Lab 3 Sample Solution

Task 2

Question 1 Answer: RIPEMD-320

wget https://gitlab.com/kalilinux/packages/hash-identifier/-/raw/kali/master/hash-id.py

root@ip-10-10-3-208:~# python3 hash-id.py

```
 ##########################################################################
 #    __  __                     __      ______          _____           #
 #   /\ \/\ \                   /\ \    /\__  _\ /\  _  `\               #
 #   \ \ \_\ \  __      ____ \ \ \___   \/_/\ \/ \ \ \/\ \              #
 #    \ \  _  \ /'__`\  /',__\ \ \  _ `\    \ \ \  \ \ \ \ \            #
 #     \ \ \ \/\ \_\ \_/\__, `\ \ \ \ \ \    \_\ \__ \ \ \_\ \           #
 #      \ \_\ \_\ \___ \_\/\____/  \ \_\ \_\      /\_____\ \ \____/      #
 #       \/_/\/_/\/__/\/_/\/___/    \/_/\/_/      \/_____/  \/___/ v1.2 #
 #                                                                        #
 #                                                  By Zion3R #           #
 #                                                www.Blackploit.com #    #
 #                                                Root@Blackploit.com #   #
 ##########################################################################

--------------------------------------------------
```

HASH:
741ebf5166b9ece4cca88a3868c44871e8370707cf19af3ceaa4a6fba006f224ae03f39153492853

Possible Hashs:

[+] RipeMD-320

[+] RipeMD-320(HMAC)

Question 2 Answer: SHA2-256

Question 3 Answer: 17800

Question 4 Answer: raw-keccak-256

root@ip-10-10-3-208:~# haiti
1aec7a56aa08b25b596057e1ccbcb6d768b770eaa0f355ccbd56aee5040e02ee
SHA-256 [HC: 1400] [JtR: raw-sha256]
GOST R 34.11-94 [HC: 6900] [JtR: gost]
SHA3-256 [HC: 17400] [JtR: dynamic_380]
Keccak-256 [HC: **17800**] [JtR: **raw-keccak-256**]
Snefru-256 [JtR: snefru-256]
RIPEMD-256 [JtR: dynamic_140]
Haval-256 (3 rounds) [JtR: haval-256-3]
Haval-256 (4 rounds) [JtR: dynamic_290]
Haval-256 (5 rounds) [JtR: dynamic_300]
GOST CryptoPro S-Box
Skein-256 [JtR: skein-256]
Skein-512(256)
PANAMA [JtR: dynamic_320]
BLAKE2-256
MD6-256
Umbraco HMAC-SHA1 [HC: 24800]

Task 3

Question 1:

git clone https://github.com/BlackArch/wordlistctl.git

python3 wordlistctl/wordlistctl.py -h

python3 wordlistctl/wordlistctl.py search rockyou

Question 2 Answer: -l

python3 wordlistctl/wordlistctl.py search -h

Task 3 Answer: /usr/share/wordlists/rockyou.txt

python3 wordlistctl/wordlistctl.py search -l rockyou

Task 4 Answer: UserPassJay

python3 wordlistctl/wordlistctl.py list -g usernames

Task 4

Question 1:

locate john.conf

Question 2:

locate 10k-most-common.txt

Create a new file *john-local.conf* and add the following:

[List.Rules:THM01]
$[0-9]$[0-9]

Question 3 Answer: moonligh56

john task4_hashes/hash1.txt --show --format=raw-md5

john hash.txt --show --format=raw-sha1

Task 5

Question 1:

root@ip-10-10-3-208:~# python3 wordlistctl/wordlistctl.py fetch -l dogs -d dogs

root@ip-10-10-3-208:~# python3 wordlistctl/wordlistctl.py search -l dogs
--==[wordlistctl by blackarch.org]==--

> /usr/share/wordlists/misc/dogs.txt (2.41 Kb)

Question 2 Answer: information

cewl -d 2 -w $(pwd)/example.txt https://example.org
vim example.txt

Questions 3- 5: run the given commands

Question 6 Answer: 1551-li

It is an md5 hash (use https://www.tunnelsup.com/hash-analyzer/ to find that out)

john --format=raw-md5 --wordlist=combination.txt hash.txt

john hash2.txt --show --format=raw-md5

Task 6

John Rules:

[List.Rules:rules01]
c$[0-9]$[0-9]$[$%&*-_+=#@~!]
cA0”[0-9!@#$%^&*()_+]”
cAz”[0-9!@#$%^&*()_+]”

[List.Rules:rules02]
c$1$2$3$4$[$%&*-_+=#@~!]

[List.Rules:rules03]
r

[List.Rules:rules04]
d
dd
ddd
dddd

Question 1

john hash.txt --format=raw-md5
--wordlist=/usr/share/wordlists/misc/top_1000_usa_malenames_english.txt --rules=rules02

Question 2

john hash.txt --format=raw-md5
--wordlist=/usr/share/wordlists/misc/top_1000_usa_femalenames_english.txt --rules=rules01

Question 3

echo 'davidguettapan' > name.txt
john hash.txt --format=Raw-SHA1 --wordlist=name.txt --rules=NT

OR use rules04 from above