CYBER SECURITY 2021

**P2: Hashed password cracking**

# **Preparation:**

Study guides about John the Ripper.

Create some normal users with simple passwords: test1, test2, test3.

Checked the directory /usr/share/wordlists and I found these text files as passwordlist files:

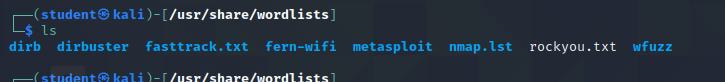


Figure 1. Password-list files

I also download 10-million-password.txt found on Github.

# **Passwd and shadow:**

Contents of passwd and shadow files:

Text

Description automatically generated

Figure 2. Content of passwd file

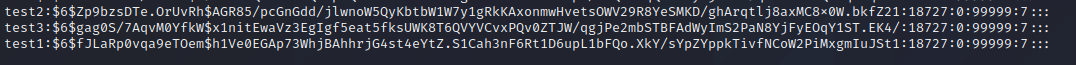


Figure 3. Content of shadow file

From the shadow information, I may conclude that all the passwords used **sha512** hash algorithm and the salts for test 1, test2 and test3 are: **fJLaRp0vqa9eTOem; Zp9bzsDTe.OrUvRh; ag0S/7AqvM0YfkW,** respectively.

The first 3 fields after username represent for type of hash, salt and hashed value; these fields are separated by **$** sign.

Using the same password and salt input for sha512 algorithm, I got the **same** hashed value for user test1:



Figure 4. Using openssl passwd command

# **John the Ripper:**

The unshadow command is used to combine the shadow and the passwd files.

Text

Description automatically generated

Figure 5. Using unshadow command

**Note:** when using command unshadow to combine 2 files and redirect the output to another file, I should use command “*sudo unshadow passwd shadow > ~/unshadowed.txt*” or “*sudo sh -e "unshadow passwd shadow" > unshadow.txt"*” since I cannot create a file in /etc folder and the sudo affects only the first command (unshadow) and not the redirect command (>).

The main command for JohnTheRipper is “john” and it comes with many parameters:

--wordlist: using a file (--stdin) or fetch words from .pot file (--pipe)

--rules[=SECTION]: enable word mangling rules for wordlist modes

Etc.

A picture containing graphical user interface

Description automatically generated

Figure 6. Crack all users

This is crack all 4 in one command (takes about 13 mins to crack all passwords), I may divide the unshadowed.txt into 4 small text files to crack each user password.

After cracking all these passwords, they will be recorded to a file “~/.john/john.pot”:

A screenshot of a computer

Description automatically generated with medium confidence

Figure 7. Content of john.pot

Now I crack 1 user at a time and compare to the time on “https://howsecureismypassword.net/”:

zxcasd: 41s (7ms on web check)

abc: 1m13s (400ns on web check)

password: 0.87s (INSTANTLY on web check)

roopoo: 7min45s (7ms on web check)

Maybe the estimated times are different because of type of machine used for cracking, type of algorithm used in the passwords?

When I change one of the user’s password to a 8-character long one, it takes john only 5.3 seconds to crack (it said proceed with password.lst, I think it is the default wordlist of john).

There are (around) 14344392 passwords in the rockyou.txt.

Luckily, I cannot find my own passwords in that list.

For the last task, cracking this unshadowed entrance: *Administrator:500:CC5E9ACBAD1B25C9AAD3B435B51404EE:996E6760CDDD8815A2C24A110CF040FB:::*

It takes only 0.88 second!!!

The password is MULLET.

ADDITIONAL task:

Crack all user passwords from shadow file:

Test1: qwerty

Test4: a1b2c3d4

These 2 are cracked in seconds.

Then it said proceeding with incremental ASCII (brute-force?), and it takes like forever to crack. (like the previous zip file, took me 10 days to crack a 9-character password)

So I stopped.