

CS392 Secure System Design: Threats and Countermeasures

Assignment 3

Sanskriti Singh
2001CS60

Aim:

First-hand experience on using password cracking tool to check for the weak passwords

Preparations:

\$ sudo apt-get install john
→ to use John-the-ripper

\$ sudo apt-get install adduser
→ to add users

```
(base) sanskriti@sans-ubuntu:~$ john
John the Ripper password cracker, version 1.8.0
Copyright (c) 1996-2013 by Solar Designer
Homepage: http://www.openwall.com/john/
```

```
Usage: john [OPTIONS] [PASSWORD-FILES]
--single                "single crack" mode
--wordlist=FILE --stdin  wordlist mode, read words from FILE or stdin
--rules                 enable word mangling rules for wordlist
--incremental[=MODE]    "incremental" mode [using section MODE]
```

Steps:

Step1

Use 'su' to change to 'root'

```
(base) sanskriti@sans-ubuntu:~$ sudo su root  
root@sans-ubuntu:/home/sanskriti#
```

Step2

Make directory 'test' and use 'chmod' to change its permissions to 777

```
root@sans-ubuntu:/home/sanskriti# mkdir test  
root@sans-ubuntu:/home/sanskriti# chmod 777 test
```

Step3

Change directory to 'test'

Download wordlist containing probable passwords (it is 'rockyou.txt')

```
root@sans-ubuntu:/home/sanskriti# cd test
root@sans-ubuntu:/home/sanskriti/test# wget http://scrapmaker.com/data/wordlists/dictionaries/rockyou.txt
--2023-03-24 15:47:58-- http://scrapmaker.com/data/wordlists/dictionaries/rockyou.txt
Resolving scrapmaker.com (scrapmaker.com)... 192.254.232.166
Connecting to scrapmaker.com (scrapmaker.com)|192.254.232.166|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 139921497 (133M) [text/plain]
Saving to: 'rockyou.txt'

rockyou.txt          100%[=====>] 133.44M   146KB/s   in 44m 12s

2023-03-24 16:32:14 (51.5 KB/s) - rockyou.txt saved [139921497/139921497]
```

Step4

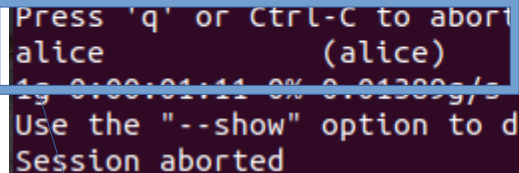
Add user 'alice' with password [alice]

```
root@sans-ubuntu:/home/sanskriti/test# adduser alice
Adding user `alice' ...
Adding new group `alice' (1001) ...
Adding new user `alice' (1001) with group `alice' ...
Creating home directory `/home/alice' ...
Copying files from `/etc/skel' ...
New password:
BAD PASSWORD: The password is shorter than 8 characters
Retype new password:
passwd: password updated successfully
Changing the user information for alice
Enter the new value, or press ENTER for the default
    Full Name []:
    Room Number []:
    Work Phone []:
    Home Phone []:
    Other []:
Is the information correct? [Y/n] y
```

Step5

Use 'john' to crack passwords

```
root@sans-ubuntu:/home/sanskriti/test# john --wordlist=rockyou.txt /etc/shadow
Created directory: /root/.john
Loaded 2 password hashes with 2 different salts (crypt, generic crypt(3) [?/64])
Will run 8 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
alice (alice)
1g 0:00:01:11 0% 0.01389g/s 1525p/s 1563c/s 1563C/s seznam..sandry
Use the "--show" option to display all of the cracked passwords reliably
Session aborted
```



The password was cracked in few seconds

Step6

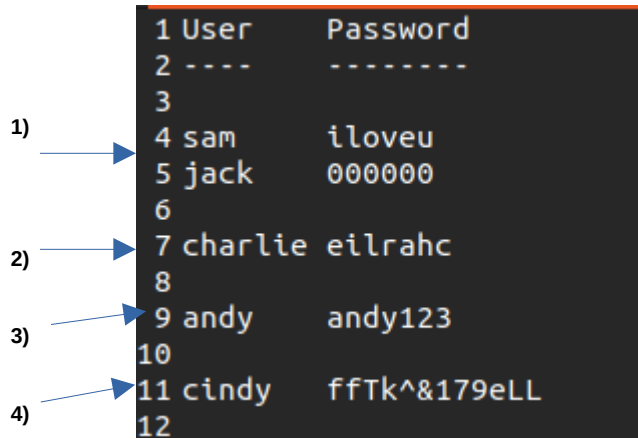
Use 'john' to crack the passwords and observe

```
root@sans-ubuntu:/home/sanskriti/test# john --wordlist=rockyou.txt /etc/shadow
Loaded 7 password hashes with 7 different salts (crypt, generic crypt(3) [?/64])
Remaining 6 password hashes with 6 different salts
Will run 8 OpenMP threads
Press q or ctrl-c to abort, almost any other key for status
000000      (jack)
iloveu      (sam)
andy123     (andy)
eilrahc     (charlie)
4g 0:01:58:53 7% 0.000560g/s 65.7p/s 351.6c/s 351.6C/s vianong..vi1986
Use the --show option to display all of the cracked passwords reliably
Session aborted
```

Step6

Make other new users and passwords to experiment

- 1) Add two users and their passwords will be chosen from the rockyou wordlist file.
- 2) Add one user with password as the reverse of the username.
- 3) Add one user with password as the 123 extension of the username.
- 4) Add one user with randomly generated strong password



1	User	Password
2	----	-----
3		
1) → 4	sam	iloveu
5	jack	000000
6		
2) → 7	charlie	eilrahc
8		
3) → 9	andy	andy123
10		
4) → 11	cindy	ffTk^&179eLL
12		

**The list of
username and
passwords that
was formed**

Observations:

- The password cracking process ran for **3 hours**
- For the users with passwords from the wordlist gave instant results
- For the user with password with 123 as extension to username gave result in about 10 min
- For the user with reverse username as password gave result in about 30-40 min
- For the user with extremely random and strong password did not give result even after 3 hours

Conclusion:

- For the users with passwords from the wordlist, it was instant as the password was available in the list and hence can be found by trying out the passwords from the list
- For the user with password with 123 as extension to username and with reverse of username took sometime but not long enough as they follow certain common patterns
- For the user with extremely random and strong password did not give result because of the extremely unpredictable and uncommon nature