**CRACKING PASSWORDS – GOLDMAN SACHS – VIRTUAL INTRERNSHIP**

* NUMBER OF PASSWORDS CRACKED – 13/19
* LIST OF PASSWORDS CRACKED:

|  |  |  |  |
| --- | --- | --- | --- |
| HASH | PASSWORD | PROTECTION TYPE | USERNAME |
| e10adc3949ba59abbe56e057f20f883e | 123456 | md5 | experthead |
| 25f9e794323b453885f5181f1b624d0b | 123456789 | md5 | interestec |
| d8578edf8458ce06fbc5bb76a58c5ca4 | qwerty | md5 | ortspoon |
| 5f4dcc3b5aa765d61d8327deb882cf99 | password | md5 | reallychel |
| 96e79218965eb72c92a549dd5a330112 | 111111 | md5 | simmson56 |
| 25d55ad283aa400af464c76d713c07ad | 12345678 | md5 | bookma |
| e99a18c428cb38d5f260853678922e03 | abc123 | md5 | popularkiya7 |
| fcea920f7412b5da7be0cf42b8c93759 | 1234567 | md5 | eatingcake1994 |
| 7c6a180b36896a0a8c02787eeafb0e4c | password1 | md5 | heroanhart |
| 6c569aabbf7775ef8fc570e228c16b98 | password! | md5 | edi\_tesla89 |
| 3f230640b78d7e71ac5514e57935eb69 | qazxsw | md5 | liveltekah |
| 917eb5e9d6d6bca820922a0c6f7cc28b | Pa$$word1 | md5 | blikimore |
| f6a0cb102c62879d397b12b62c092c06 | bluered | md5 | johnwick007 |

* Each of the passwords which I was able to crack used the md5 algorithm and could easily be found using the hashcat tool on the terminal and the rockyou.txt dictionary
* The level of protection for the algorithm found, i.e., the md5 is very low as it has no salting and is very easily cracked by a hacker due to its nature.
* To make it harder to crack the password one can take various steps including: increase the length of the password (at least above 8-10 characters), avoid using general and common passwords, use a mix of special symbols, use capital and small letters
* The organization clearly does not limit the length of the password user can enter.
* They allow the user to enter common passwords.
* To make it tougher for the user to crack the password the organization can set some ground rules to avoid breakage. Some of them being:

1. Keep minimum length of 10 characters at least and do not allow common passwords related to the username or date of birth of user.
2. Only allow user to proceed if he has used a mixture of Capital, small letters, Special symbols and numbers in the password