

Lab 2

58119125 JiangZhuoyang


1.Password Cracking

Q1:What is your method to find the correct password of user “cis4510suser”?

Solution:

1) We have obtained the salt value used in the password encryption result of the user and the encrypted result of SHA512 in the shadow file. Therefore, we can use the python program to traverse the possible passwords of the user "cis4510suser", call the crypt method on these passwords respectively to calculate the results of their SHA512 encryption, and compare these results with the known encryption results. If the encryption results of a possible password are consistent with the encryption results in the shadow file, it can be seen that the password is the password of the user "cis4510suser", and the decoding is successful.

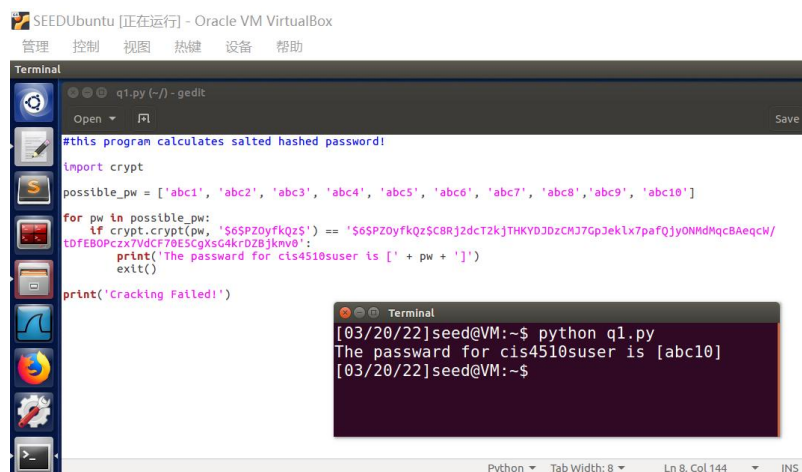
2) Program:

A screenshot of a text editor window titled 'q1.py (-) - gedit'. The code is a Python script that attempts to crack a password by comparing SHA512 hashes. It imports the 'crypt' module and defines a list of possible passwords: ['abc1', 'abc2', 'abc3', 'abc4', 'abc5', 'abc6', 'abc7', 'abc8', 'abc9', 'abc10']. It then iterates through this list, for each password 'pw', it calculates the SHA512 hash using 'crypt.crypt(pw, '\$6\$PZ0yfkQz\$C8Rj2dcT2kJTHKYD3DzCH37GpJekLx7paFQjYONMhQcBAeqch/tDfE80Pczx7VdCF70EScgXsG4krDZBjkmv0:')' and compares it to the target hash '\$6\$PZ0yfkQz\$C8Rj2dcT2kJTHKYD3DzCH37GpJekLx7paFQjYONMhQcBAeqch/tDfE80Pczx7VdCF70EScgXsG4krDZBjkmv0:'. If they match, it prints the password and exits. If not, it prints 'Cracking Failed!' after the loop.

```
q1.py (-) - gedit
#this program calculates salted hashed password!
import crypt
possible_pw = ['abc1', 'abc2', 'abc3', 'abc4', 'abc5', 'abc6', 'abc7', 'abc8', 'abc9', 'abc10']
for pw in possible_pw:
    if crypt.crypt(pw, '$6$PZ0yfkQz$C8Rj2dcT2kJTHKYD3DzCH37GpJekLx7paFQjYONMhQcBAeqch/tDfE80Pczx7VdCF70EScgXsG4krDZBjkmv0:') == '$6$PZ0yfkQz$C8Rj2dcT2kJTHKYD3DzCH37GpJekLx7paFQjYONMhQcBAeqch/tDfE80Pczx7VdCF70EScgXsG4krDZBjkmv0:':
        print('The password for cis4510suser is [' + pw + ']')
        exit()
print('Cracking Failed!')
```

Fig.1 Program of Q1

3) Result:

A screenshot of a terminal window titled 'Terminal'. It shows the execution of the Python script 'q1.py'. The output is: 'The password for cis4510suser is [abc10]'. The terminal prompt is '[03/20/22]seed@VM:~\$'.

```
Terminal
[03/20/22]seed@VM:~$ python q1.py
The password for cis4510suser is [abc10]
[03/20/22]seed@VM:~$
```

Fig.2 Result of Q1

Q2:What is the password for user “cis4510suser”?

Answer:

The password for cis4510suser is ‘**abc10**’

2. Unix Password Hashes Cracking using John the Ripper

Q3~6. Note the Timing for cracking the password:

Answer:

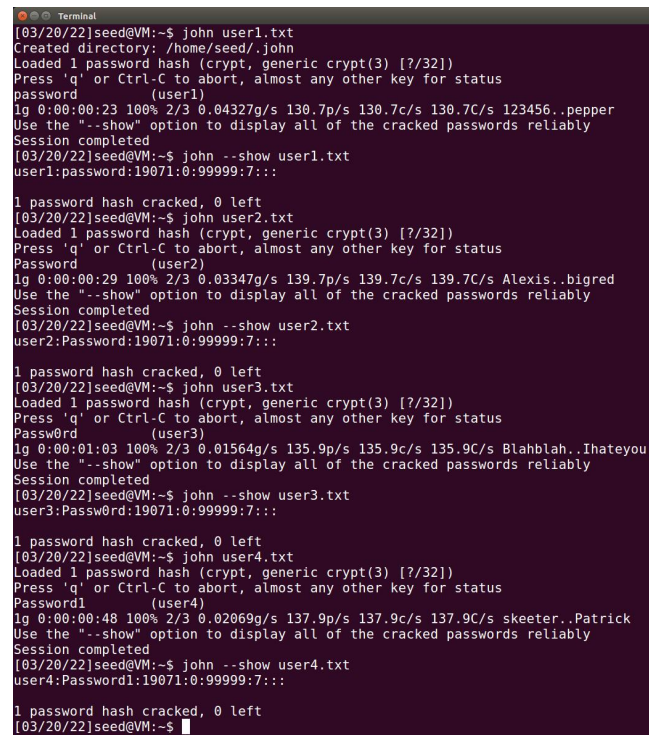
Q3: 0:00:00:23

Q4: 0:00:00:29

Q5: 0:00:01:03

Q6: 0:00:00:48

The result is directly showed below:



```
[03/20/22]seed@VM:~$ john user1.txt
Created directory: /home/seed/.john
Loaded 1 password hash (crypt, generic crypt(3) [?/32])
Press 'q' or Ctrl-C to abort, almost any other key for status
password
(user1)
lg 0:00:00:23 100% 2/3 0.04327g/s 130.7p/s 130.7c/s 130.7C/s 123456..pepper
Use the "--show" option to display all of the cracked passwords reliably
Session completed
[03/20/22]seed@VM:~$ john --show user1.txt
user1:password:19071:0:99999:7:::

1 password hash cracked, 0 left
[03/20/22]seed@VM:~$ john user2.txt
Loaded 1 password hash (crypt, generic crypt(3) [?/32])
Press 'q' or Ctrl-C to abort, almost any other key for status
Password
(user2)
lg 0:00:00:29 100% 2/3 0.03347g/s 139.7p/s 139.7c/s 139.7C/s Alexis..bigred
Use the "--show" option to display all of the cracked passwords reliably
Session completed
[03/20/22]seed@VM:~$ john --show user2.txt
user2:Password:19071:0:99999:7:::

1 password hash cracked, 0 left
[03/20/22]seed@VM:~$ john user3.txt
Loaded 1 password hash (crypt, generic crypt(3) [?/32])
Press 'q' or Ctrl-C to abort, almost any other key for status
Passw0rd
(user3)
lg 0:00:01:03 100% 2/3 0.01564g/s 135.9p/s 135.9c/s 135.9C/s Blahblah..Ihateyou
Use the "--show" option to display all of the cracked passwords reliably
Session completed
[03/20/22]seed@VM:~$ john --show user3.txt
user3:Passw0rd:19071:0:99999:7:::

1 password hash cracked, 0 left
[03/20/22]seed@VM:~$ john user4.txt
Loaded 1 password hash (crypt, generic crypt(3) [?/32])
Press 'q' or Ctrl-C to abort, almost any other key for status
Password1
(user4)
lg 0:00:00:48 100% 2/3 0.02069g/s 137.9p/s 137.9c/s 137.9C/s skeeter..Patrick
Use the "--show" option to display all of the cracked passwords reliably
Session completed
[03/20/22]seed@VM:~$ john --show user4.txt
user4:Password1:19071:0:99999:7:::

1 password hash cracked, 0 left
[03/20/22]seed@VM:~$
```

Fig.3 Result of Jonh the Ripper

Q7: In your opinion, which password is the most complex one, password, Password, Passw0rd or Password1? Did you notice a correlation between the times it took to crack a password versus the complexity of the password? You should have seen that more complex passwords take longer to recover.

Solution:

The Password “Passw0rd” is the most complex.

Firstly, from the character composition of the password, the password of user3 and user4 contains uppercase letters, lowercase letters and numbers, so they are more complex than user2’s password without number character. And of cause, they are all more complex than user1’s password which just has the lowercase letters character.

Then, from the character arrangement order of the password, in user4’s password, the three characters of the password are arranged alternately. While user3’s password just sort the three characters of the password in order of type.

And of course, the password with higher complexity take longer to decode.

Q8. Conduct a study by surveying some online articles and give one tip to choose a strong password.

Answer:

A study of Symantec Research Labs on advanced password decoding technology showed that setting a password containing numbers and uppercase letters does not significantly improve the security of the password, while increasing the length of the password or setting a password containing symbols is more effective.

Q9. Using John the ripper, try to break the passwords in the passwords.txt file provided. What passwords were you able to crack?

Solution:

Only the password contains uppercase letters, lowercase letters and numbers can be cracked. The result is showed below: (Aborted after 5min)

```
[03/20/22]seed@VM:~$ john passwords.txt
Loaded 17 password hashes with 17 different salts (md5crypt [MD5 32/32])
Press 'q' or Ctrl-C to abort, almost any other key for status
monkey          (user2)
monkey1         (user4)
a               (user0)
Monkey          (user14)
mnbvcxz         (user11)
5g 0:00:09:21 3/3 0.008908g/s 894.8p/s 10508c/s 10508C/s amomal
Use the "--show" option to display all of the cracked passwords reliably
Session aborted
```

Fig.4 Result of Jonh the Ripper on passwords.txt

3. Cracking the password in Q1 using John the Ripper

Q10: Clearly describe what you do to use John the Ripper to crack the password of user “cis4510suser”

Solution:

- 1) Create the .txt file to store the SHA password information.

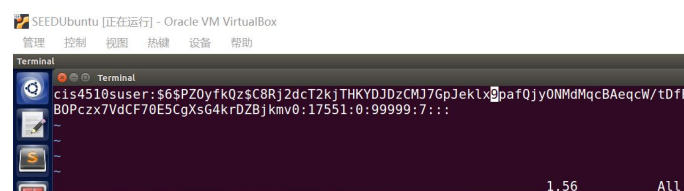


Fig.5 The cis4510suser.txt

- 2) Use John the Ripper to crack it.
- 3) Abort after it had run more than 5 min.

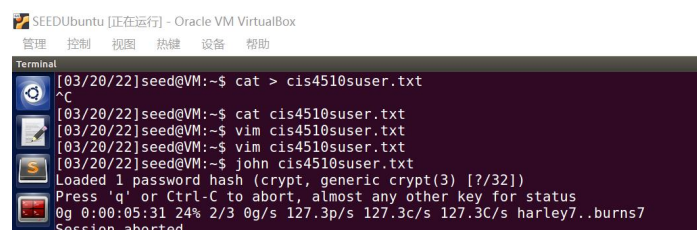


Fig.6 Process and result of John the Ripper

Q11: Does John the Ripper successfully crack the password for user “cis4510suser”?

Answer: no