CYSE 270: Linux System for Cybersecurity

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]**.

james, steve, trevor, josh, william, ryan

1. For user1, the password should be a simple dictionary word (all lowercase)

   orange

2. For user2, the password should consist of 4 digits.

   1234

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

   orange123

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

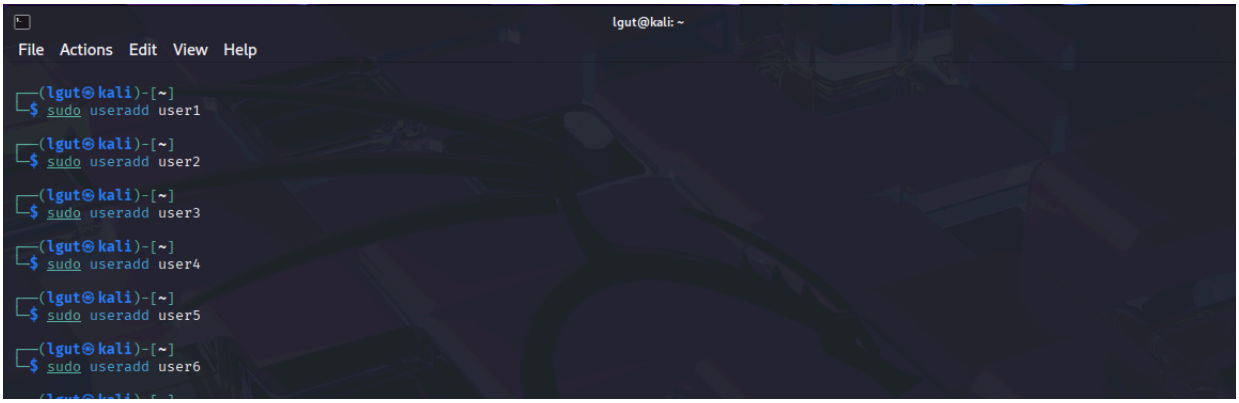
   orange123$

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

   blue123

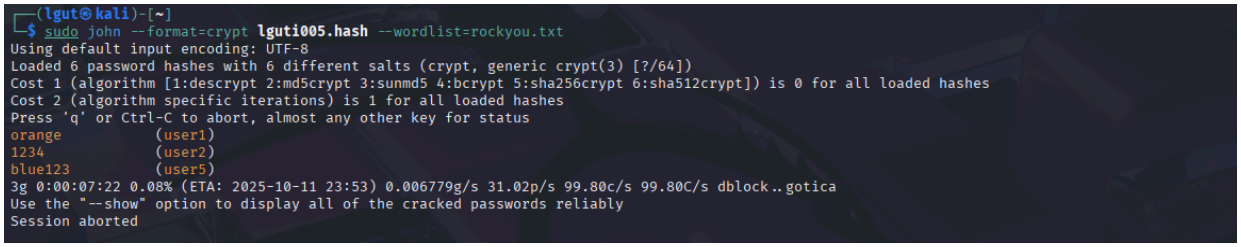
6. For user6, the password should consist of a simple dictionary word (with a combination of lower and upper case) + digits + symbols.

Blue123$



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]**



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

3 passwords were cracked in the timespan. User1, user2, and user5 were cracked.

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

I attempted to crack it but I could not figure it out.