Anthony Constantino
Project 7

Password Cracking

1)

Times are rounded. Chars 6-12 are estimated since they take too long.
2 chars: 1 minute
4 chars: 15 minutes
6 chars: 5.5 hours
8 chars: 2 days
10 chars: 26 days
12 chars: 540 days

2)

I do not think that the password meter is a good indication of password security. This is because you can have a long password and it will say that it is strong even if it only includes characters and maybe numbers. Ideally you would want to make sure that you include special characters and capitals in the password to increase the subset of characters that a hacker would have to go through to break your password.

3)

Using the system with the 4 Radeon 5970 GPUs
6 chars: .3 seconds
8 chars: 4 seconds
10 chars: 45 seconds
12 chars: 10 minutes.

With speeds like this it makes it seem like no password is safe because of how fast the GPUs can perform the hashes.

4)

With the given technology, out there these algorithms are no longer safe to a dedicated set of hackers with the proper equipment. It may work against those who are doing it without a lot of resources, but for those who are really determined they will be able to crack it eventually with the proper time and machinery.

5)

Salt can help since it is random it adds another level of security to the password. It helps prevent the hacker use known and common words in attempts to get at the password by making it a mixture of known word(s) and random characters.

6)

No being offline doesn't help your system if the machines are not isolated completely. If the machine is not completely off the grid, then a hacker can still get at it whether it is offline. All he would have to do it crack it offline and then wait for it to go online and they would be ready for the attack.