CYSE 270: Linux System for Cybersecurity

Assignment: Lab 5 – Password cracking

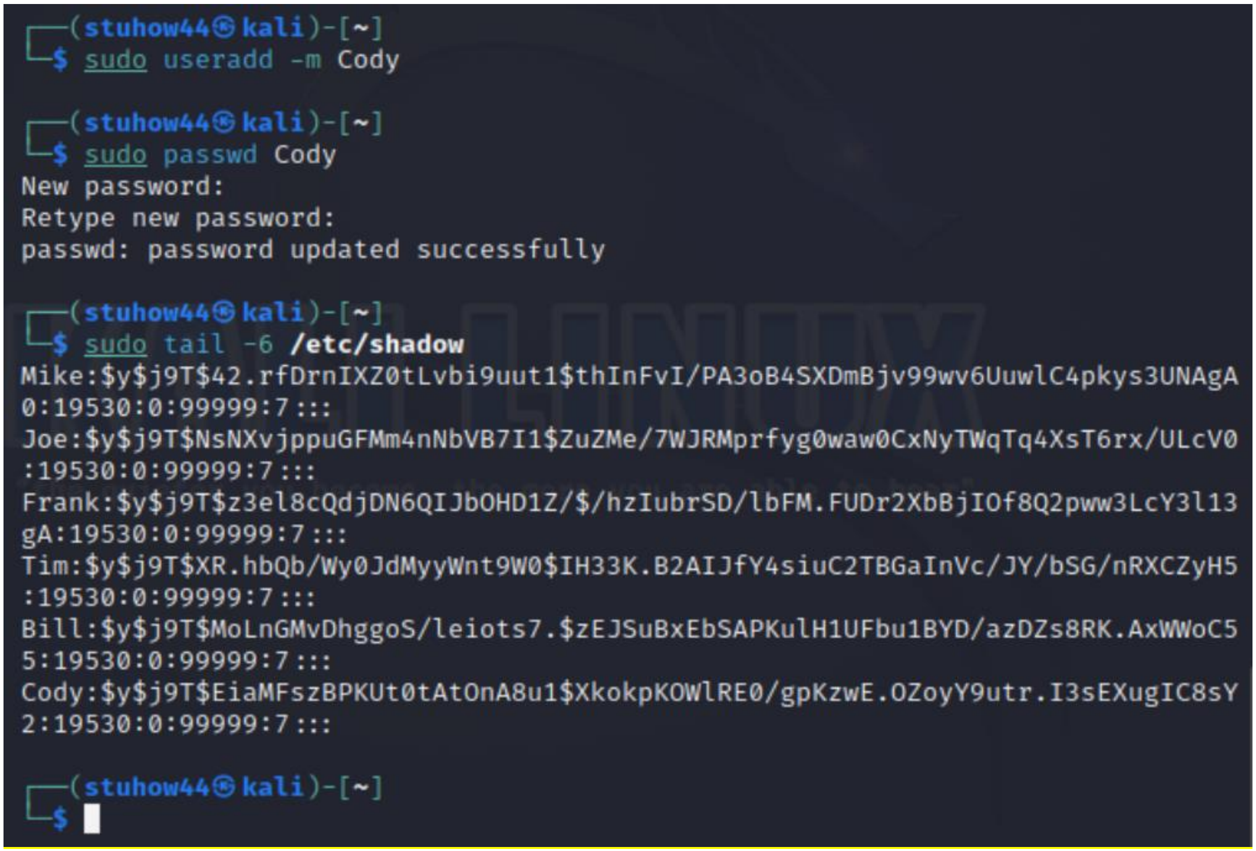
CYSE 270: Linux System for Cybersecurity

The goal of this lab is to test the strength of different passwords.

Task A – Password Cracking

1. Create 6 users in your Linux system, then assign each user a password that meets the following complexity requirement respectively. You should list the passwords created for each user. **[6 * 5 = 30 points]**

1. A simple dictionary word (all lowercase)
2. 4-character digits
3. A simple dictionary word (all lowercase) + digits
4. A simple dictionary word (all lowercase) + digits +symbols
5. A simple dictionary word (all lowercase) + digits
6. A simple dictionary word (w. a mix of lower and upper case) + digits +symbols



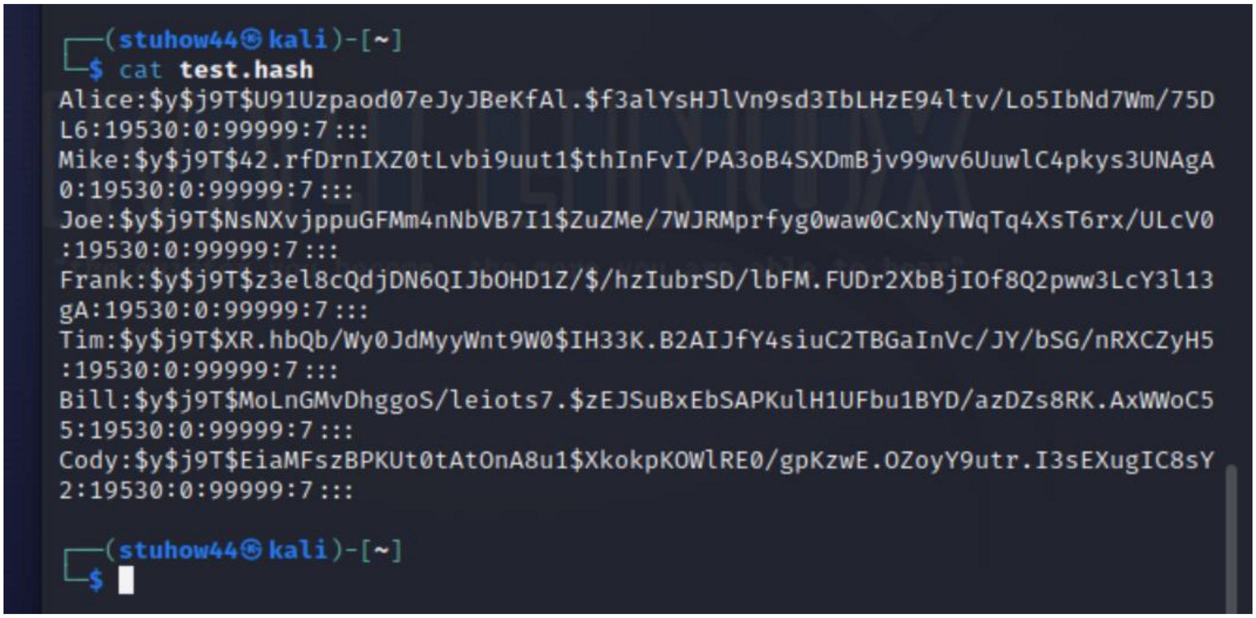
```
┌──(stuhow44㉿kali)-[~]
└─$ sudo useradd -m Cody

┌──(stuhow44㉿kali)-[~]
└─$ sudo passwd Cody
New password:
Retype new password:
passwd: password updated successfully

┌──(stuhow44㉿kali)-[~]
└─$ sudo tail -6 /etc/shadow
Mike:$y$j9T$42.rfDrnIXZ0tLvbi9uut1$thInFvI/PA3oB4SXDmBjv99wv6UuwlC4pkys3UNAgA
0:19530:0:99999:7:::
Joe:$y$j9T$NsNXvjppuGFMm4nNbVB7I1$ZuZMe/7WJRMprfyg0waw0CxNyTWqTq4XsT6rx/ULcV0
:19530:0:99999:7:::
Frank:$y$j9T$z3el8cQdjDN6QIJbOHD1Z/$/hzIubrSD/lbFM.FUDr2XbBjIOf8Q2pww3LcY3l13
gA:19530:0:99999:7:::
Tim:$y$j9T$XR.hbQb/Wy0JdMyyWnt9W0$IH33K.B2AIJfY4siuC2TBGaInVc/JY/bSG/nRXCZyH5
:19530:0:99999:7:::
Bill:$y$j9T$MoLnGMvDhggoS/leiots7.$zEJSuBxEbSAPKulH1UFbu1BYD/azDZs8RK.AxWWoC5
5:19530:0:99999:7:::
Cody:$y$j9T$EiaMFszBPKUt0tAtOnA8u1$XkokpKOWlRE0/gpKzwE.OZoyY9utr.I3sEXugIC8sY
2:19530:0:99999:7:::

┌──(stuhow44㉿kali)-[~]
└─$ █
```

2. Export above users' hash into a file named test.hash (replace xxx with your MIDAS ID) and use

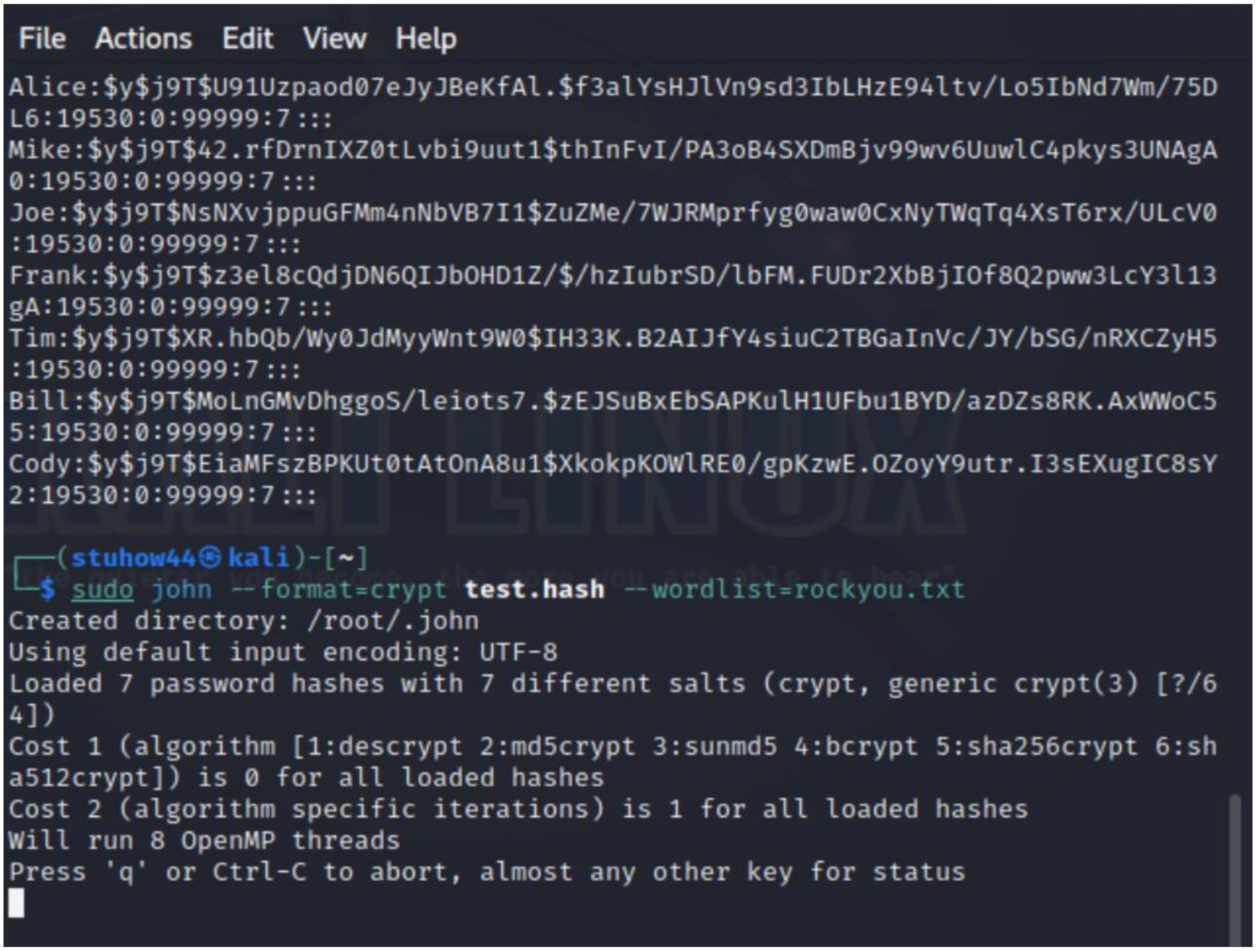


```
┌──(stuhow44㉿kali)-[~]
└─$ cat test.hash
Alice:$y$j9T$U91Uzpaod07eJyJBeKfAl.$f3alYsHJlVn9sd3IbLHzE94ltv/Lo5IbNd7Wm/75D
L6:19530:0:99999:7:::
Mike:$y$j9T$42.rfDrnIXZ0tLvbi9uut1$thInFvI/PA3oB4SXDmBjv99wv6UuwlC4pkys3UNAgA
0:19530:0:99999:7:::
Joe:$y$j9T$NsNXvjppuGFMm4nNbVB7I1$ZuZMe/7WJRMprfyg0waw0CxNyTWqTq4XsT6rx/ULcV0
:19530:0:99999:7:::
Frank:$y$j9T$z3el8cQdjDN6QIJbOHD1Z/$/hzIubrSD/lbFM.FUDr2XbBjIOf8Q2pww3LcY3l13
gA:19530:0:99999:7:::
Tim:$y$j9T$XR.hbQb/Wy0JdMyyWnt9W0$IH33K.B2AIJfY4siuC2TBGaInVc/JY/bSG/nRXCZyH5
:19530:0:99999:7:::
Bill:$y$j9T$MoLnGMvDhggoS/leiots7.$zEJSuBxEbSAPKulH1UFbu1BYD/azDZs8RK.AxWWoC5
5:19530:0:99999:7:::
Cody:$y$j9T$EiaMFszBPKUt0tAtOnA8u1$XkokpKOWlRE0/gpKzwE.OZoyY9utr.I3sEXugIC8sY
2:19530:0:99999:7:::

┌──(stuhow44㉿kali)-[~]
└─$ █
```

John the Ripper to crack their passwords in wordlist mode (use rockyou.txt). **[40 points]** 3.

Keep your john the ripper cracking for at least 10 minutes. How many passwords have been successfully cracked? [30 points]



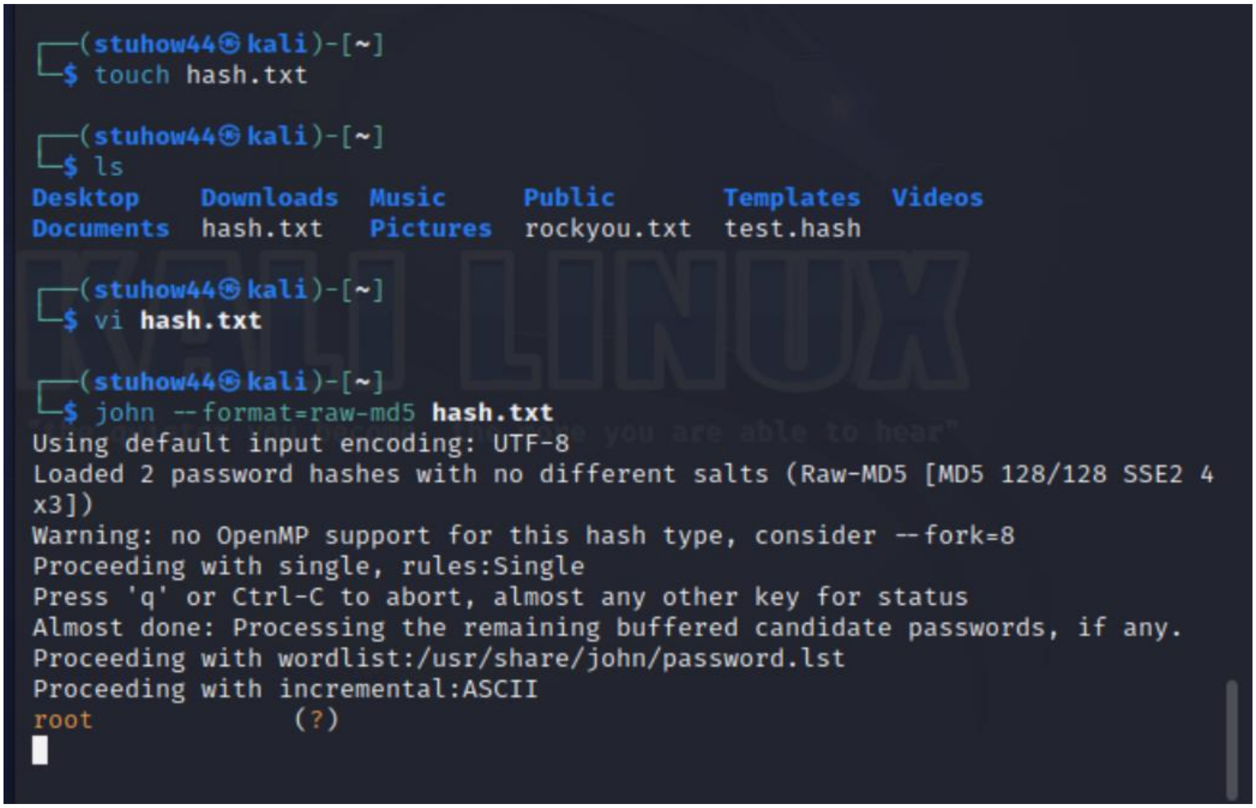
```
Alice:$y$j9T$U91Uzpaod07eJyJBeKfAl.$f3alYsHJlVn9sd3IbLHzE94ltv/Lo5IbNd7Wm/75D
L6:19530:0:99999:7:::
Mike:$y$j9T$42.rfDrnIXZ0tLvbi9uut1$thInFvI/PA3oB4SXDmBjv99wv6UuwlC4pkys3UNAgA
0:19530:0:99999:7:::
Joe:$y$j9T$NsNXvjppuGFMm4nNbVB7I1$ZuZMe/7WJRMprfyg0waw0CxNyTWqTq4XsT6rx/ULcV0
:19530:0:99999:7:::
Frank:$y$j9T$z3el8cQdjDN6QIJbOHD1Z/$/hzIubrSD/lbFM.FUDr2XbBjIOf8Q2pww3LcY3l13
gA:19530:0:99999:7:::
Tim:$y$j9T$XR.hbQb/Wy0JdMyyWnt9W0$IH33K.B2AIJfY4siuC2TBGaInVc/JY/bSG/nRXCZyH5
:19530:0:99999:7:::
Bill:$y$j9T$MoLnGMvDhggoS/leiots7.$zEJSuBxEbSAPKulH1UFbu1BYD/azDZs8RK.AxWWoC5
5:19530:0:99999:7:::
Cody:$y$j9T$EiaMFszBPKUt0tAtOnA8u1$XkokpKOWlRE0/gpKzwE.OZoyY9utr.I3sEXugIC8sY
2:19530:0:99999:7:::

┌──(stuhow44㉿kali)-[~]
└─$ sudo john --format=crypt test.hash --wordlist=rockyou.txt
Created directory: /root/.john
Using default input encoding: UTF-8
Loaded 7 password hashes with 7 different salts (crypt, generic crypt(3) [?/6
4])
Cost 1 (algorithm [1:descrypt 2:md5crypt 3:sunmd5 4:bcrypt 5:sha256crypt 6:sh
a512crypt]) is 0 for all loaded hashes
Cost 2 (algorithm specific iterations) is 1 for all loaded hashes
Will run 8 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
█
```

Extra credit (10 points):

1. Find and use the proper format in John the ripper to crack the following MD5 hash. Show your steps and results.

- 5f4dcc3b5aa765d61d8327deb882cf99
- 63a9f0ea7bb98050796b649e85481845



```
┌──(stuhow44㉿kali)-[~]
└─$ touch hash.txt

┌──(stuhow44㉿kali)-[~]
└─$ ls
Desktop    Downloads  Music     Public      Templates  Videos
Documents  hash.txt   Pictures  rockyou.txt test.hash

┌──(stuhow44㉿kali)-[~]
└─$ vi hash.txt

┌──(stuhow44㉿kali)-[~]
└─$ john --format=raw-md5 hash.txt
Using default input encoding: UTF-8
Loaded 2 password hashes with no different salts (Raw-MD5 [MD5 128/128 SSE2 4
x3])
Warning: no OpenMP support for this hash type, consider --fork=8
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
Proceeding with incremental:ASCII
root             (?)
█
```

- Create a file containing the MD5 hashes you want to crack called "hash.txt"
- add the hashes manually using the vi editor:
  - Open the hashes.txt file using the vi editor:
  - Press the "i" key to enter the insert mode in vi.
  - Manually type in the hashes in the file, one per line.
  - Press the "Esc" key to exit the insert mode.
  - wq and press Enter to save the changes and exit vi.
- Use John the Ripper to crack the hash