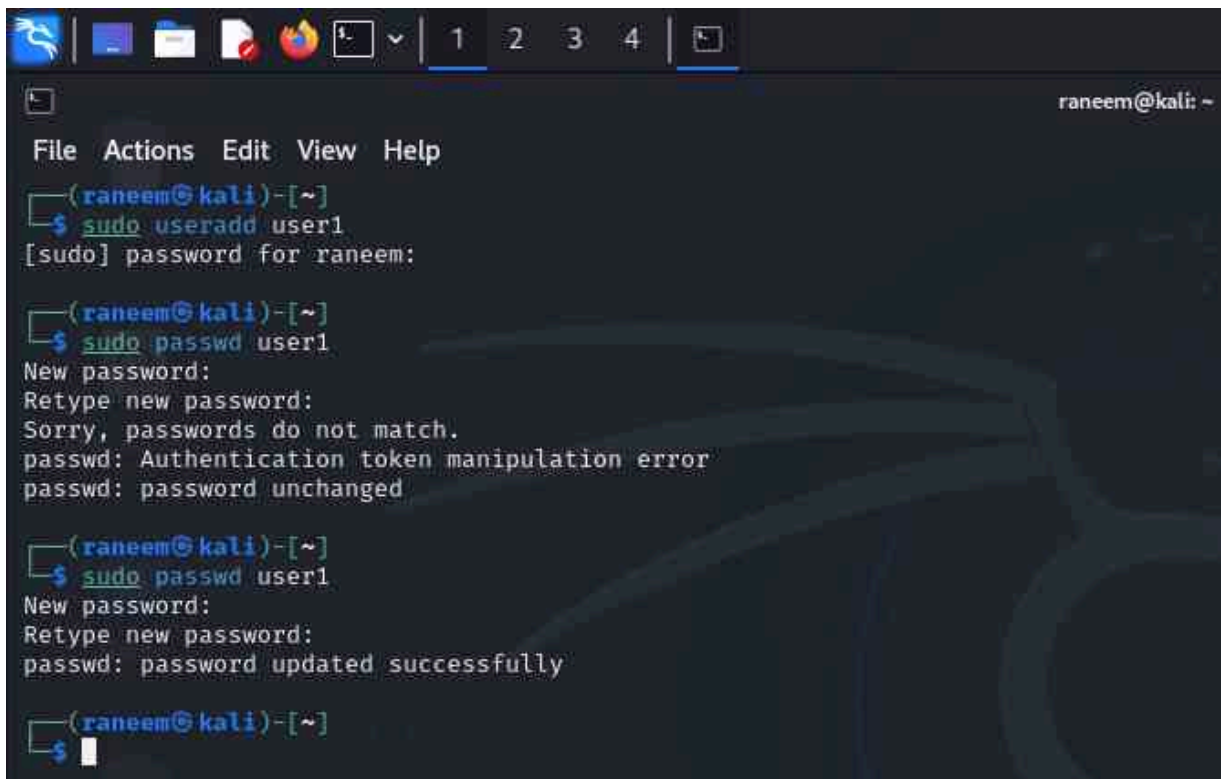


TASK A – Password Cracking

Step 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

1. For user1, the password should be a simple dictionary word (all lowercase)
 - **Password created:** apple
2. For user2, the password should consist of 4 digits
 - **Password created:** 5678
3. For user3, the password should consist of a simple dictionary word of any length characters (all lowercase) + digits
 - **Password created:** flowers987
4. For user4, the password should consist of a simple dictionary word characters (all lowercase) + digits + symbols
 - **Password created:** flowers123!@
5. For user5, the password should consist of a simple dictionary word (all lowercase) + digits
 - **Password created:** strawberry45
6. For user6, the password should consist of a simple dictionary word (with a combination of lower and upper case) + digits + symbols
 - **Password created:** Ge0rgla7#



```
(raneem@kali)-[~]
└─$ sudo useradd user1
[sudo] password for raneem:
(raneem@kali)-[~]
└─$ sudo passwd user1
New password:
Retype new password:
Sorry, passwords do not match.
passwd: Authentication token manipulation error
passwd: password unchanged
(raneem@kali)-[~]
└─$ sudo passwd user1
New password:
Retype new password:
passwd: password updated successfully
(raneem@kali)-[~]
└─$
```

```
(raneem@kali)~  
$ sudo useradd user2  
  
(raneem@kali)~  
$ sudo passwd user2  
New password:  
Retype new password:  
passwd: password updated successfully  
  
(raneem@kali)~  
$ sudo useradd user3  
  
(raneem@kali)~  
$ sudo passwd user3  
New password:  
Retype new password:  
passwd: password updated successfully  
  
(raneem@kali)~  
$ sudo useradd user4  
  
(raneem@kali)~  
$ sudo passwd user4  
New password:  
Retype new password:  
passwd: password updated successfully  
  
(raneem@kali)~  
$ sudo useradd user5  
  
(raneem@kali)~  
$ sudo passwd user5  
New password:  
Retype new password:  
passwd: password updated successfully  
  
(raneem@kali)~  
$ sudo useradd user6  
  
(raneem@kali)~  
$ sudo passwd user6  
New password:  
Retype new password:  
passwd: password updated successfully  
  
(raneem@kali)~  
$
```

Step 2: Export/save 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)

```
raneem@kali: ~  
File Actions Edit View Help  
  
(raneem@kali)-[~]  
└─$ sudo grep 'user[1-6]:' /etc/shadow | cut -d: -f1,2 > ralar002.hash  
  
(raneem@kali)-[~]  
└─$ cat ralar002.hash  
user1:$y$j9T$NqkFU21QxhgqnsW4RBi/b/$8Vt78s0T/TmYqZX1Kd9a/6PRYloPcFbv/m.wi6eCg09  
user2:$y$j9T$dGw8qDyIQ.62madDgW7Ei/$LVRWXWhgM8pn3klo7N4hNlRtxfT0M.oEeWcJLpv90e4  
user3:$y$j9T$KjVzNeRtdWZzgbDnPjI2Q0$ac0n29BdEbiHJgtgzYqmKeSmFTiUq6PbXvIPU0SFt01  
user4:$y$j9T$QIMagzv7fxoboGpV3c/Gt0$I3rM3F7CvQntyXcIszLX6fLSX796q0JI.S6lK.Ao9E7  
user5:$y$j9T$tPzT/pL7eHMspJr24SR/N1$AC65tdGcGnPGV/yhbSI8u/2tusL5nHOLEiKqwhsxME3  
user6:$y$j9T$NksQ1Fy8PoMB9X.CPzXam/$MuA.iqmSU4rZ24ES2.qfVyC7wowvqUu14lMvID7t6e4  
  
(raneem@kali)-[~]  
└─$
```

```
raneem@kali: ~  
File Actions Edit View Help  
  
(raneem@kali)-[~]  
└─$ ls /usr/share/wordlists/  
amass dirb dirbuster dnsmap.txt fasttrack.txt fern-wifi john.lst legion metasploit nmap.lst rockyou.txt.gz sqlmap.txt wfuzz wifite.txt  
  
(raneem@kali)-[~]  
└─$ gunzip /usr/share/wordlists/rockyou.txt.gz  
gzip: /usr/share/wordlists/rockyou.txt: Permission denied  
  
(raneem@kali)-[~]  
└─$ sudo gunzip /usr/share/wordlists/rockyou.txt.gz  
  
(raneem@kali)-[~]  
└─$
```

```
raneem@kali: ~  
File Actions Edit View Help  
  
(raneem@kali)-[~]  
└─$ cat ralar002.hash  
user1:$y$j9T$NqkFU21QxhgqnsW4RBi/b/$8Vt78s0T/TmYqZX1Kd9a/6PRYloPcFbv/m.wi6eCg09  
user2:$y$j9T$dGw8qDyIQ.62madDgW7Ei/$LVRWXWhgM8pn3klo7N4hNlRtxfT0M.oEeWcJLpv90e4  
user3:$y$j9T$KjVzNeRtdWZzgbDnPjI2Q0$ac0n29BdEbiHJgtgzYqmKeSmFTiUq6PbXvIPU0SFt01  
user4:$y$j9T$QIMagzv7fxoboGpV3c/Gt0$I3rM3F7CvQntyXcIszLX6fLSX796q0JI.S6lK.Ao9E7  
user5:$y$j9T$tPzT/pL7eHMspJr24SR/N1$AC65tdGcGnPGV/yhbSI8u/2tusL5nHOLEiKqwhsxME3  
user6:$y$j9T$NksQ1Fy8PoMB9X.CPzXam/$MuA.iqmSU4rZ24ES2.qfVyC7wowvqUu14lMvID7t6e4  
  
(raneem@kali)-[~]  
└─$ sudo john --format=crypt --wordlist=rockyou.txt ralar002.hash  
Using default input encoding: UTF-8  
Loaded 6 password hashes with 6 different salts (crypt, generic crypt(3) [?/64])  
Cost 1 (algorithm [1:descript 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  
Will run 2 OpenMP threads  
Press 'q' or Ctrl-C to abort, almost any other key for status  
└─$
```

Step 3: Keep your John the Ripper cracking for 10 minutes. How many passwords have been successfully cracked?

```
raneem@kali: ~  
File Actions Edit View Help  
  
(raneem@kali)-[~]  
└─$ cat ralar002.hash  
user1:$y$j9T$NqkFU21QxhgqnsW4Rbi/b/$8Vt78s0T/TmYqZX1Kd9a/6PRYloPcFbv/m.wi6eCg09  
user2:$y$j9T$dgw8qDyIQ.62madDgW7Ei/$LVRWXWhgM8pn3klo7N4hNlRtxft0M.oEeWcJLpv90e4  
user3:$y$j9T$KjVzNeRtdWZzgbDnPjI2Q0$acOn29BdEbiHJgtgzYqmKeSmFTiUq6PbXvIPU0Sft01  
user4:$y$j9T$QIMagzv7fxoboGpV3c/Gt0$I3rM3F7CvQntyXcIszlX6fLSX796q0JI.S6lK.Ao9E7  
user5:$y$j9T$tPzT/pL7eHmSpJr24SR/N1$AC65tdGcGnPGV/yhbSI8u/2tusL5nHOLEiKqwhsxME3  
user6:$y$j9T$NksQ1Fy8PoMB9X.CPzXam/$MuA.iqmSU4rZ24ES2.qfVyC7wowvqUu14lMvID7t6e4  
  
(raneem@kali)-[~]  
└─$ sudo john --format=crypt --wordlist=rockyou.txt ralar002.hash  
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  
Will run 2 OpenMP threads  
Press 'q' or Ctrl-C to abort, almost any other key for status  
apple (user1)  
1g 0:00:07:24 0.05% (ETA: 2024-06-25 16:39) 0.002248g/s 17.91p/s 91.96c/s 91.96C/s shinichi..yogibear  
1g 0:00:09:54 0.06% (ETA: 2024-06-25 11:20) 0.001681g/s 18.23p/s 92.97c/s 92.97C/s pink69..keren  
1g 0:00:10:24 0.07% (ETA: 2024-06-25 10:40) 0.001602g/s 18.30p/s 93.06c/s 93.06C/s warrior1..snuffy  
└─$
```

```
raneem@kali: ~  
File Firefox ESR Browse the World Wide Web  
  
(raneem@kali)-[~]  
└─$ sudo john --show ralar002.hash  
user1:apple  
  
1 password hash cracked, 0 left  
  
(raneem@kali)-[~]  
└─$
```