We were able to decrypt seven out of the all given passwords – using hashcat6.1.1

e10adc3949ba59abbe56e057f20f883e:123456

e99a18c428cb38d5f260853678922e03:abc123

96e79218965eb72c92a549dd5a330112:111111

d8578edf8458ce06fbc5bb76a58c5ca4:qwerty

3f230640b78d7e71ac5514e57935eb69:qazxsw

fcea920f7412b5da7be0cf42b8c93759:1234567

f6a0cb102c62879d397b12b62c092c06:bluered

The hashing algorithm used to protect the password was MD5. Since it was designed to convert plain text to hashed text, it is unsuitable and does not really offer much protection to the passwords.

In order to make the passwords much harder to crack, a better hashing algorithm like BLAKE or BLAKE2 may be adopted.

The organization’s password policy includes –

1. A minimum length of 6 characters
2. No key spaces

The changes that may be implemented in the password to make the passwords harder to crack, are –

1. A combination of uppercase and lowercase characters (At least one uppercase and one lowercase character)
2. At least one special character
3. No two consecutive characters are to be the same