CYSE 270: Linux System for Cybersecurity

Jade Ames Moore

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)

       First Step: sudo is to have the admin permission, useradd adds the user, user 1 is the user.

       Second Step: Sudo is the admin permission, passwd is to create a password for the user, user 1 is the user for the password.

       (Covers all Users)

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

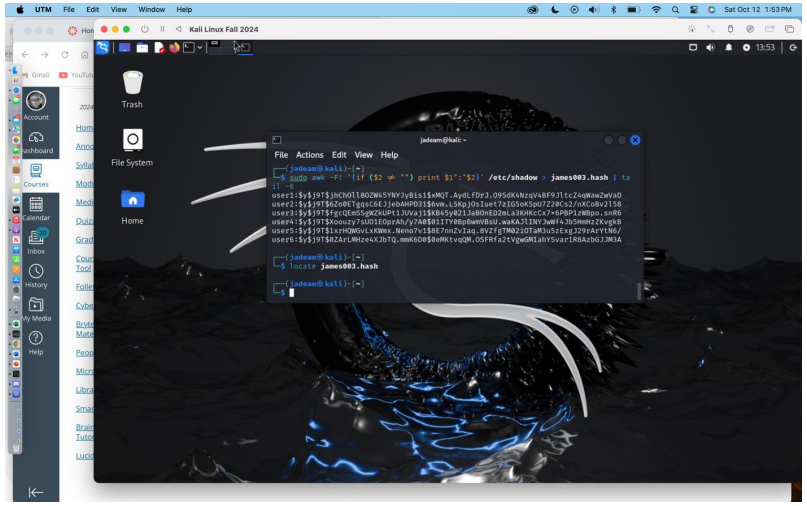
    3. For user3, the password should consist of a simple dictionary word of any length characters (all lowercase) + digits.
    4. For user4, the password should consist of a simple dictionary word characters (all lowercase) + digits + symbols.

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

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

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]**

The ones that we're cracked were the more basic and easy password with no symbol and capitalizing letter put together.
This goes to show that basic and easy to remember passwords are not the best for security.