Ava McLaughlin

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

Ava McLaughlin

CYSE 270: Linux System for Cybersecurity

Extra credit (10 points):

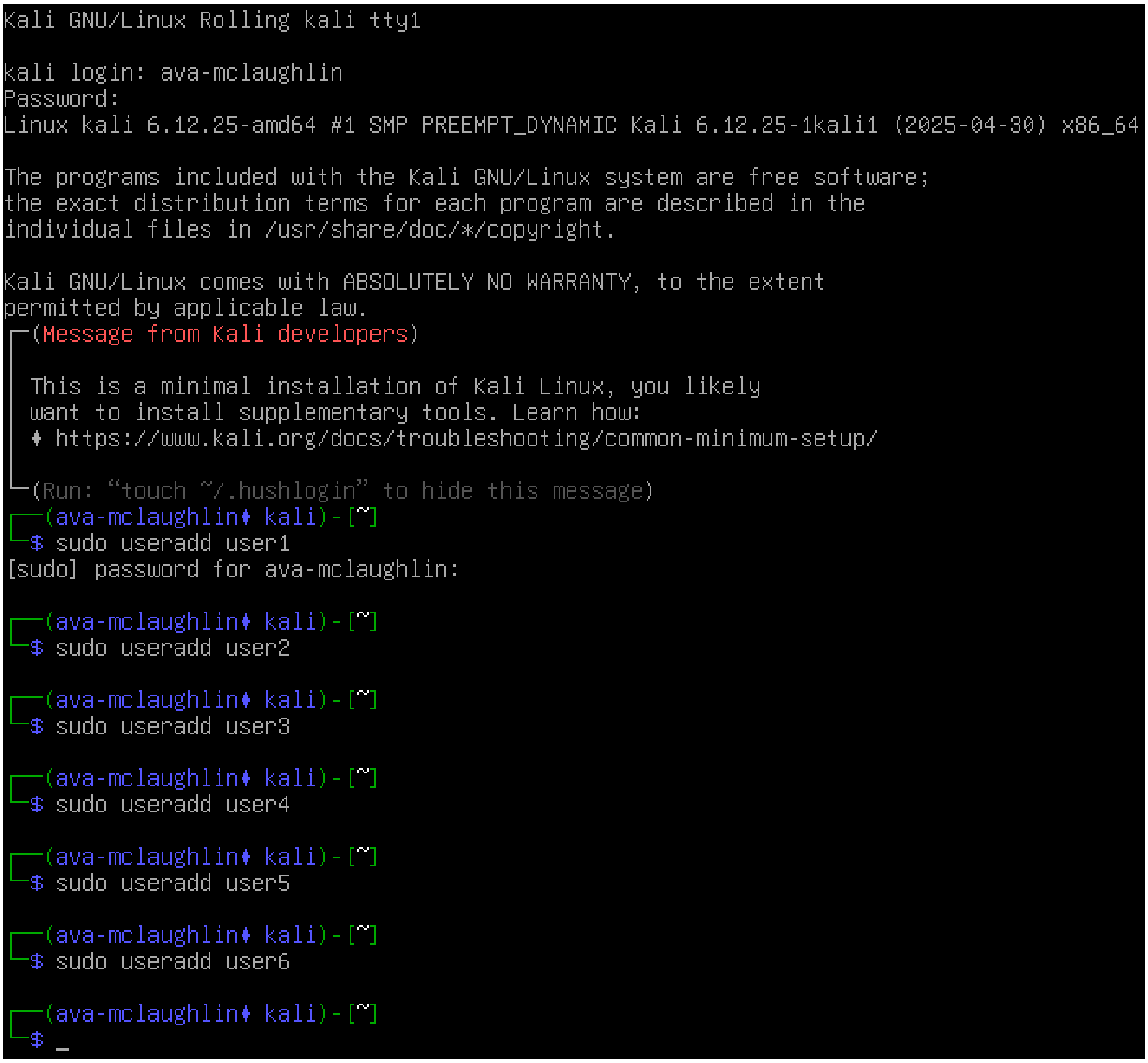
1. Find and use the proper format in John the ripper to crack the following **MD5 hash**.

Show your steps and results.

a. 5f4dcc3b5aa765d61d8327deb882cf99

b. 63a9f0ea7bb98050796b649e85481845

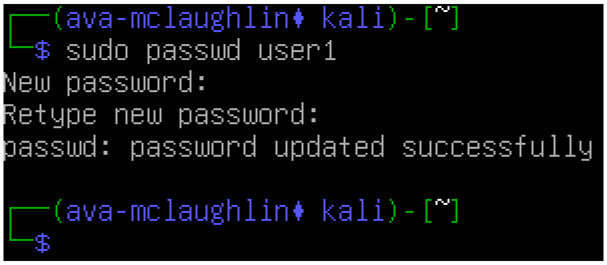
Step 1:



```
Kali GNU/Linux Rolling kali tty1

kali login: ava-mclaughlin
Password:
Linux kali 6.12.25-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.12.25-1kali1 (2025-04-30) x86_64

The programs included with the Kali GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
┌(Message from Kali developers)
│
│ This is a minimal installation of Kali Linux, you likely
│ want to install supplementary tools. Learn how:
│ ⇒ https://www.kali.org/docs/troubleshooting/common-minimum-setup/
│
└(Run: "touch ~/.hushlogin" to hide this message)
┌──(ava-mclaughlin⧫ kali)-[~]
└─$ sudo useradd user1
[sudo] password for ava-mclaughlin:

┌──(ava-mclaughlin⧫ kali)-[~]
└─$ sudo useradd user2

┌──(ava-mclaughlin⧫ kali)-[~]
└─$ sudo useradd user3

┌──(ava-mclaughlin⧫ kali)-[~]
└─$ sudo useradd user4

┌──(ava-mclaughlin⧫ kali)-[~]
└─$ sudo useradd user5

┌──(ava-mclaughlin⧫ kali)-[~]
└─$ sudo useradd user6

┌──(ava-mclaughlin⧫ kali)-[~]
└─$ _
```

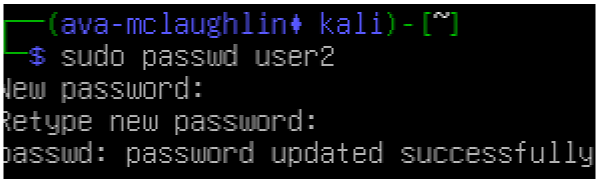
Ava McLaughlin

Step 1.1: Password used: princess



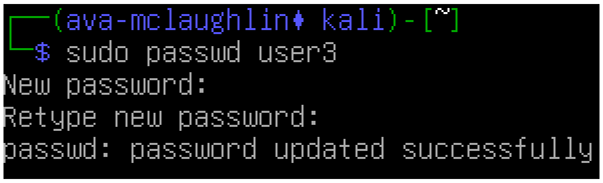
```
┌──(ava-mclaughlin㉿kali)-[~]
└─$ sudo passwd user1
New password:
Retype new password:
passwd: password updated successfully

┌──(ava-mclaughlin㉿kali)-[~]
└─$
```

Step 1.2: Password used: 9876



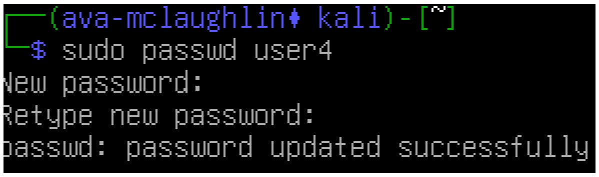
```
┌──(ava-mclaughlin㉿kali)-[~]
└─$ sudo passwd user2
New password:
Retype new password:
passwd: password updated successfully
```

Step 1.3: Password used: cookies123



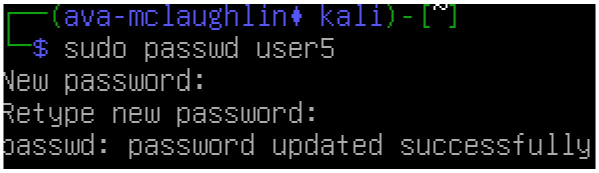
```
┌──(ava-mclaughlin㉿kali)-[~]
└─$ sudo passwd user3
New password:
Retype new password:
passwd: password updated successfully
```

Step 1.4: Password used: baseball757_!



```
┌──(ava-mclaughlin㉿kali)-[~]
└─$ sudo passwd user4
New password:
Retype new password:
passwd: password updated successfully
```

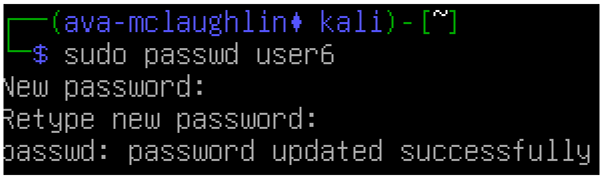
Step 1.5: Password used: cheese835



```
┌──(ava-mclaughlin㉿kali)-[~]
└─$ sudo passwd user5
New password:
Retype new password:
passwd: password updated successfully
```

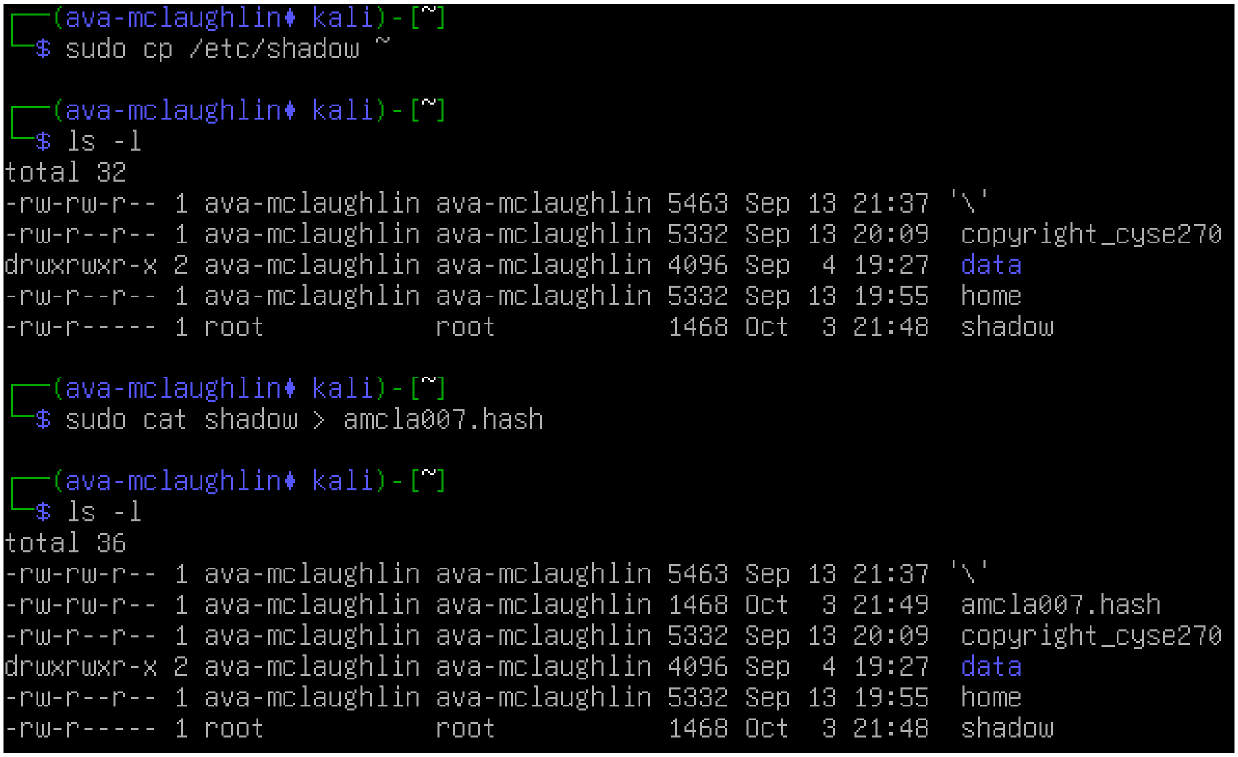
Ava McLaughlin

Step 1.6: Password used: FreeDoM@1776$



```
┌──(ava-mclaughlin㉿ kali)-[~]
└─$ sudo passwd user6
New password:
Retype new password:
passwd: password updated successfully
```

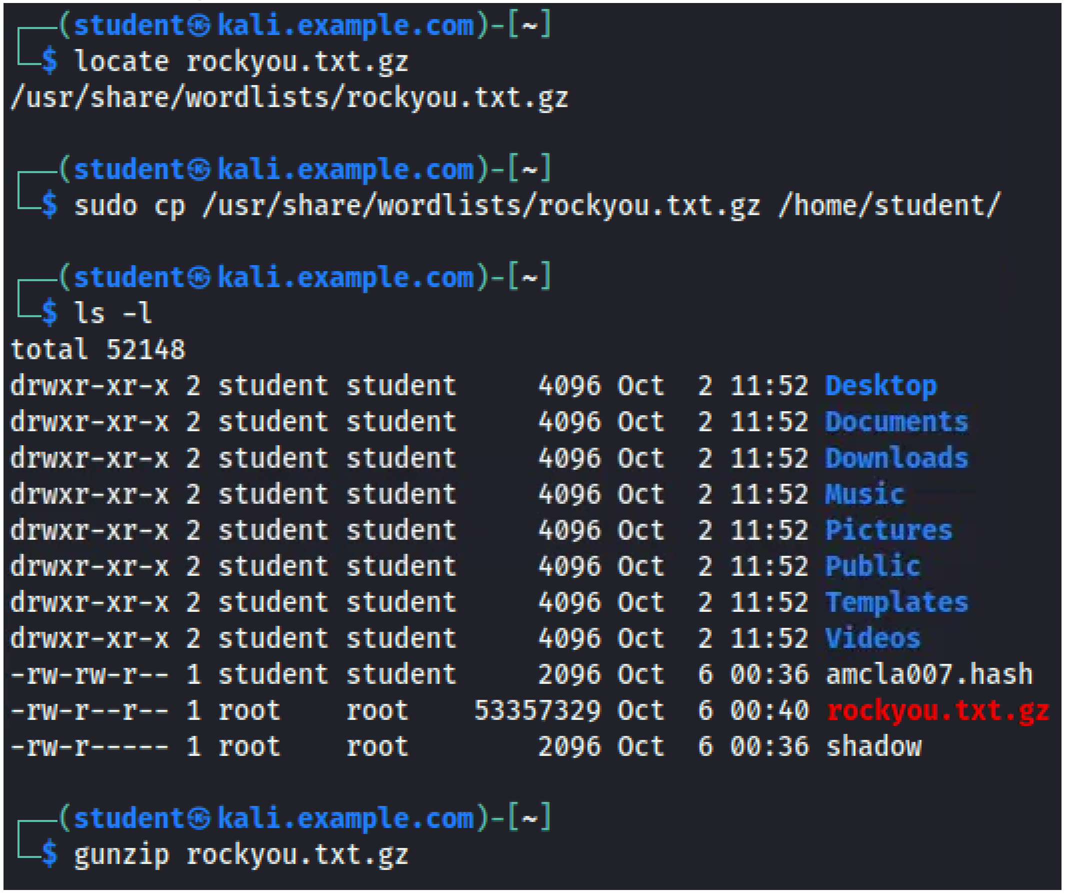
Step 2: Exporting user's hashes into file



```
┌──(ava-mclaughlin㉿ kali)-[~]
└─$ sudo cp /etc/shadow ~

┌──(ava-mclaughlin㉿ kali)-[~]
└─$ ls -l
total 32
-rw-rw-r-- 1 ava-mclaughlin ava-mclaughlin 5463 Sep 13 21:37 '\'
-rw-r--r-- 1 ava-mclaughlin ava-mclaughlin 5332 Sep 13 20:09  copyright_cyse270
drwxrwxr-x 2 ava-mclaughlin ava-mclaughlin 4096 Sep  4 19:27  data
-rw-r--r-- 1 ava-mclaughlin ava-mclaughlin 5332 Sep 13 19:55  home
-rw-r----- 1 root           root           1468 Oct  3 21:48  shadow

┌──(ava-mclaughlin㉿ kali)-[~]
└─$ sudo cat shadow > amcla007.hash

┌──(ava-mclaughlin㉿ kali)-[~]
└─$ ls -l
total 36
-rw-rw-r-- 1 ava-mclaughlin ava-mclaughlin 5463 Sep 13 21:37 '\'
-rw-rw-r-- 1 ava-mclaughlin ava-mclaughlin 1468 Oct  3 21:49  amcla007.hash
-rw-r--r-- 1 ava-mclaughlin ava-mclaughlin 5332 Sep 13 20:09  copyright_cyse270
drwxrwxr-x 2 ava-mclaughlin ava-mclaughlin 4096 Sep  4 19:27  data
-rw-r--r-- 1 ava-mclaughlin ava-mclaughlin 5332 Sep 13 19:55  home
-rw-r----- 1 root           root           1468 Oct  3 21:48  shadow
```

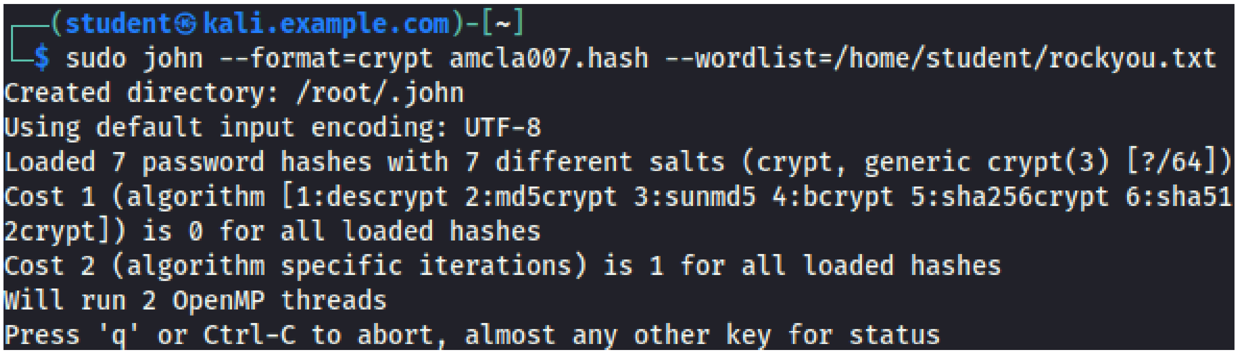
Step 2: Preparing rockyou (switched to CyberRange because I was unable to locate rockyou in my Linux)

Ava McLaughlin



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

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

┌──(student㉿kali.example.com)-[~]
└─$ ls -l
total 52148
drwxr-xr-x 2 student student     4096 Oct  2 11:52 Desktop
drwxr-xr-x 2 student student     4096 Oct  2 11:52 Documents
drwxr-xr-x 2 student student     4096 Oct  2 11:52 Downloads
drwxr-xr-x 2 student student     4096 Oct  2 11:52 Music
drwxr-xr-x 2 student student     4096 Oct  2 11:52 Pictures
drwxr-xr-x 2 student student     4096 Oct  2 11:52 Public
drwxr-xr-x 2 student student     4096 Oct  2 11:52 Templates
drwxr-xr-x 2 student student     4096 Oct  2 11:52 Videos
-rw-rw-r-- 1 student student     2096 Oct  6 00:36 amcla007.hash
-rw-r--r-- 1 root    root    53357329 Oct  6 00:40 rockyou.txt.gz
-rw-r----- 1 root    root        2096 Oct  6 00:36 shadow

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

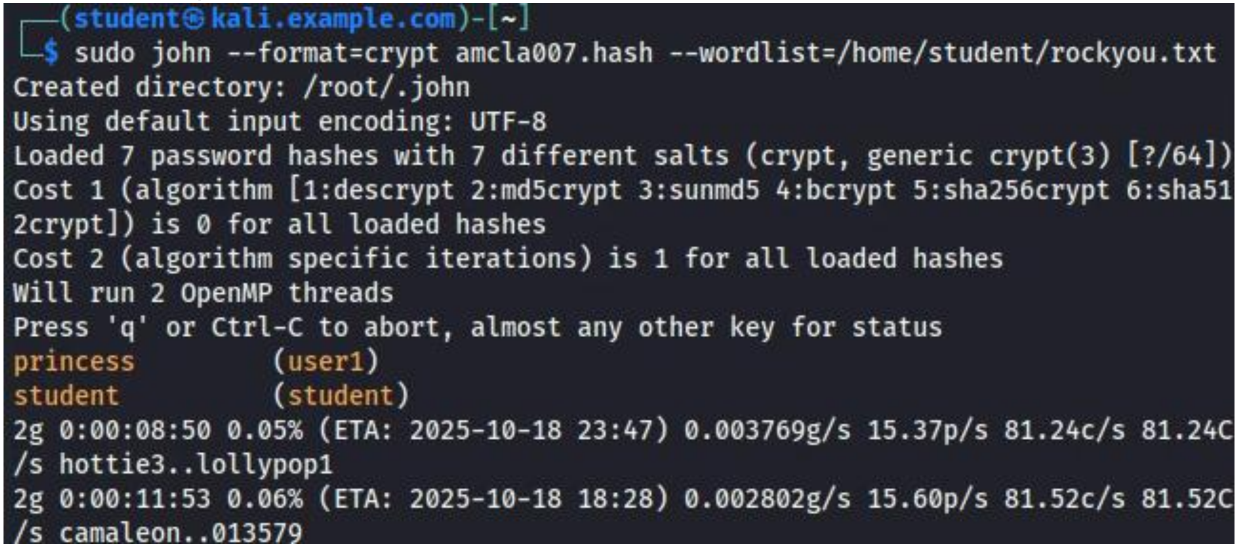
Step 2: Using John The Ripper Tool



```
┌──(student㉿kali.example.com)-[~]
└─$ sudo john --format=crypt amcla007.hash --wordlist=/home/student/rockyou.txt
Created directory: /root/.john
Using default input encoding: UTF-8
Loaded 7 password hashes with 7 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
Press 'q' or Ctrl-C to abort, almost any other key for status
```

Step 3: After 10 minutes, two passwords were cracked.

Ava McLaughlin



```
┌──(student㉿kali.example.com)-[~]
└─$ sudo john --format=crypt amcla007.hash --wordlist=/home/student/rockyou.txt
Created directory: /root/.john
Using default input encoding: UTF-8
Loaded 7 password hashes with 7 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
Press 'q' or Ctrl-C to abort, almost any other key for status
princess         (user1)
student          (student)
2g 0:00:08:50 0.05% (ETA: 2025-10-18 23:47) 0.003769g/s 15.37p/s 81.24c/s 81.24C
/s hottie3..lollypop1
2g 0:00:11:53 0.06% (ETA: 2025-10-18 18:28) 0.002802g/s 15.60p/s 81.52c/s 81.52C
/s camaleon..013579
```