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 Terminal, then set the password for each user that meets the following complexity requirement respectively. You should list the passwords created for each user. **[6 * 5 = 30 points]**.
    1. For user1, the password should be a simple dictionary word (all lowercase)

       A: (pebbles)
    2. For user2, the password should consist of 4 digits.

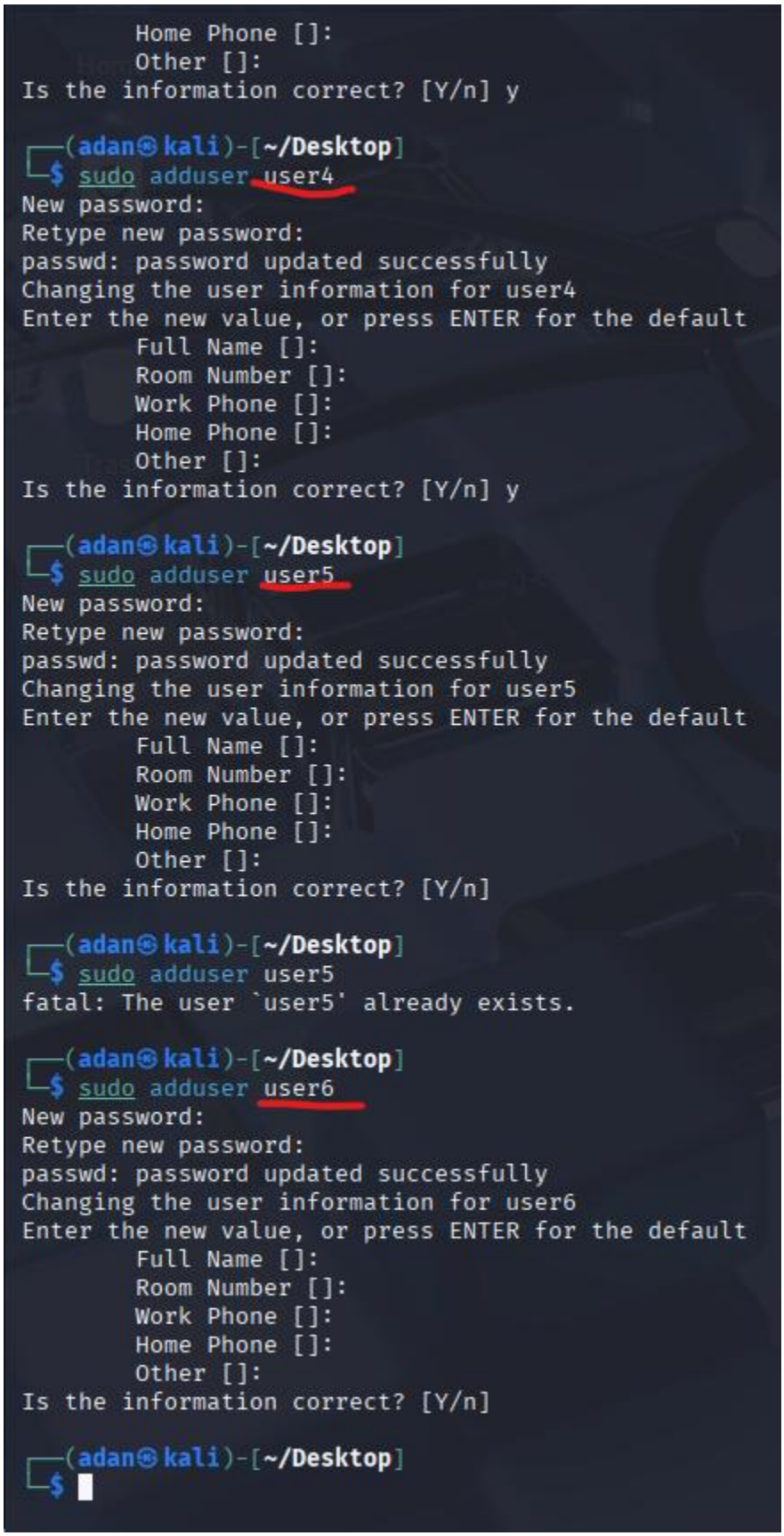
    A: (1234)
    3. For user3, the password should consist of a simple dictionary word of any length characters (all lowercase) + digits.

    A: (catfish99)
    4. For user4, the password should consist of a simple dictionary word characters (all lowercase) + digits + symbols.

    A: (barn25!)
    5. For user5, the password should consist of a simple dictionary word (all lowercase) + digits.

    A: (truck60)
    6. For user6, the password should consist of a simple dictionary word (with a combination of lower and upper case) + digits + symbols.

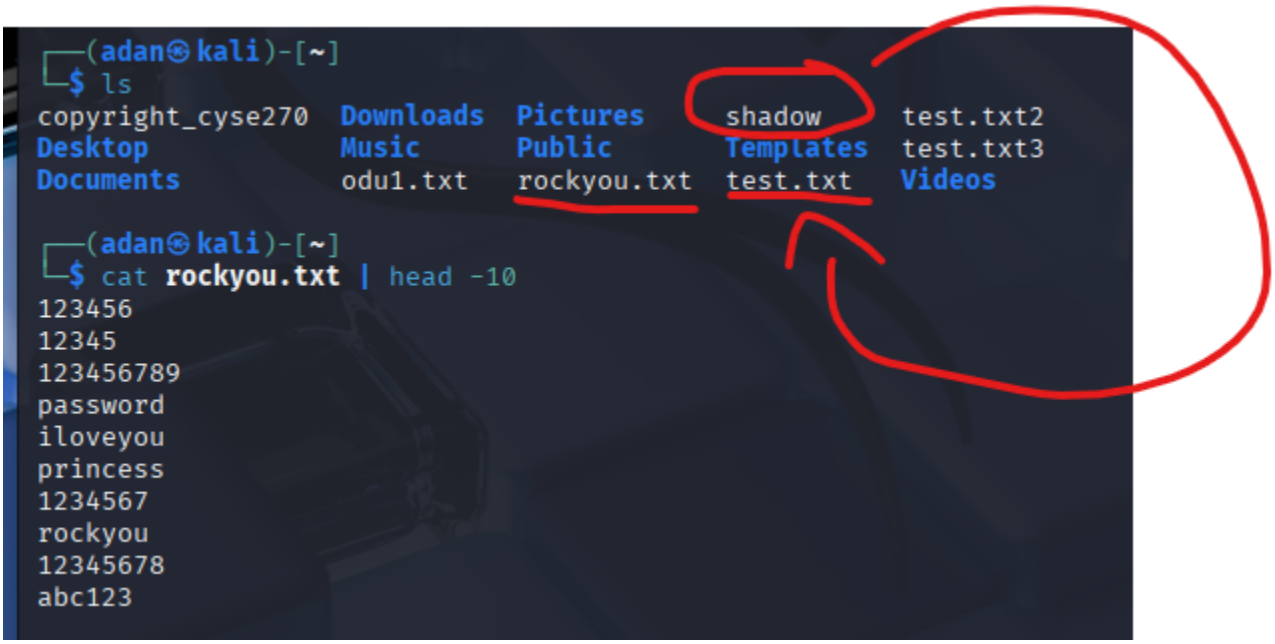
    A: (RedFishspace99!)



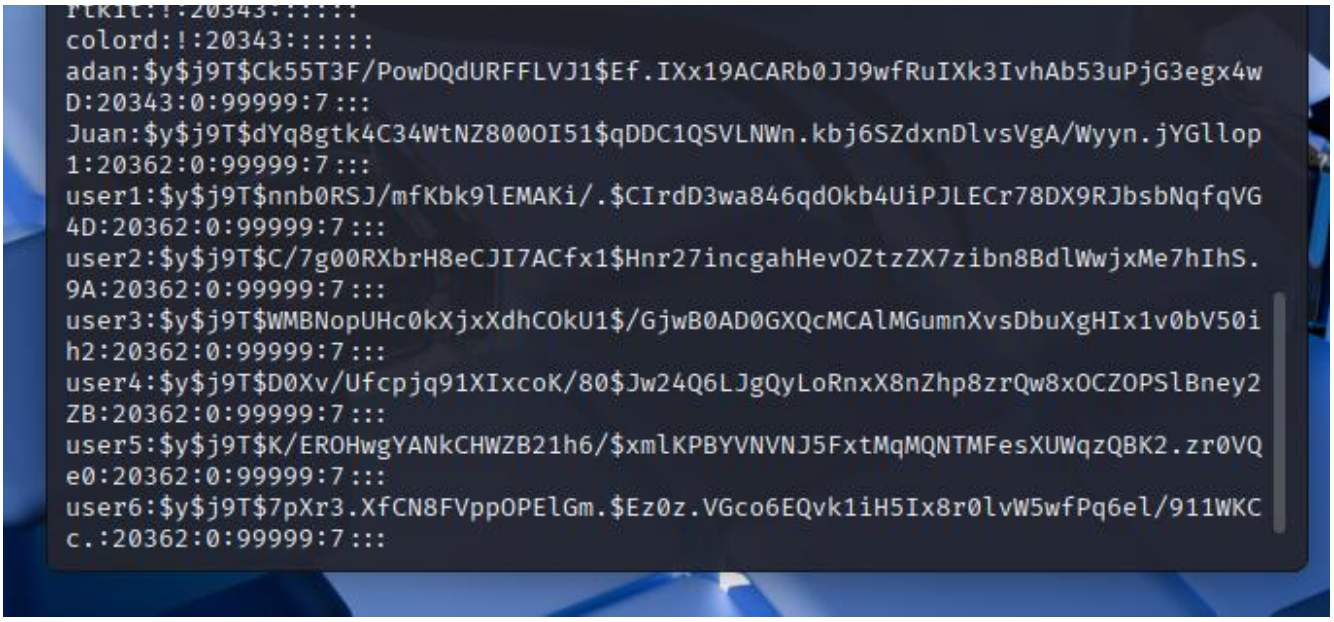
Remember, do not use the passwords for your real-world accounts.

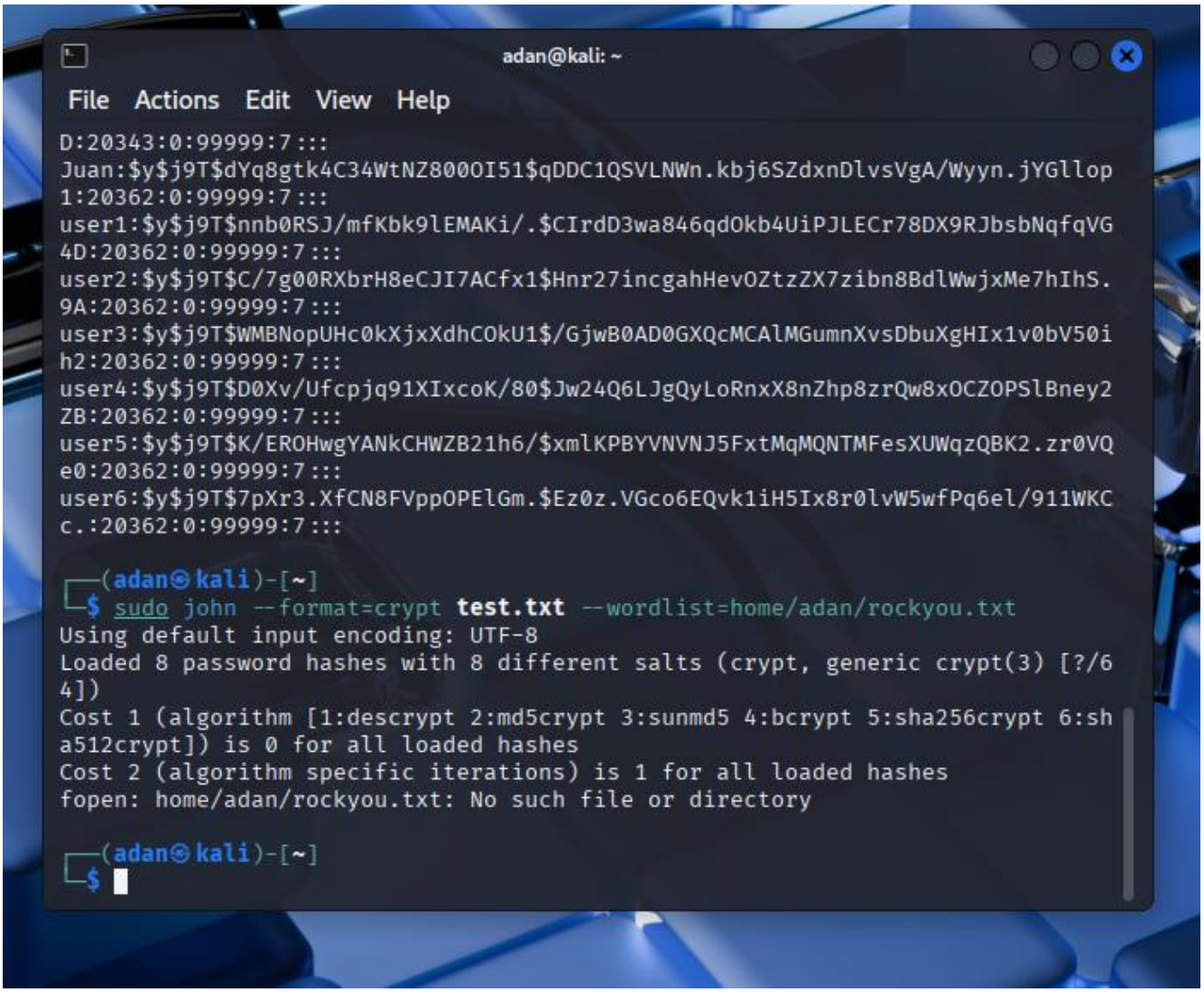
2. Export above users' hashes into a file named **xxx.hash** **(replace xxx with your MIDAS name)** and use John the Ripper tool to crack their passwords in wordlist mode (use rockyou.txt). **[40 points]**

I had many problems with this step and I tried many things to fix it. I will reach out for help. I am confused on why this does not work. I have done this before in other classes. So I am familiar with password cracking. Everything is in the home directory.



The shadow directory was moved to my home directory into "test.txt". I have the rockyou.txt un zip in the home directory. I showed proof of me reading each file. One has the password and the other has the hashes.


colord:!:20343::::::
adan:yj9T$Ck55T3F/PowDQdURFFLVJ1$Ef.IXx19ACARb0JJ9wfRuIXk3IvhAb53uPjG3egx4w
D:20343:0:99999:7:::
Juan:yj9T$dYq8gtk4C34WtNZ800OI51$qDDC1QSVLNWn.kbj6SZdxnDlvsVgA/Wyyn.jYGllop
1:20362:0:99999:7:::
user1:yj9T$nnb0RSJ/mfKbk9lEMAKi/.$CIrdD3wa846qdOkb4UiPJLECr78DX9RJbsbNqfqVG
4D:20362:0:99999:7:::
user2:yj9T$C/7g00RXbrH8eCJI7ACfx1$Hnr27incgahHevOZtzZX7zibn8BdlWwjxMe7hIhS.
9A:20362:0:99999:7:::
user3:yj9T$WMBNopUHc0kXjxXdhCOkU1$/GjwB0AD0GXQcMCAlMGumnXvsDbuXgHIx1v0bV50i
h2:20362:0:99999:7:::
user4:yj9T$D0Xv/Ufcpjq91XIxcoK/80$Jw24Q6LJgQyLoRnxX8nZhp8zrQw8xOCZOPSlBney2
ZB:20362:0:99999:7:::
user5:yj9T$K/EROHwgYANkCHWZB21h6/$xmlKPBYVNVNJ5FxtMqMQNTMFesXUWqzQBK2.zr0VQ
e0:20362:0:99999:7:::
user6:yj9T$7pXr3.XfCN8FVppOPElGm.$Ez0z.VGco6EQvk1iH5Ix8r0lvW5wfPq6el/911WKC
c.:20362:0:99999:7:::


adan@kali: ~
File Actions Edit View Help
D:20343:0:99999:7:::
Juan:yj9T$dYq8gtk4C34WtNZ800OI51$qDDC1QSVLNWn.kbj6SZdxnDlvsVgA/Wyyn.jYGllop
1:20362:0:99999:7:::
user1:yj9T$nnb0RSJ/mfKbk9lEMAKi/.$CIrdD3wa846qdOkb4UiPJLECr78DX9RJbsbNqfqVG
4D:20362:0:99999:7:::
user2:yj9T$C/7g00RXbrH8eCJI7ACfx1$Hnr27incgahHevOZtzZX7zibn8BdlWwjxMe7hIhS.
9A:20362:0:99999:7:::
user3:yj9T$WMBNopUHc0kXjxXdhCOkU1$/GjwB0AD0GXQcMCAlMGumnXvsDbuXgHIx1v0bV50i
h2:20362:0:99999:7:::
user4:yj9T$D0Xv/Ufcpjq91XIxcoK/80$Jw24Q6LJgQyLoRnxX8nZhp8zrQw8xOCZOPSlBney2
ZB:20362:0:99999:7:::
user5:yj9T$K/EROHwgYANkCHWZB21h6/$xmlKPBYVNVNJ5FxtMqMQNTMFesXUWqzQBK2.zr0VQ
e0:20362:0:99999:7:::
user6:yj9T$7pXr3.XfCN8FVppOPElGm.$Ez0z.VGco6EQvk1iH5Ix8r0lvW5wfPq6el/911WKC
c.:20362:0:99999:7:::
┌──(adan㉿kali)-[~]
└─$ sudo john --format=crypt test.txt --wordlist=home/adan/rockyou.txt
Using default input encoding: UTF-8
Loaded 8 password hashes with 8 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
fopen: home/adan/rockyou.txt: No such file or directory
┌──(adan㉿kali)-[~]
└─$

I finally run john to crack the passwords, and this is all I get. Is the path to rockyou.txt not correct? It's in my home directory so I am confused. I know I have the right idea, but it is not executing.

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

CYSE 270: Linux System for Cybersecurity

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.
    a. 5f4dcc3b5aa765d61d8327deb882cf99
    b. 63a9f0ea7bb98050796b649e85481845