11 password hashes with 11 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
pink123          (user5)
```

I understand why password for user 4 and user6 weren’t cracked as they both use letters, digits, symbols, and user6 additionally using uppercase letters, but I am not sure why the simpler passwords like “cloud” or “9999” weren’t cracked.

I have added each user and their passwords the exact same way. The only thing I can conclude is that maybe the words I have chosen are much more down the list than “pink”.

As I was typing user1’s password has been cracked so I think my theory maybe correct.

```
┌──(jayden-goldsmith㉿kali)-[~]
└─$ sudo john --format=crypt jgold033.hash --wordlist=/home/jayden-goldsmith/rockyou.txt
Using default input encoding: UTF-8
Loaded 14 password hashes with 14 different salts (crypt, generic crypt(3) [?/64])
Remaining 11 password hashes with 11 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
pink123          (user5)
cloud            (user1)
```

EXTRA CREDIT

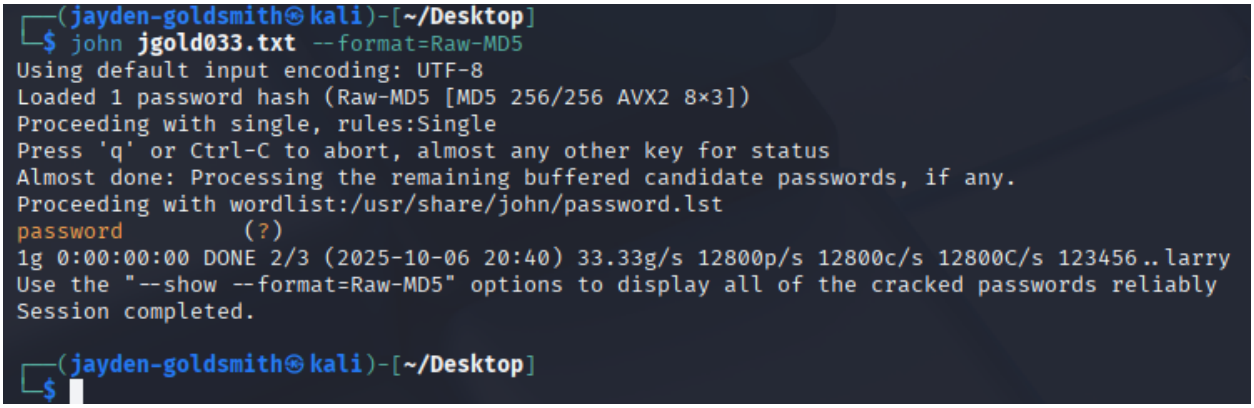
1.

First, I used echo to put the first hash into a new txt file in the Desktop directory.

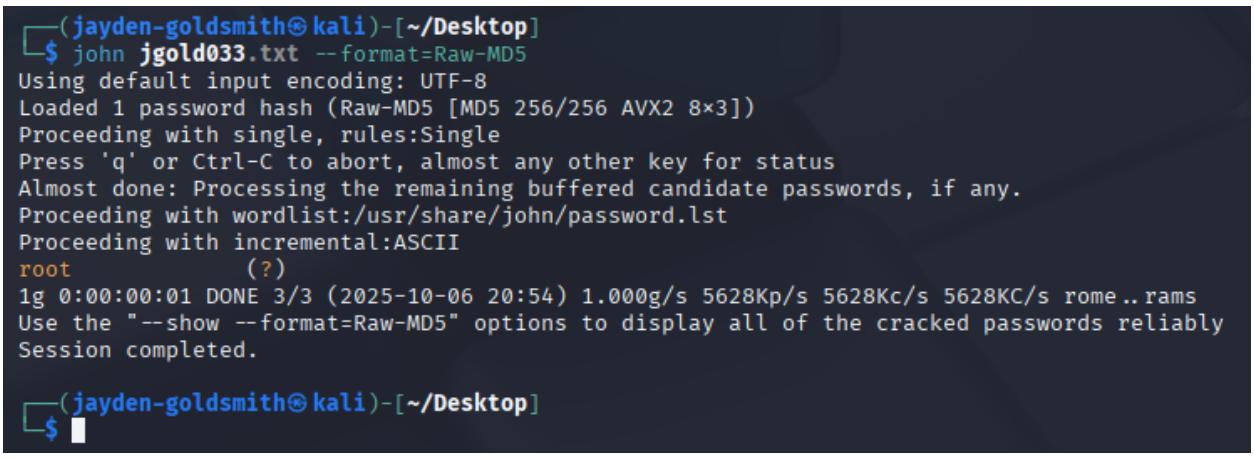
```
┌──(jayden-goldsmith㉿kali)-[~]
└─$ echo 5f4dcc3b5aa765d61d8327deb882cf99 > /home/jayden-goldsmith/Desktop/jgold033.txt
```

I then switched to the Desktop directory with “cd”, checked its contents with “ls” then checked if the file had the hash inside with “cat”.

Then, I used the john command on the txt file using “—format=Raw-MD5”, “Raw” meaning it will crack plain hashes and “MD5” cracking hashes in the MD5 format.



I then repeated this process to crack the second hash.



Jayden Goldsmith

a. 5f4dcc3b5aa765d61d8327deb882cf99 = password

b. 63a9f0ea7bb98050796b649e85481845 = root