Hi Sir/ Ma’am,

As per the given task, I have gone through all the resources that were provided to me and tried cracking the passwords provided in the ‘password dump’ file. The following describes the several weaknesses that were found in your policy and a few points to remember to improve the password policy.

All the passwords that were found vulnerable uses MD5.

MD5(Message Digest Algorithm 5) is a cryptographic hash algorithm that is used to create a 128-bit string value from an arbitrary length string. It is still widely used even though there have been insecurities identified with MD5. It is usually not recommended for password because several collision-based weaknesses have been demonstrated and it can expose a user's password. And also because it provides only one-way authentication(not mutual authentication) of wireless clients.

Changing the password encryption mechanism from MD5(Message Direct Algorithm 5) to SHA(Secure Hash Algorithm) is suggestible. Although slower, SHA is secure than MD5 because it produces 160-bit string value and not 128-bit, so an attack would be more difficult to carry out. Also there are no collisions in SHA.

The following are the few things I found about the organization’s password policy. The organization does not have any set of requirements for the users to set up passwords. Users can use any combination of alphabets or numbers to set a password.

The following are the few things I would change in password policy to make breaking the passwords harder.

* Passwords should be a mixture of upper case, lower case, letters, special characters.
* Avoid using common names, their own names or words from the dictionary that are not guessable by any program.
* Not to use the same password that is used to access other websites or accounts.
* Longer passwords should be preferred.
* Make the users read the password policy.