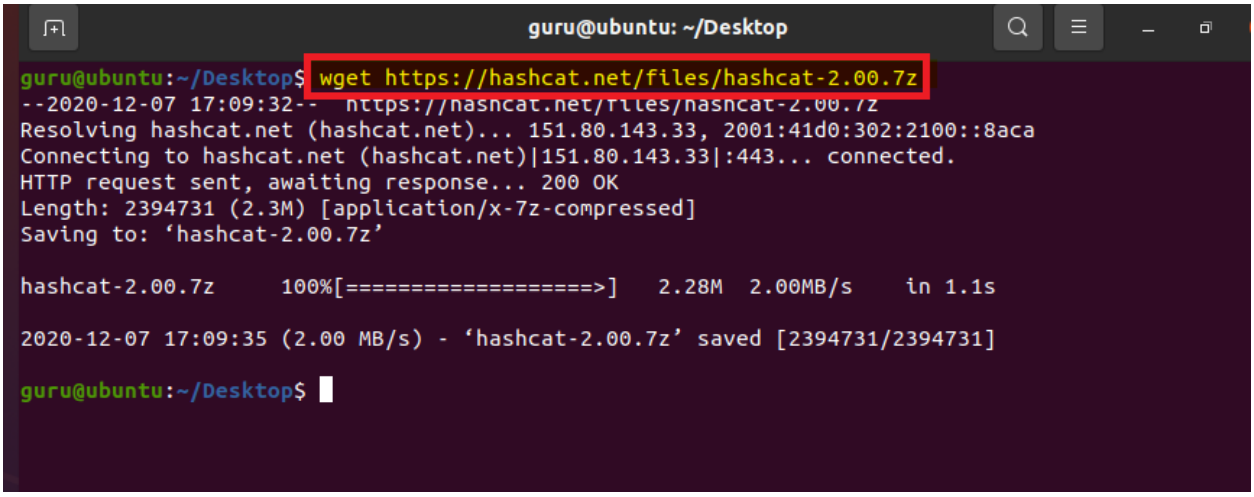
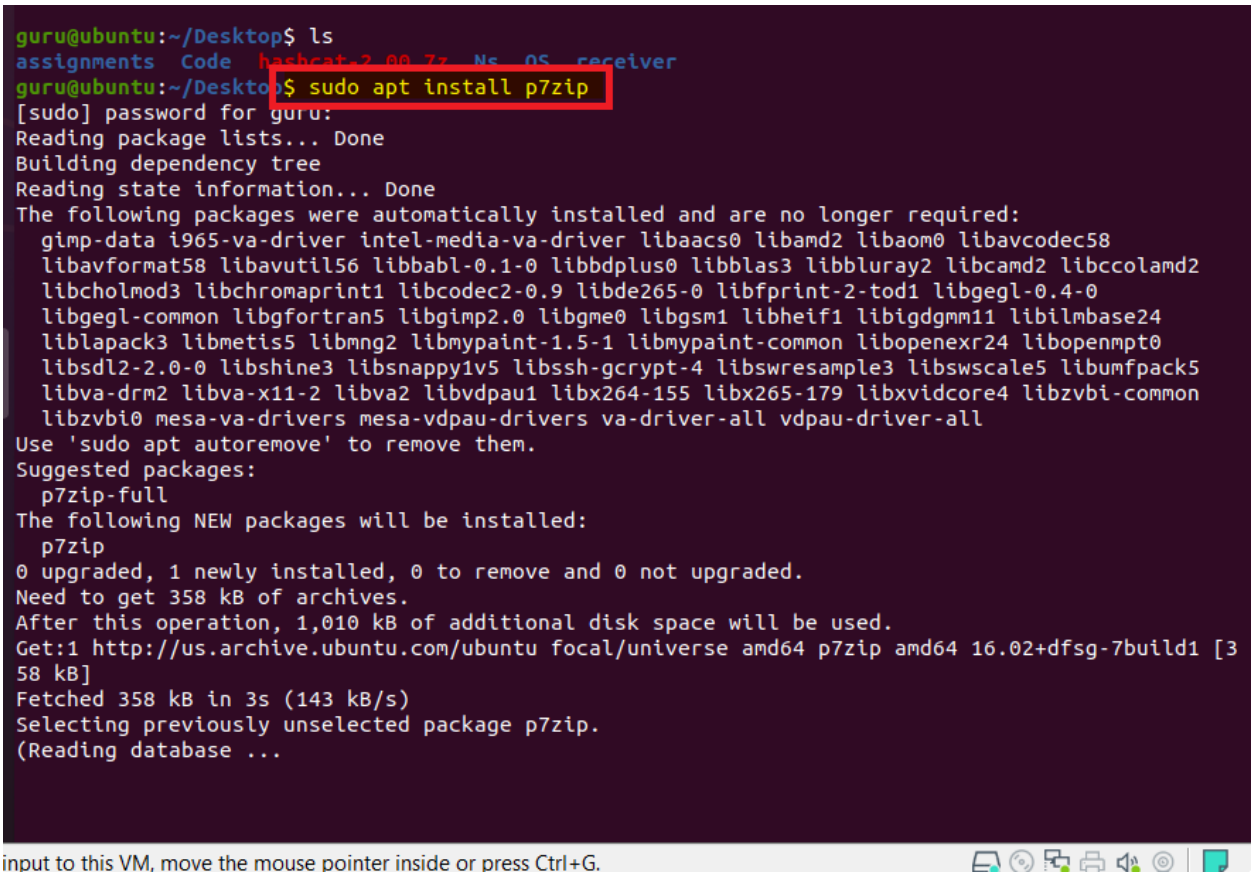
ASSIGNMENT-9(Password Cracking)

-D.V.Guru Saran(AM.EN.P2CSN20010)

1. Download hastcat setup file from website:https://hashcat.net/files/hashcat-2.00.7z



2. The downloaded setup is in zip file. Extract hashcat.2.00.7z using pzip.
   (i) Install p7zip using command "sudo apt install p7zip"



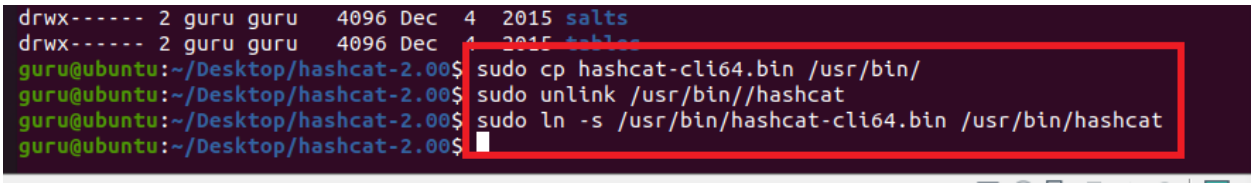
(ii) Extract the zip file using command: p7zip -d hashcat-2.000.7z

```
Processing triggers for man-db (2.9.1-1) ...
guru@ubuntu:~/Desktop$ p7zip -d hashcat-2.00.7z

7-Zip (a) [64] 16.02 : Copyright (c) 1999-2016 Igor Pavlov : 2016-05-21
p7zip Version 16.02 (locale=en_US.UTF-8,Utf16=on,HugeFiles=on,64 bits,4 CPUs Intel(R) Core(TM) i
5-8300H CPU @ 2.30GHz (106A5),ASM,AES-NI)

Scanning the drive for archives:
1 file, 2394731 bytes (2339 KiB)

Extracting archive: hashcat-2.00.7z
--
Path = hashcat-2.00.7z
Type = 7z
Physical Size = 2394731
Headers Size = 2417
Method = LZMA:24 BCJ
Solid = +
Blocks = 2

Everything is Ok

Folders: 37
Files: 178
Size:       13330637
Compressed: 2394731
guru@ubuntu:~/Desktop$
```

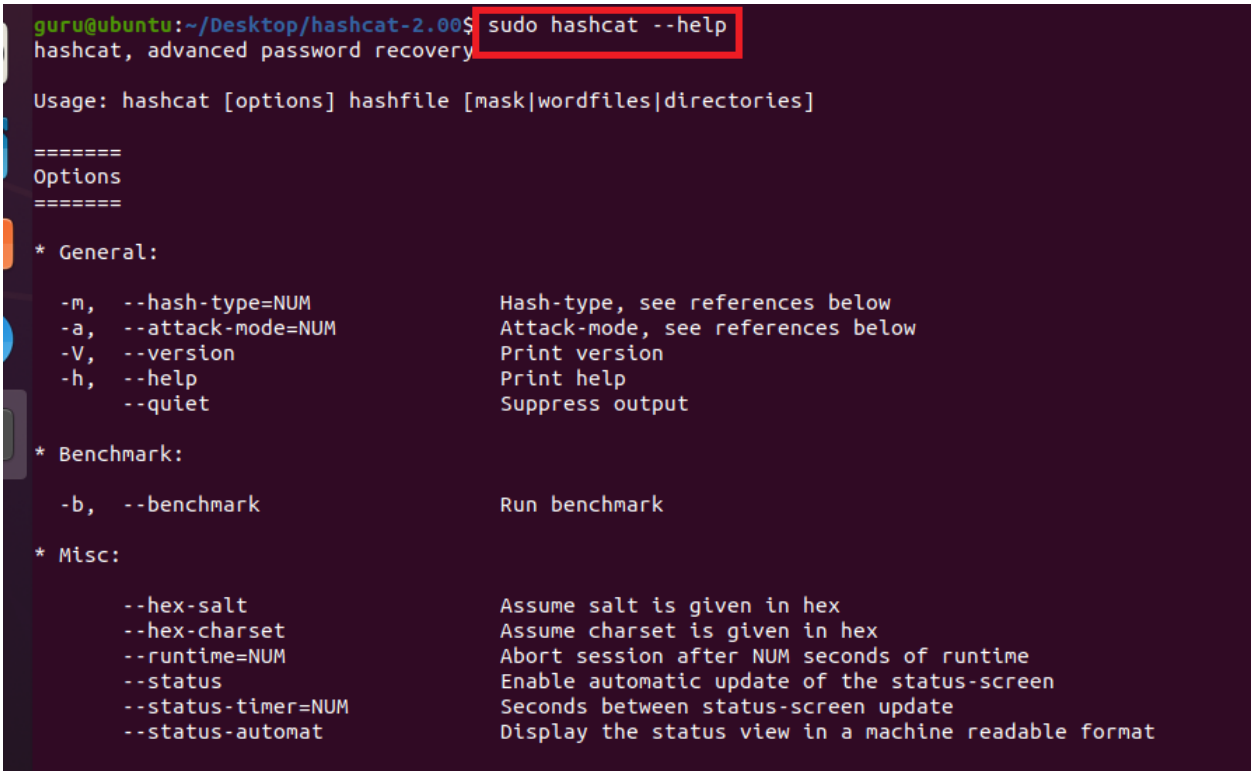
3. Here are the extracted files

```
Compressed: 2394731
guru@ubuntu:~/Desktop$ ls
assignments  Code  hashcat-2.00  Ns  OS  receiver
guru@ubuntu:~/Desktop$ cd hashcat-2.00/
guru@ubuntu:~/Desktop/hashcat-2.00$ ls -l
total 6224
drwx------ 5 guru guru   4096 Nov 23  2015 charsets
drwx------ 2 guru guru   4096 Dec  4  2015 docs
drwx------ 2 guru guru   4096 Dec  4  2015 examples
-rwx------ 1 guru guru 919596 Dec  4  2015 hashcat-cli32.bin
-rw------- 1 guru guru 932352 Dec  4  2015 hashcat-cli32.exe
-rwx------ 1 guru guru 940360 Dec  4  2015 hashcat-cli64.app
-rwx------ 1 guru guru 891944 Dec  4  2015 hashcat-cli64.bin
-rw------- 1 guru guru 935936 Dec  4  2015 hashcat-cli64.exe
-rwx------ 1 guru guru 838696 Dec  4  2015 hashcat-cliXOP.bin
-rw------- 1 guru guru 880128 Dec  4  2015 hashcat-cliXOP.exe
drwx------ 2 guru guru   4096 Dec  4  2015 rules
drwx------ 2 guru guru   4096 Dec  4  2015 salts
drwx------ 2 guru guru   4096 Dec  4  2015 tables
guru@ubuntu:~/Desktop/hashcat-2.00$
input to this VM, move the mouse pointer inside or press Ctrl+G.
```

4. To install the hashcat-2.00 use the following commands:

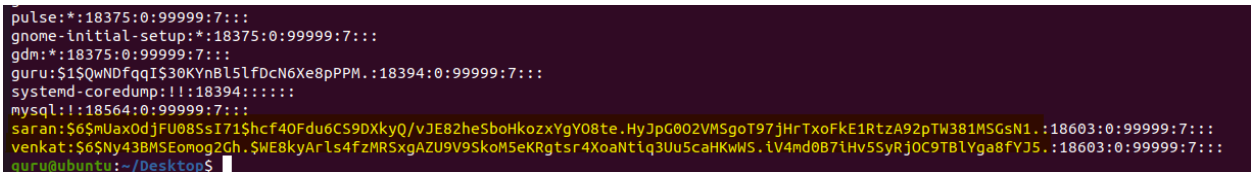


5. Check whether the hashcat is installed or not using some hashcat commands.

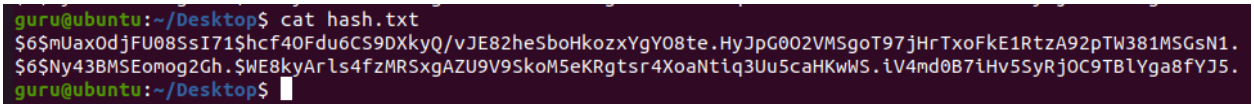


6. To crack the password in hashcat, we need:
   (i) hashes from shadow files
   (ii) wordlist to crack the password
   (iii) type of hashing used to encrypt the password

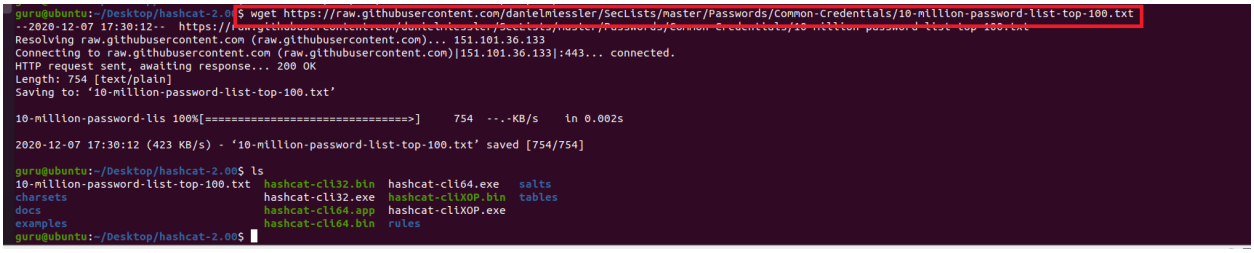
7. Get the password hash value using command: sudo cat /etc/shadow



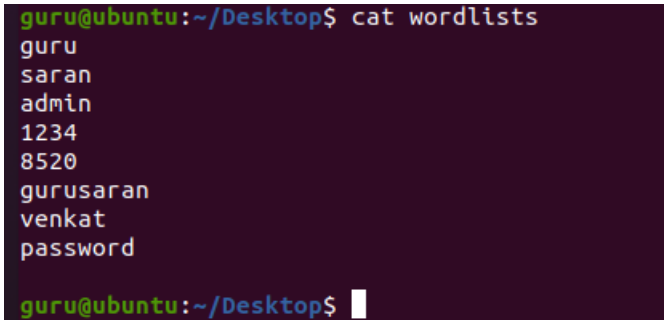
8. Copy the hash value to a text file



9. Download the wordlist from website. But these wordlists are not helpful to crack the password



10. Create a wordlist consists of users' password



11. Checking what type of algorithm used for hashing in /etc/login.defs

```
guru@ubuntu:~/Desktop/hashcat-2.00$ cat /etc/login.defs
#
# /etc/login.defs - Configuration control definitions for the login package.
#
# Three items must be defined:  MAIL_DIR, ENV_SUPATH, and ENV_PATH.
# If unspecified, some arbitrary (and possibly incorrect) value will
# be assumed.  All other items are optional - if not specified then
# the described action or option will be inhibited.
#
# Comment lines (lines beginning with "#") and blank lines are ignored.
#
# Modified for Linux.  --marekm

# REQUIRED for useradd/userdel/usermod
#   Directory where mailboxes reside, _or_ name of file, relative to the
#   home directory.  If you _do_ define MAIL_DIR and MAIL_FILE,
#   MAIL_DIR takes precedence.
#
#   Essentially:
#      - MAIL_DIR defines the location of users mail spool files
#        (for mbox use) by appending the username to MAIL_DIR as defined
#        below.
#      - MAIL_FILE defines the location of the users mail spool files as the
#        fully-qualified filename obtained by prepending the user home
#        directory before $MAIL_FILE
#
# NOTE: This is no more used for setting up users MAIL environment variable
```

SHA512 encryption method is used for hashing

```
# This variable is deprecated. You should use ENCRYPT_METHOD.
#
#MD5_CRYPT_ENAB no

#
# If set to MD5 , MD5-based algorithm will be used for encrypting password
# If set to SHA256, SHA256-based algorithm will be used for encrypting password
# If set to SHA512, SHA512-based algorithm will be used for encrypting password
# If set to DES, DES-based algorithm will be used for encrypting password (default)
# Overrides the MD5_CRYPT_ENAB option
#
# Note: It is recommended to use a value consistent with
# the PAM modules configuration.
#
ENCRYPT_METHOD SHA512

#
# Only used if ENCRYPT_METHOD is set to SHA256 or SHA512.
#
# Define the number of SHA rounds.
# With a lot of rounds, it is more difficult to brute forcing the password.
# But note also that it more CPU resources will be needed to authenticate
# users.
#
# If not specified, the libc will choose the default number of rounds (5000).
# The values must be inside the 1000-999999999 range.
# If only one of the MIN or MAX values is set, then this value will be used.
# If MIN > MAX, the highest value will be used.
#
# SHA_CRYPT_MIN_ROUNDS 5000
# SHA_CRYPT_MAX_ROUNDS 5000
```

12. Use this command to crack the passwords in hash.txt file
    Command: sudo hashcat -m 1800 -a 0 -o cracked.txt hash.txt wordlists
    (i) Since hashing uses SHA-512 use -m 1800
    (ii) Use dictionary attack -a 0
    (iii) hash.txt -> contains hash values
    (iv) wordlists -> contains few passwords
    (v) -o cracked.txt -> cracked passwords are stored in cracked.txt

13. Cracked.txt file contains decrypted passwords