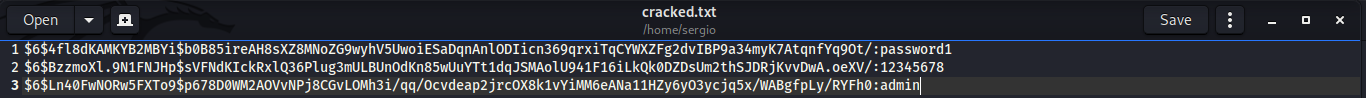
**Screen Shot 1)** Take a screen shot of your John the Ripper results showing the passwords that were cracked.

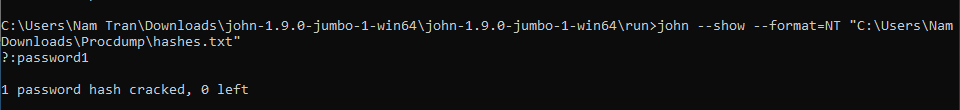
Text

Description automatically generated

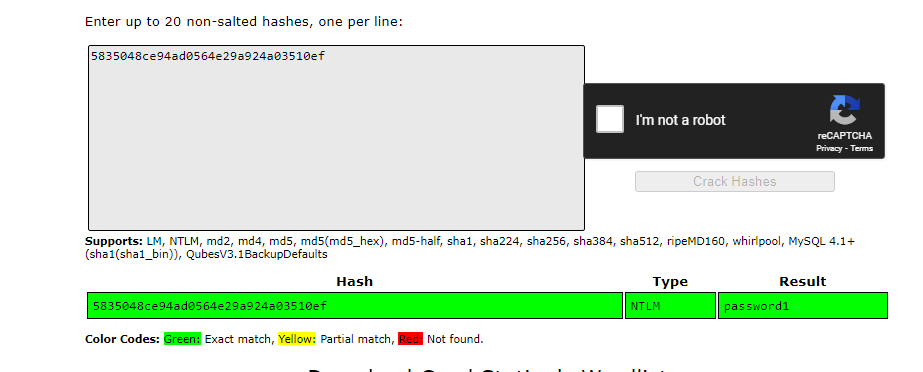
**Screen Shot 2)** Take a screen shot of your Hashcat results showing the passwords that were cracked.

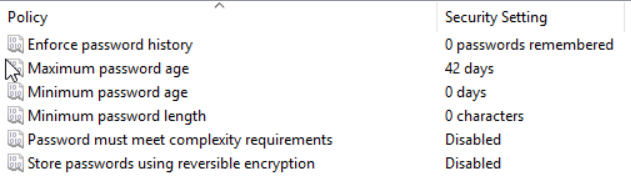


**Screen Shot 3)** Take a screen shot of your John the Ripper results showing the password that was cracked.



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

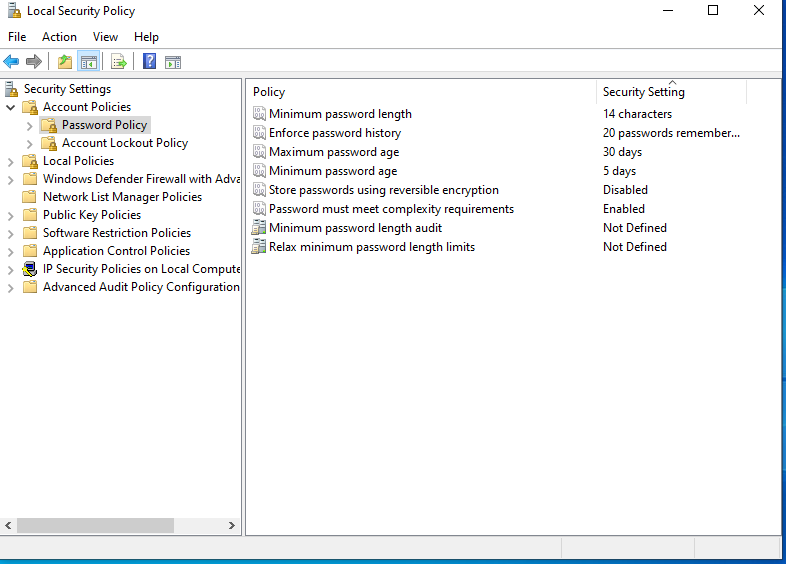




**Question 1)** Do you feel these default password policies are strong enough? Why or why not?

No, they are not strong enough. They allow passwords that are not complex. They also give enough time for the adversary to break the password.

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



**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?

Yes, because the current computer is still using the current passwords which allows the user to login. Thus the current password still let the user login until it is updated by the user.

**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?

No, I was not able to do these because they do not meet the new enforced requirements. When I make it conform to the requirements it worked.

**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.).

PAM is used most to enforce password polices on a Linux operating system.

Redhat: @/etc/pam.d/system-auth

Debian:@/ect/pam.d/common-password

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

Yes I enjoyed this lab because it taught me why we care about password complexities.

**Linux Hashes:**

$6$Tb/MEhvAuMczADJc$u3A8gCyn4p3qwAJxghxHMct41cS9Y2G7RYfAyO8bNSfy3uvU3uGlgqwhPMR/kmNhGmWerhzzcN8dKOdKnr3/K.

**Hint:** This is not a strong password and it does not meet the enforced complexity requirements.

$6$BMBrsE1pFCV96k9b$o/9NDLUlDp7q1kfUsGOegrad/3STPJ5qCI6onj1cEcAWSnAXioOiowOxIZ96Gnj2aWlnWJ7qdnv1z.f8Es1.k.

**Hint:** This is a strong password that meets the enforced complexity requirements.

**Windows NTLM Hashes:**

9075168608b7aba2428c8387bfeb9aee

Passoword: Hacker123

**Hint:** This is not a strong password and it does not meet the enforced complexity requirements.

603d0577c4928244c02a1b7b2a9a62da

**Hint:** This is a strong password that meets the enforced complexity requirements.