

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>

```
guru@ubuntu: ~/Desktop
guru@ubuntu:~/Desktop$ wget https://hashcat.net/files/hashcat-2.00.7z
--2020-12-07 17:09:32-- https://hashcat.net/files/hashcat-2.00.7z
Resolving hashcat.net (hashcat.net)... 151.80.143.33, 2001:41d0:302:2100::8aca
Connecting to hashcat.net (hashcat.net)|151.80.143.33|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 2394731 (2.3M) [application/x-7z-compressed]
Saving to: 'hashcat-2.00.7z'

hashcat-2.00.7z      100%[=====>]  2.28M  2.00MB/s   in 1.1s

2020-12-07 17:09:35 (2.00 MB/s) - 'hashcat-2.00.7z' saved [2394731/2394731]

guru@ubuntu:~/Desktop$
```

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

```
guru@ubuntu:~/Desktop$ ls
assignments Code hashcat-2.00.7z Ms-DOS receiver
guru@ubuntu:~/Desktop$ sudo apt install p7zip
[sudo] password for guru:
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
  gimp-data i965-va-driver intel-media-va-driver libaacs0 libamd2 libaom0 libavcodec58
  libavformat58 libavutil56 libbabi-0.1-0 libbdplus0 libblas3 libbluray2 libcamd2 libccolamd2
  libcholmod3 libchromaprint1 libcodec2-0.9 libde265-0 libffprint-2-tod1 libgegl-0.4-0
  libgegl-common libgfortran5 libgimp2.0 libgme0 libgsm1 libheif1 libigdgmm11 libilmbase24
  liblapack3 libmetis5 libmng2 libmypaint-1.5-1 libmypaint-common libopenexr24 libopenmpt0
  libSDL2-2.0-0 libshine3 libsnappy1v5 libssh-gcrypt-4 libswresample3 libswscale5 libumfpack5
  libva-drm2 libva-x11-2 libva2 libvdpau1 libx264-155 libx265-179 libxvidcore4 libzvb1-common
  libzvb10 mesa-va-drivers mesa-vdpau-drivers va-driver-all vdpau-driver-all
Use 'sudo apt autoremove' to remove them.
Suggested packages:
  p7zip-full
The following NEW packages will be installed:
  p7zip
0 upgraded, 1 newly installed, 0 to remove and 0 not upgraded.
Need to get 358 kB of archives.
After this operation, 1,010 kB of additional disk space will be used.
Get:1 http://us.archive.ubuntu.com/ubuntu focal/universe amd64 p7zip amd64 16.02+dfsg-7build1 [358 kB]
Fetched 358 kB in 3s (143 kB/s)
Selecting previously unselected package p7zip.
(Reading database ...
```

input to this VM, move the mouse pointer inside or press Ctrl+G.

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

```
Processing triggers for man-db (2.8.1-1)
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 No 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:

```
drwx----- 2 guru guru 4096 Dec 4 2015 salts
drwx----- 2 guru guru 4096 Dec 4 2015 tables
guru@ubuntu:~/Desktop/hashcat-2.00$ sudo cp hashcat-cli64.bin /usr/bin/
guru@ubuntu:~/Desktop/hashcat-2.00$ sudo unlink /usr/bin//hashcat
guru@ubuntu:~/Desktop/hashcat-2.00$ sudo ln -s /usr/bin/hashcat-cli64.bin /usr/bin/hashcat
guru@ubuntu:~/Desktop/hashcat-2.00$
```

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

```
guru@ubuntu:~/Desktop/hashcat-2.00$ sudo hashcat --help
hashcat, advanced password recovery

Usage: hashcat [options] hashfile [mask|wordfiles|directories]

=====
Options
=====

* General:

-m, --hash-type=NUM      Hash-type, see references below
-a, --attack-mode=NUM    Attack-mode, see references below
-V, --version            Print version
-h, --help              Print help
--quiet                 Suppress output

* Benchmark:

-b, --benchmark          Run benchmark

* Misc:

--hex-salt               Assume salt is given in hex
--hex-charset            Assume charset is given in hex
--runtime=NUM           Abort session after NUM seconds of runtime
--status                Enable automatic update of the status-screen
--status-timer=NUM      Seconds between status-screen update
--status-automat        Display the status view in a machine readable format
```

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`

```
pulse*:18375:0:99999:7::
gnome-initial-setup*:18375:0:99999:7::
gdm*:18375:0:99999:7::
guru:$1$QWDFqQIS30KYnBL5lFdCN6Xe8pPPM.:18394:0:99999:7::
systemd-coredump:!:18394:!!!!:
mysql:!:18564:0:99999:7::
saran:$6$MuXo0dJF0855I71$hcF40du6CS9DXkyQ/vJE82heSboHkozYgY08te.HyJpG002VMSgoT97JhTxoFkE1RtzA92pTbW381MSGsN1.:18603:0:99999:7::
venkat:$6$Ny43BMSEomog2Gh.$WE8kyArLsf4ZMR5xgAZU9V9SkoM5eKrgtsr4XoaNtlq3Uu5caHKwWS.lV4md0B7lHv5SyRjoc9TBtVga8fYJ5.:18603:0:99999:7::
guru@ubuntu:~/Desktop$
```

8. Copy the hash value to a text file

```
guru@ubuntu:~/Desktop$ cat hash.txt
$6$mUax0dJfU08SsI71$hcF40Fdu6CS9DXkyQ/vJE82heSboHkozXyG08te.HyJpG002VMSgoT97jHrTxoFkE1RtzA92pTW381MSGsN1.
$6$Ny43BMSEomog2Gh.$WE8kyArLs4fzMRsXgAZU9V9SkoM5eKRgtsr4XoaNtiq3Uu5caHKWwS.iV4md0B7iHv5SYrj0C9TBLYga8fYJ5.
guru@ubuntu:~/Desktop$
```

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

```

guru@ubuntu:~/desktop/hashcat-2.00$ wget https://raw.githubusercontent.com/danielmiessler/SecLists/master/Passwords/Common-Credentials/10-million-password-list-top-100.txt
--2020-12-07 17:30:12-- https://raw.githubusercontent.com/danielmiessler/SecLists/master/Passwords/Common-Credentials/10-million-password-list-top-100.txt
Resolving raw.githubusercontent.com (raw.githubusercontent.com)... 151.101.36.133
Connecting to raw.githubusercontent.com (raw.githubusercontent.com)[151.101.36.133]:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 754 [text/plain]
Saving to: '10-million-password-list-top-100.txt'

10-million-password-lis 100%[=====] 754 --.-KB/s in 0.002s

2020-12-07 17:30:12 (423 KB/s) - '10-million-password-list-top-100.txt' saved [754/754]

guru@ubuntu:~/desktop/hashcat-2.00$ ls
10-million-password-list-top-100.txt  hashcat-cli32.bin  hashcat-cli64.exe  salts
charsets                             hashcat-cli32.exe  hashcat-clix900.bin  tables
docs                                 hashcat-cli64.app  hashcat-clixop.exe
examples                             hashcat-cli64.bin  rules
guru@ubuntu:~/desktop/hashcat-2.00$

```

10. Create a wordlist consists of users' password

```
guru@ubuntu:~/Desktop$ cat wordlists
guru
saran
admin
1234
8520
gurusaran
venkat
password

guru@ubuntu:~/Desktop$
```

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

```
guru@ubuntu:~/Desktop/hashcat-2.0.9$ 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

```
guru@ubuntu:~/Desktop$ sudo hashcat -m 1800 -a 0 -o cracked.txt hash.txt wordlists
Initializing hashcat v2.00 with 4 threads and 32Mb segment-size...

Skipping line: $1$QwNdfqqI$30KYnBl5lfDcN6Xe8pPPM. (signature unmatched)
Added hashes from file hash.txt: 2 (2 salts)

All hashes have been recovered

Input.Mode: Dict (wordlists)
Index.....: 1/1 (segment), 9 (words), 54 (bytes)
Recovered.: 2/2 hashes, 2/2 salts
Speed/sec.: - plains, - words
Progress...: 8/9 (88.89%)
Running...: 00:00:00:01
Estimated.: --:--:--:--

Started: Mon Dec 7 18:56:04 2020
Stopped: Mon Dec 7 18:56:05 2020
guru@ubuntu:~/Desktop$
```

13. Cracked.txt file contains decrypted passwords

```
guru@ubuntu:~/Desktop$ cat cracked.txt
$6$mUaxOdjFU08SsI71$hcF40Fdu6CS9DXkyQ/vJE82heSboHkozYgY08te.HyJpG002VMSgoT97jHrTxoFkE1RtzA92pTW381MSGsN1.gurusaran
$6$Ny43BMSEomog2Gh.$WE8kyArLs4fzMRsXgAZU9V9SkoM5eKRgtsr4XoaNtiq3Uu5caHKwWS.lV4md0B7iHv55SyRjOC9TBLYga8fYJ5.venkat
guru@ubuntu:~/Desktop$
```