

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

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

Blue123\$

```
lgut@kali: ~  
File Actions Edit View Help  
[lgut@kali]~$ sudo useradd user1  
[lgut@kali]~$ sudo useradd user2  
[lgut@kali]~$ sudo useradd user3  
[lgut@kali]~$ sudo useradd user4  
[lgut@kali]~$ sudo useradd user5  
[lgut@kali]~$ sudo useradd user6
```

```
[lgut@kali]~$ sudo passwd user1  
New password:  
Retype new password:  
passwd: password updated successfully  
[lgut@kali]~$ sudo passwd user2  
New password:  
Retype new password:  
passwd: password updated successfully  
[lgut@kali]~$ sudo passwd user3  
New password:  
Retype new password:  
passwd: password updated successfully  
[lgut@kali]~$ sudo passwd user4  
New password:  
Retype new password:  
passwd: password updated successfully  
[lgut@kali]~$ sudo passwd user5  
New password:  
Retype new password:  
passwd: password updated successfully  
[lgut@kali]~$ sudo passwd user6  
New password:  
Retype new password:  
passwd: password updated successfully  
[lgut@kali]~$
```

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]**

```
lgut@kali: ~
File Actions Edit View Help
(lgut@kali)-[~]
└─$ sudo cat /etc/shadow | grep 'user[1-6]' > ~/lguti005.hash
(lgut@kali)-[~]
└─$
```

```
(lgut@kali)-[~]
└─$ sudo john --format=crypt lguti005.hash --wordlist=rockyou.txt
Using default input encoding: UTF-8
Loaded 6 password hashes with 6 different salts (crypt, generic crypt(3) [?/64])
Cost 1 (algorithm [1:descrypt 2:md5crypt 3:sunmd5 4:bcrypt 5:sha256crypt 6:sha512crypt]) is 0 for all loaded hashes
Cost 2 (algorithm specific iterations) is 1 for all loaded hashes
Press 'q' or Ctrl-C to abort, almost any other key for status
orange (user1)
1234 (user2)
blue123 (user5)
3g 0:00:07:22 0.08% (ETA: 2025-10-11 23:53) 0.006779g/s 31.02p/s 99.80c/s 99.80C/s dblock..gotica
Use the "--show" option to display all of the cracked passwords reliably
Session aborted
```

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):

- Find and use the proper format in John the ripper to crack the following **MD5 hash**. Show your steps and results.
 - 5f4dcc3b5aa765d61d8327deb882cf99
 - 63a9f0ea7bb98050796b649e85481845

Logan Gutierrez

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