Hashing and Crack Password Lab

Lab Environment

We have created two accounts in the VM. The usernames and passwords are listed in the following:

- User ID: root, Password: seedubuntu.
  - Note: Ubuntu does not allow root to login directly from the login window. You have to login as a normal user, and then use the command su to login to the root account.
- User ID: seed, Password: dees

Task 1: MD5 hashing

1. Use command md5Sum for hashing.
   1.1 Type `md5um --help`

```
seed@Server(10.0.2.4):--$ md5sum --help
Usage: md5sum [OPTION]... [FILE]...
Print or check MD5 (128-bit) checksums.
With no FILE, or when FILE is -, read standard input.

   -b, --binary   read in binary mode
   -c, --check    read MD5 sums from the FILEs and check them
   -t, --text     read in text mode (default)

The following three options are useful only when verifying checksums:
   --quiet        don't print OK for each successfully verified file
   --status       don't output anything, status code shows success
   -w, --warn     warn about improperly formatted checksum lines

   --strict       with --check, exit non-zero for any invalid input
   --help         display this help and exit
   --version      output version information and exit
```

2. `echo` will normally output a newline, which is suppressed with `-n`
3. Questions:
   3.1 Find the original password

<table>
<thead>
<tr>
<th>Original password</th>
<th>MD5 hashed Password</th>
<th>hints</th>
</tr>
</thead>
<tbody>
<tr>
<td>7c6a180b36896a0a8c02787eae9b0e4c</td>
<td>17c6a180b36896a0a8c02787eae9b0e4c</td>
<td>5 digits and 4 letters</td>
</tr>
<tr>
<td>6cb75f652a9b52798eb6cf2201057c73</td>
<td>6cb75f652a9b52798eb6cf2201057c73</td>
<td>4 digits</td>
</tr>
<tr>
<td>a047343bf4ba65fd4c4ef9596c92960c</td>
<td>a047343bf4ba65fd4c4ef9596c92960c</td>
<td></td>
</tr>
<tr>
<td>827ccb0eea8a706c4c34a16891f84e7b</td>
<td>827ccb0eea8a706c4c34a16891f84e7b</td>
<td></td>
</tr>
</tbody>
</table>

4. You need to create a shell program to generate a list of hashed password
   4.1 Create a shell program, named `generatedmd5`

   ```bash
   #!/bin/bash
   seed=0
   for((i=0;i<5;i++))
     do
       echo -n "$i" | md5sum
   done
   ```

   4.2 Make the program executable and run.

   ```bash
   seed@Server(10.0.2.4):~$ gedit generatedmd5
   seed@Server(10.0.2.4):~$ chmod +x generatedmd5
   seed@Server(10.0.2.4):~$ ./generatedmd5
   ```

   ```bash
   cfcd288495d565ef66e7df9f9f98764da -
   c4ca4238a0b923820d5cc59a6f75849b -
   c81728d9d4c2f636f067f89cc14862c -
   ecdbcb7e4b5c6e2fe28308fd9f2af3 -
   a87ff679a2f3e71d9181a67b7542122c -
   e4da3b7fbce2345d7772b0674a318d5 -
   seed@Server(10.0.2.4):~$ ```