**Screen Shot 1)** Take a screen shot of your John the Ripper results showing the passwords that were cracked.

Text

Description automatically generated

**Screen Shot 2)** Take a screen shot of your Hashcat results showing the passwords that were cracked.

A screenshot of a computer

Description automatically generated with medium confidence

**Screen Shot 3)** Take a screen shot of your John the Ripper results showing the password that was cracked

**.Text

Description automatically generated**

**Screen Shot 4)** Take a screen shot showing the hash, type, and result from the web page.

**Graphical user interface

Description automatically generated**

**Question 1)** Do you feel these default password policies are strong enough? Why or why not?

**ANS:** No, because it doesn’t enforce the complexity of the password which makes it easier for attackers to crack the password easily. If we see the default minimum password length of the windows password policy, it is very short which is not a recommended password length.

**Screen Shot 5)** Take a screen shot showing the stricter password policies you have set.

Graphical user interface, text, application

Description automatically generated

**Question 2)** Since the password on your current account is probably set with a password that does not meet these new policies, what do you think will happen if you logout and try to log back in?

Try it… Why were you successful?

**ANS:** If I logged out, I should be able to log in back since the minimum age of the password I have is still young. But after the minimum age, I will be forced to change my password that meets the policies. I tried to log out and log in back and I was successful.

**Question 3)** Try changing your existing password to something like Password123. Were you successful? Why or why not? Now change it to a password that meets the new, enforced requirements. Were you successful?

**ANS:** I was not able to change the old password to the one provided above because it is less than the minimum password length, which is 15 characters.

**Question 4)** What is one way of enforcing password policy on a Linux operating system? You can choose which Linux distribution you would like to research (i.e., Red Hat, Suse, Ubuntu, Debian, Fedora, etc.).

**Enforcing password policy on an Ubuntu Linux operating system:**

Install libpam-cracklib

*Sudo apt-get install libpam-cracklib --force-yes –y*

Password criteria

*gedit etc/pam.d/common-password*

Add the lines below to an open space of the *common-password.txt* file

Password requisite pam\_cracklib.so retry=3 minlen=8 difok=3 reject\_username minclass=3 maxrepeat=2 dcredit=1 ucredit=1 lcredit=1 ocredit=1

Password requisite pam\_pwhistory.so use\_authtok remember=24 enforce\_for\_root

Minimum and maximum days

*sudo gedit /etc/login.defs*

modify the days to:

PASS\_MAX\_DAY 30

PASS\_MIN\_DAY 5

PASS\_WARN\_AGE 14

**Question 5)** Last question….Did you like this lab? Why or why not?

ANS: This lab was great. It showed me how important it is to have a strong and complex password as we discussed in class. Also, I was able to crack passwords which is fun 😊 when its legal lol. Thank you professor.