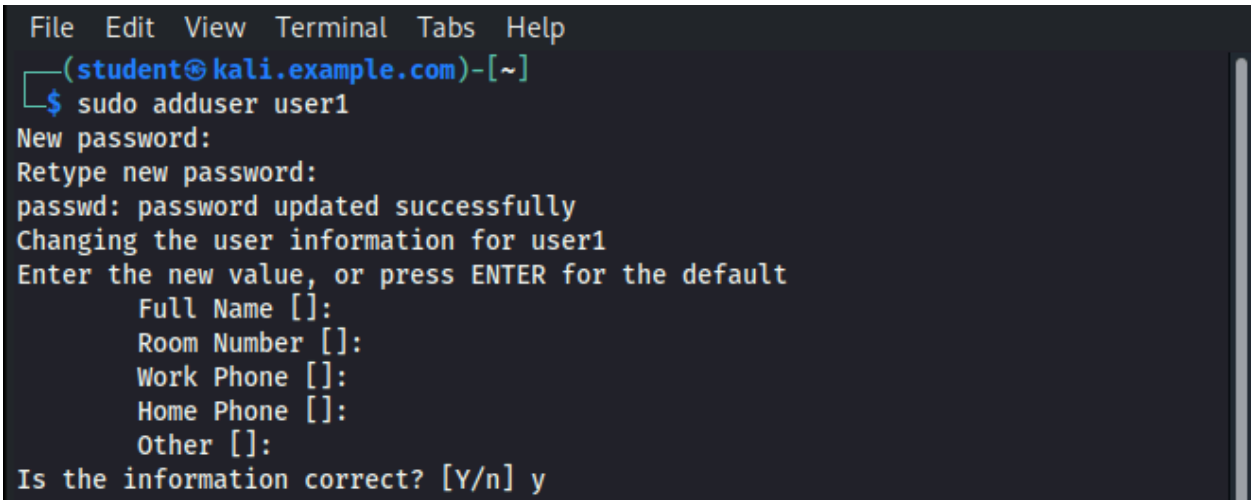
Bryce Baxter

10/4/25

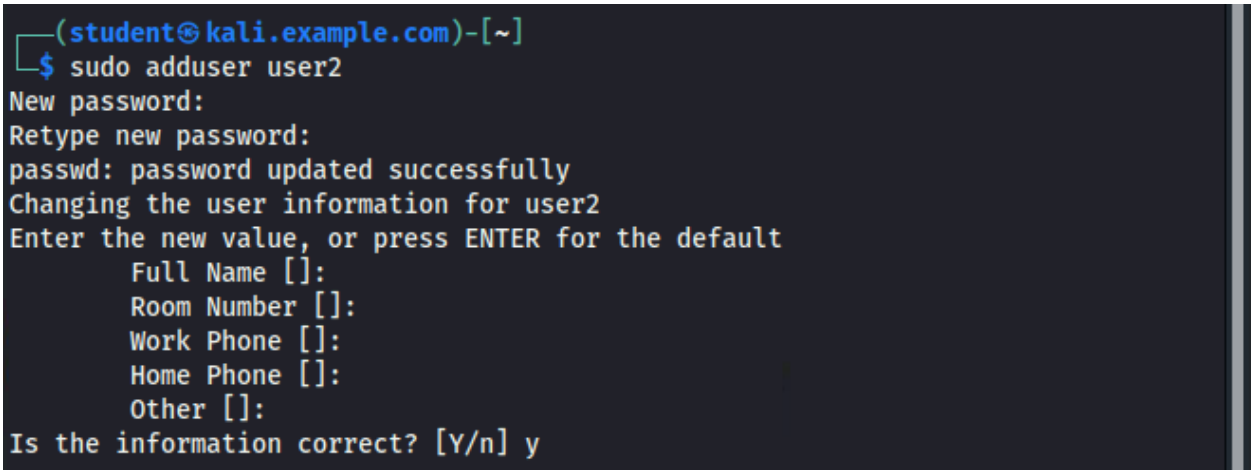
CYSE 270

Lab 5 – Password Cracking

Step 1 – user1 password: **apple**



Step 2 – user2 password: **1234**



Step 3 – user3 password: **banana123**

```
┌──(student㉿kali.example.com)-[~]
└─$ sudo adduser user3
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for user3
Enter the new value, or press ENTER for the default
        Full Name []:
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:
Is the information correct? [Y/n] y
```

Step 4 – user4 password: **orange45!**

```
┌──(student㉿kali.example.com)-[~]
└─$ sudo adduser user4
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for user4
Enter the new value, or press ENTER for the default
        Full Name []:
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:
Is the information correct? [Y/n] y
```

Step 5 – user5 password: **grape789**

```
┌──(student㉿kali.example.com)-[~]
└─$ sudo adduser user5
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for user5
Enter the new value, or press ENTER for the default
        Full Name []:
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:
Is the information correct? [Y/n] y
```

Step 6 – user6 password: **Mango123@**

```
┌──(student㉿kali.example.com)-[~]
└─$ sudo adduser user6
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for user6
Enter the new value, or press ENTER for the default
        Full Name []:
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:
Is the information correct? [Y/n] y
```

Step 7: Moved passwords into **01294121.hash** file and using John the Ripper

```
┌──(student㉿kali.example.com)-[~]
└─$ sudo unshadow /etc/passwd /etc/shadow > 01294121.hash
Created directory: /root/.john
```

```
┌──(student㉿kali.example.com)-[~]
└─$ sudo gunzip /usr/share/wordlists/rockyou.txt.gz
```

Step 8

```
┌──(student㉿kali.example.com)-[~]
└─$ sudo john --format=crypt 01294121.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:sha51
2crypt]) is 0 for all loaded hashes
Cost 2 (algorithm specific iterations) is 1 for all loaded hashes
Will run 2 OpenMP threads
```

EXTRA CREDIT:

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

┌──(student㉿kali.example.com)-[~]
└─$ ls
01294121.hash  Public                  data           hash.txt
Desktop        Templates               demo.txt       input.txt
Documents      Videos                  demo.txt.gz    practice_folder
Downloads      archive.tar             filename.txt
Music          copyright               filname.txt
Pictures       copyright_cyse270.txt   groupfile.txt

┌──(student㉿kali.example.com)-[~]
└─$ vi hash.txt
```

```
┌──(student㉿kali.example.com)-[~]
└─$ john --format=raw-md5 hash.txt
Using default input encoding: UTF-8
Loaded 2 password hashes with no different salts (Raw-MD5 [MD5 512/512 AVX512BW
16x3])
Warning: no OpenMP support for this hash type, consider --fork=2
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
password         (?)
Proceeding with incremental:ASCII
root             (?)
2g 0:00:00:01 DONE 3/3 (2025-10-04 16:01) 1.015g/s 2857Kp/s 2857Kc/s 2857KC/s 01
02000101..rams
Use the "--show --format=Raw-MD5" options to display all of the cracked password
s reliably
Session completed.
```