Anna Mae Boubacar

03/05/2025

CYSE 270_28494

Professor Al Kinoon

Lab 5 – Password Cracking

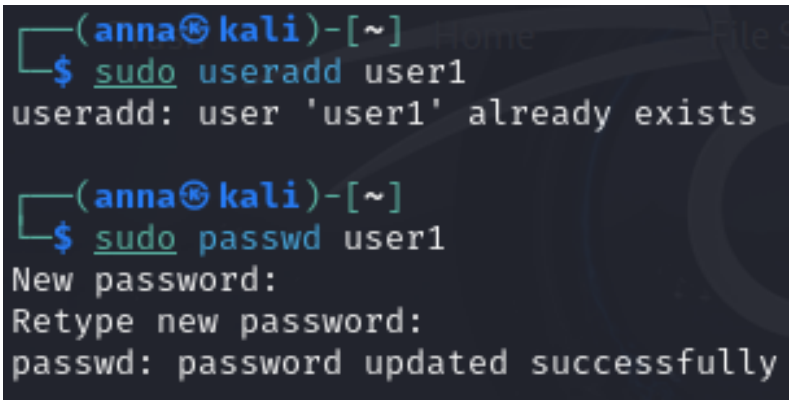
The goal of this lab is to test the strength of different passwords.

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].

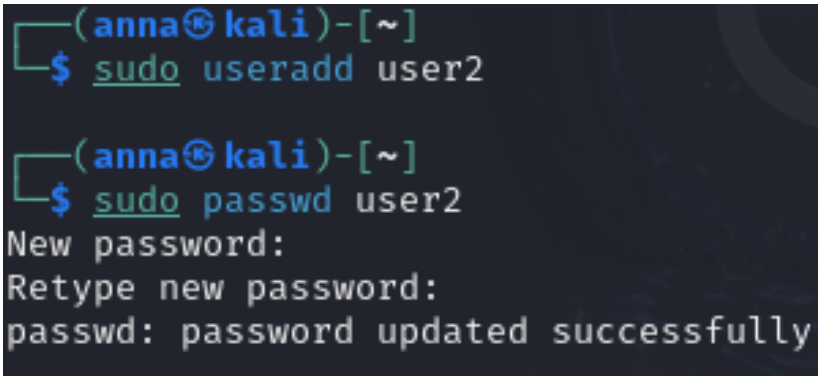
1. For user1, the password should be a simple dictionary word (all lowercase)

Password: apple



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

Password: 5674



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

Password: oranges4m3

```
┌──(anna㉿kali)-[~]
└─$ sudo useradd user3

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

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

Password: strawberry44

```
┌──(anna㉿kali)-[~]
└─$ sudo useradd user4

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

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

Password: mango1977

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

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

Password: 18PercenT%

```
┌──(anna㉿kali)-[~]
└─$ sudo useradd user6

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

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)

```
┌──(anna㉿kali)-[~]
└─$ sudo getent shadow user1 user2 user3 user4 user5 user6 > atabo003.hash

┌──(anna㉿kali)-[~]
└─$ cat atabo003.hash
user1:$y$j9T$TeOdDvWnz5b634QePc9Tl1$xpZAQvrECls3vc7.PeQ9MIQbhxpnxgceQ40HT09B
2QD:20153:0:99999:7:::
user2:$y$j9T$l2npO8n7jiFn4OegybZ6y1$Un1grSdkLzT4Qc0fV8sCG1FqS9qSja6oHJj2DL5B
912:20153:0:99999:7:::
user3:$y$j9T$1rf6KG54KKpnAfLImT6L91$8fms00SHTCyMUUfndT2IoBRrxGfWIgR3Y955Wylt
jsB:20153:0:99999:7:::
user4:$y$j9T$jEUVW7A0ZQ7hBcRHJt9lV/$i9Y69RyOJLTs/2ViBHZtiK5hZSPWXsG/tuxoMAFI
ta0:20153:0:99999:7:::
user5:$y$j9T$eqp4T3j32oVeAwi8S6YaD0$ln4gI7E2hrStCj0X1q9NAg8aBwLmAvtkX4zD3Ai6
XJ2:20153:0:99999:7:::
user6:$y$j9T$mAzEqn4tm2Cye0CLUPL8T.$AjaGPd6mM.o.McJTthu2VPAMbDvjJGBu/fqcNm7f
XH2:20153:0:99999:7:::
```

use John the Ripper tool to crack their passwords in wordlist mode (use rockyou.txt). [40 points]

timmy passwd: dominion26!

```
┌──(anna㉿kali)-[~]
└─$ sudo john --format=crypt test.txt --wordlist=/home/anna/rockyou.txt
Created directory: /root/.john
Using default input encoding: UTF-8
Loaded 8 password hashes with 8 different salts (crypt, generic crypt(3) [?/
64])
Cost 1 (algorithm [1:descrypt 2:md5crypt 3:sunmd5 4:bcrypt 5:sha256crypt 6:s
ha512crypt]) 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
```

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