Hashing and Crack Password Lab

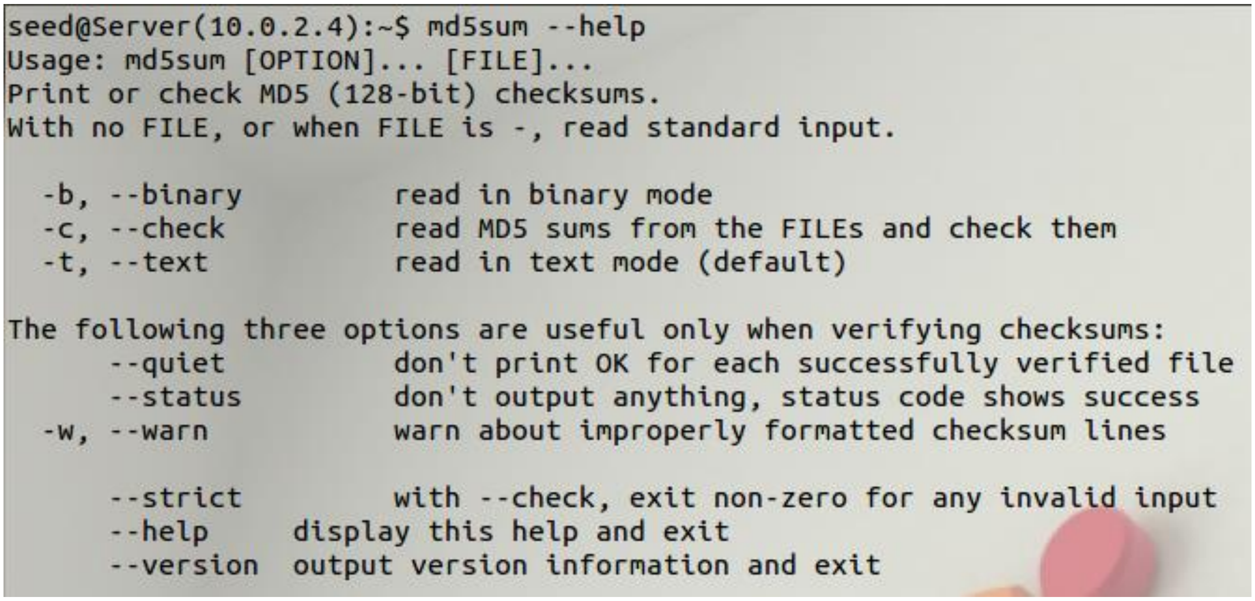
Lab Environment

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



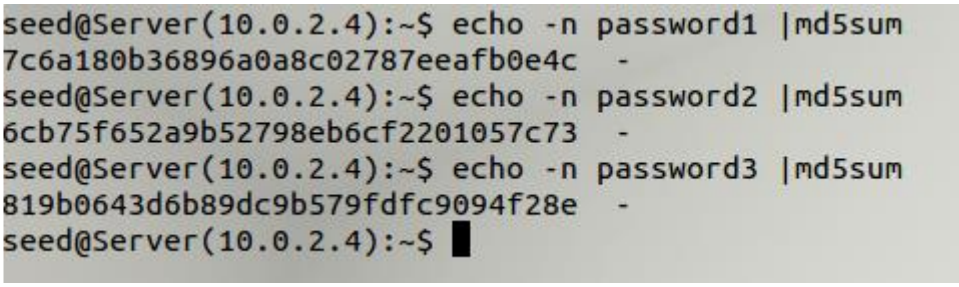
```
seed@Server(10.0.2.4):~$ md5sum --help
Usage: md5sum [OPTION]... [FILE]...
Print or check MD5 (128-bit) checksums.
With no FILE, or when FILE is -, read standard input.

  -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`

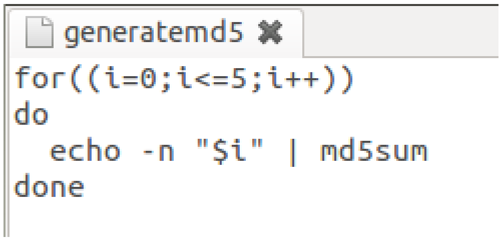


```
seed@Server(10.0.2.4):~$ echo -n password1 |md5sum
7c6a180b36896a0a8c02787eeafb0e4c  -
seed@Server(10.0.2.4):~$ echo -n password2 |md5sum
6cb75f652a9b52798eb6cf2201057c73  -
seed@Server(10.0.2.4):~$ echo -n password3 |md5sum
819b0643d6b89dc9b579fdfc9094f28e  -
seed@Server(10.0.2.4):~$ 
```

3. Questions:
   3.1 Find the original password

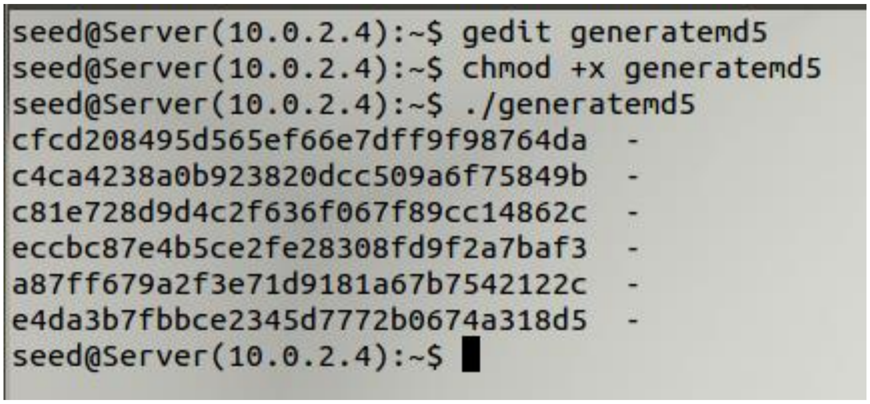
Original password	MD5 hashed Password	hints
	7c6a180b36896a0a8c02787eeafb0e4c	
	6cb75f652a9b52798eb6cf2201057c73	
	a047343bf4ba65fd4c4ef9596c92960c	5 digits and 4 letters
	827ccb0eea8a706c4c34a16891f84e7b	4 digits

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



```
for((i=0;i<=5;i++))
do
  echo -n "$i" | md5sum
done
```

   4.2 Make the program executable and run.



```
seed@Server(10.0.2.4):~$ gedit generatemd5
seed@Server(10.0.2.4):~$ chmod +x generatemd5
seed@Server(10.0.2.4):~$ ./generatemd5
cfcd208495d565ef66e7dff9f98764da  -
c4ca4238a0b923820dcc509a6f75849b  -
c81e728d9d4c2f636f067f89cc14862c  -
eccbc87e4b5ce2fe28308fd9f2a7baf3  -
a87ff679a2f3e71d9181a67b7542122c  -
e4da3b7fbbce2345d7772b0674a318d5  -
seed@Server(10.0.2.4):~$ 
```