

CS392 – Secure System Design

Assignment 3

Threats and Countermeasures

Tarusi Mittal

1901CS65

Overview:

The learning objective of this assignment is for students to gain the first-hand experience on using password cracking tool to check for the weak passwords. A system administrator needs to be careful that users should not use easy to crack passwords.

Explanation:

1. Install John The Ripper

```
[04/05/22]seed@VM:~$ sudo apt-get install john
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  john-data
The following NEW packages will be installed:
  john john-data
0 upgraded, 2 newly installed, 0 to remove and 3 not upgraded.
Need to get 4,481 kB of archives.
After this operation, 8,418 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://us.archive.ubuntu.com/ubuntu xenial/main i386 john-data all 1.8.0-2 [4,263 kB]
Get:2 http://us.archive.ubuntu.com/ubuntu xenial/main i386 john i386 1.8.0-2 [218 kB]
Fetched 4,481 kB in 40s (111 kB/s)
Selecting previously unselected package john-data.
(Reading database ... 215092 files and directories currently installed.)
Preparing to unpack .../john-data_1.8.0-2_all.deb ...
Unpacking john-data (1.8.0-2) ...
Selecting previously unselected package john.
Preparing to unpack .../archives/john_1.8.0-2_i386.deb ...
Unpacking john (1.8.0-2) ...
Processing triggers for man-db (2.7.5-1) ...
Setting up john-data (1.8.0-2) ...
Setting up john (1.8.0-2) ...
[04/05/22]seed@VM:~$
```

2.Change to root -> create a folder name test -> change its permissions to 777

```
[04/05/22]seed@VM:~$ su - root
```

```
Password:
```

```
root@VM:~# mkdir test
```

```
root@VM:~# chmod 777 test
```

```
root@VM:~# ls
```

```
test
```

```
root@VM:~# ls -l
```

```
total 4
```

```
drwxrwxrwx 2 root root 4096 Apr  5 14:00 test
```

```
root@VM:~#
```

3. Download the wordlist dictionary

```
root@VM:~# cd test
root@VM:~/test# wget http://scrapmaker.com/data/wordlists/dictionaries/rockyou.txt --no-check-certificate
--2022-04-05 14:04:05-- 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... 301 Moved Permanently
Location: https://www.scrapmaker.com/data/wordlists/dictionaries/rockyou.txt [following]
--2022-04-05 14:04:06-- https://www.scrapmaker.com/data/wordlists/dictionaries/rockyou.txt
Resolving www.scrapmaker.com (www.scrapmaker.com)... 192.254.232.166
Connecting to www.scrapmaker.com (www.scrapmaker.com)|192.254.232.166|:443... connected.
WARNING: cannot verify www.scrapmaker.com's certificate, issued by 'CN=R3,0=Let's Encrypt,C=US':
Unable to locally verify the issuer's authority.
HTTP request sent, awaiting response... 200 OK
Length: 139921497 (133M) [text/plain]
Saving to: 'rockyou.txt'

rockyou.txt          100%[=====>] 133.44M  323KB/s  in 12m 10s

2022-04-05 14:16:17 (187 KB/s) - 'rockyou.txt' saved [139921497/139921497]

root@VM:~/test# ls
rockyou.txt
root@VM:~/test#
```

4.Create an account for new user. With username Alice and password Alice.

```
rockyou.txt
root@VM:~/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' ...
Enter new UNIX password:
Retype new UNIX 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
root@VM:~/test#
```

Checking etc/shadow:

```
root@VM: ~/test
root@VM:~/test# cat /etc/shadow
root:$6$Nrf4601p$.vDnKEtVFC2bXslxkRuT4FcBqPpxLqW05IoECr0XKzEE05wj8aU3GRHW2BaodUn4K3vgYEjwPspr/kqzAqtcu.:17400:0:99999:7:::
daemon*:17212:0:99999:7:::
bin*:17212:0:99999:7:::
sys*:17212:0:99999:7:::
sync*:17212:0:99999:7:::
games*:17212:0:99999:7:::
man*:17212:0:99999:7:::
lp*:17212:0:99999:7:::
mail*:17212:0:99999:7:::
news*:17212:0:99999:7:::
uucp*:17212:0:99999:7:::
proxy*:17212:0:99999:7:::
www-data*:17212:0:99999:7:::
backup*:17212:0:99999:7:::
list*:17212:0:99999:7:::
irc*:17212:0:99999:7:::
gnats*:17212:0:99999:7:::
nobody*:17212:0:99999:7:::
systemd-timesync*:17212:0:99999:7:::
systemd-network*:17212:0:99999:7:::
systemd-resolve*:17212:0:99999:7:::
systemd-bus-proxy*:17212:0:99999:7:::
syslog*:17212:0:99999:7:::
_apt*:17212:0:99999:7:::
messagebus*:17212:0:99999:7:::
uuidd*:17212:0:99999:7:::
lightdm*:17212:0:99999:7:::
whoopsie*:17212:0:99999:7:::
avahi-autoipd*:17212:0:99999:7:::
avahi*:17212:0:99999:7:::
dnsmasq*:17212:0:99999:7:::
colord*:17212:0:99999:7:::
speech-dispatcher:!:17212:0:99999:7:::
hplip*:17212:0:99999:7:::
kernoops*:17212:0:99999:7:::
pulse*:17212:0:99999:7:::
```

```
pulse*:17212:0:99999:7:::
rtkit*:17212:0:99999:7:::
saned*:17212:0:99999:7:::
usbmux*:17212:0:99999:7:::
seed:$6$wDRrWCQz$IsBXp9.9wz9SGrF.nbiHpoN5w.zQx02sht4cTY8qI7YKh00wN/sfYvDeCAcEo2QYzCfpZoaEVJ8sbCT7hkxXY/:17372:0:99999:7:::
vboxadd!:17372:0:99999:7:::
telnetd*:17372:0:99999:7:::
sshd*:17372:0:99999:7:::
ftp*:17372:0:99999:7:::
bind*:17372:0:99999:7:::
mysql:!:17372:0:99999:7:::
alice:$6$0.BuiBUo$08dAbj.hqzSZrAp51HkDJwa.9dyHxltV.x9f6YhIvtzPxZCFpazl0pLZXNFnTp9jU1z0Et6eMTNbJ63yhCG3X.:19087:0:99999:7:::
root@VM:~/test#
```

5. Cracking the password for alice using john the ripper

P.T.O

```

M: ~/test
root@VM:~/test# john --wordlist=rockyou.txt /etc/shadow
Created directory: /root/.john
Loaded 3 password hashes with 3 different salts (crypt, generic crypt(3) [?/32])
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:09 0% 0g/s 31.54p/s 105.1c/s 105.1C/s adidas..michael1
0g 0:00:00:15 0% 0g/s 31.14p/s 105.9c/s 105.9C/s teiubesc..parola
0g 0:00:00:18 0% 0g/s 31.61p/s 105.3c/s 105.3C/s evelyn..kelly
0g 0:00:00:22 0% 0g/s 33.95p/s 106.1c/s 106.1C/s football1..felipe
0g 0:00:00:24 0% 0g/s 31.88p/s 103.6c/s 103.6C/s football1..felipe
0g 0:00:00:26 0% 0g/s 32.35p/s 100.6c/s 100.6C/s chichi..sandy
0g 0:00:00:29 0% 0g/s 33.08p/s 99.24c/s 99.24C/s mariel..stars
0g 0:00:00:32 0% 0g/s 32.51p/s 97.53c/s 97.53C/s dancerr1..summer1
0g 0:00:00:35 0% 0g/s 30.12p/s 95.86c/s 95.86C/s dancerr1..summer1
0g 0:00:00:36 0% 0g/s 31.72p/s 95.18c/s 95.18C/s 753951..shirley
0g 0:00:00:37 0% 0g/s 30.53p/s 94.14c/s 94.14C/s 753951..shirley
0g 0:00:00:38 0% 0g/s 29.63p/s 93.85c/s 93.85C/s 753951..shirley
0g 0:00:00:40 0% 0g/s 31.17p/s 93.52c/s 93.52C/s dragons..phoebe
0g 0:00:00:45 0% 0g/s 29.68p/s 93.28c/s 93.28C/s teacher..michel
0g 0:00:00:48 0% 0g/s 29.66p/s 92.93c/s 92.93C/s rachel..mexico1
0g 0:00:00:50 0% 0g/s 30.21p/s 92.54c/s 92.54C/s clover..punkrock
0g 0:00:00:52 0% 0g/s 29.41p/s 91.93c/s 91.93C/s clover..punkrock
0g 0:00:00:54 0% 0g/s 29.95p/s 91.61c/s 91.61C/s mollie..argentina
0g 0:00:00:56 0% 0g/s 30.38p/s 91.15c/s 91.15C/s 2hot4u..eastside
0g 0:00:00:58 0% 0g/s 29.64p/s 90.59c/s 90.59C/s 2hot4u..eastside
0g 0:00:01:00 0% 0g/s 30.04p/s 90.14c/s 90.14C/s cristiano..hercules
0g 0:00:01:03 0% 0g/s 28.94p/s 89.87c/s 89.87C/s cristiano..hercules
0g 0:00:01:07 0% 0g/s 29.73p/s 89.21c/s 89.21C/s harris..morado
0g 0:00:01:09 0% 0g/s 29.14p/s 88.82c/s 88.82C/s harris..morado
0g 0:00:01:11 0% 0g/s 29.48p/s 88.44c/s 88.44C/s laurita..brittany1
0g 0:00:01:13 0% 0g/s 28.89p/s 88.00c/s 88.00C/s laurita..brittany1
0g 0:00:01:15 0% 0g/s 29.28p/s 87.86c/s 87.86C/s bamboo..abcdefgh
0g 0:00:01:19 0% 0g/s 28.87p/s 87.83c/s 87.83C/s skyblue..blingbling
0g 0:00:01:21 0% 0g/s 28.38p/s 87.53c/s 87.53C/s skyblue..blingbling
0g 0:00:01:23 0% 0g/s 28.75p/s 87.40c/s 87.40C/s batman1..althea
0g 0:00:01:28 0% 0g/s 29.22p/s 87.67c/s 87.67C/s star123..nugget
0g 0:00:01:30 0% 0g/s 28.50p/s 87.62c/s 87.62C/s star123..nugget
alice (alice)

```

Here we can see that password for alice is cracked

And after that we will press q or Cntrl+c to terminate

```

0g 0:00:01:28 0% 0g/s 29.22p/s 87.67c/s 87.67C/s star123..nugget
0g 0:00:01:30 0% 0g/s 28.50p/s 87.62c/s 87.62C/s star123..nugget
alice (alice)
lg 0:00:01:32 0% 0.01082g/s 29.10p/s 87.31c/s 87.31C/s my3kids..victoria1
lg 0:00:01:42 0% 0.009783g/s 30.99p/s 88.28c/s 88.28C/s grecia..jeter2
Use the "--show" option to display all of the cracked passwords reliably
Session aborted
root@VM:~/test#

```

Add 5 users as:

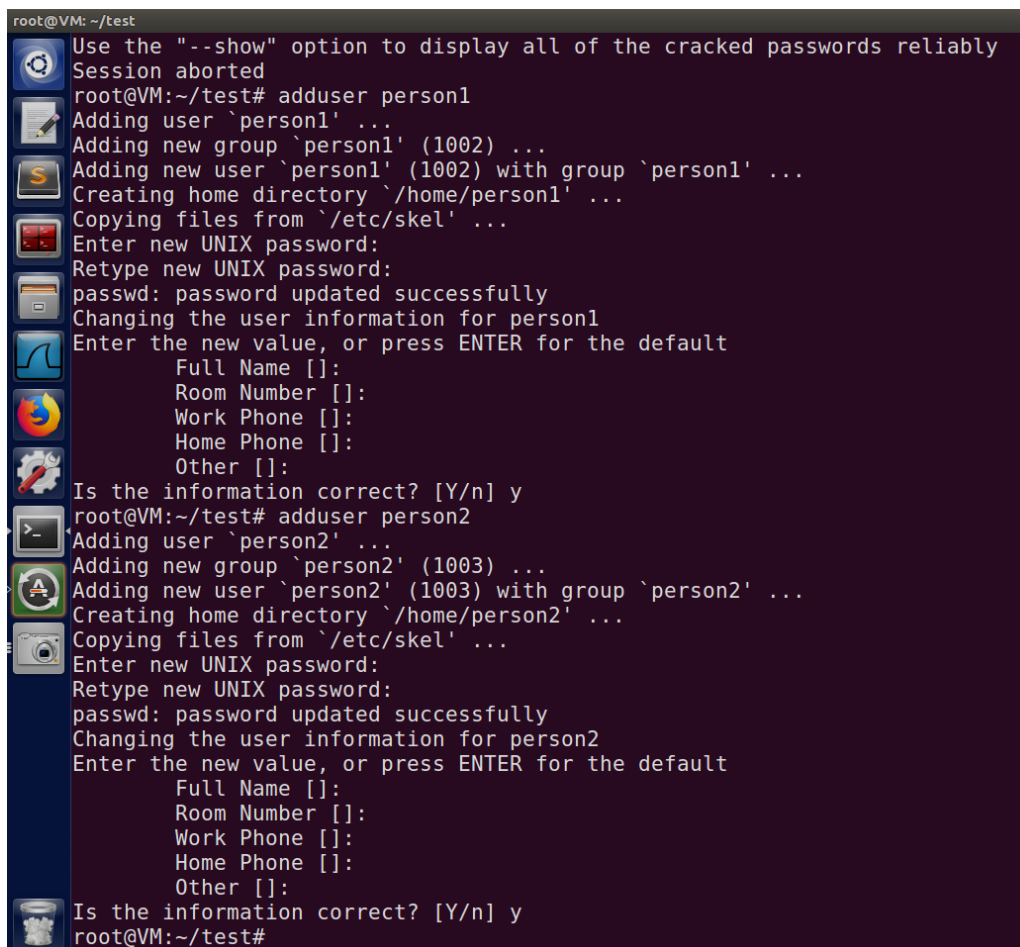
Add two users and their passwords will be chosen from the rockyou wordlist file.

1. Username -> person1

Password -> diana

2. Username -> person2

Password -> oliver



```
root@VM: ~/test
Use the "--show" option to display all of the cracked passwords reliably
Session aborted
root@VM:~/test# adduser person1
Adding user `person1' ...
Adding new group `person1' (1002) ...
Adding new user `person1' (1002) with group `person1' ...
Creating home directory `/home/person1' ...
Copying files from `/etc/skel' ...
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
Changing the user information for person1
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
root@VM:~/test# adduser person2
Adding user `person2' ...
Adding new group `person2' (1003) ...
Adding new user `person2' (1003) with group `person2' ...
Creating home directory `/home/person2' ...
Copying files from `/etc/skel' ...
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
Changing the user information for person2
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
root@VM:~/test#
```

3. Add one user with password as the reverse of the username.

Username -> tarusi

Password-> isurat

```
root@VM:~/test# adduser tarusi
Adding user `tarusi' ...
Adding new group `tarusi' (1004) ...
Adding new user `tarusi' (1004) with group `tarusi' ...
Creating home directory `/home/tarusi' ...
Copying files from `/etc/skel' ...
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
Changing the user information for tarusi
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
```

4. Add one user with password as the 123 extension of the username. So if the username is bob then password will be bob123

Username -> bob

Password -> bob123

5. Add one user with randomly generated strong password

Username-> tough

Password-> Mitt@20*00

```
root@VM: ~/test
Other []:
Is the information correct? [Y/n] y
root@VM:~/test# adduser bob
Adding user `bob' ...
Adding new group `bob' (1005) ...
Adding new user `bob' (1005) with group `bob' ...
Creating home directory `/home/bob' ...
Copying files from `/etc/skel' ...
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
Changing the user information for bob
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
root@VM:~/test# adduser tough
Adding user `tough' ...
Adding new group `tough' (1006) ...
Adding new user `tough' (1006) with group `tough' ...
Creating home directory `/home/tough' ...
Copying files from `/etc/skel' ...
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
Changing the user information for tough
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
root@VM:~/test#
```


Cracking the password with John The ripper:

```
root@VM:~/test# time john --wordlist=rockyou.txt /etc/shadow
Loaded 8 password hashes with 8 different salts (crypt, generic crypt(3) [?/32])
Remaining 7 password hashes with 7 different salts
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:03 0% 0g/s 0p/s 105.4c/s 105.4C/s 123456..yellow
0g 0:00:00:06 0% 0g/s 15.00p/s 105.0c/s 105.0C/s daniela..november
0g 0:00:00:08 0% 0g/s 11.41p/s 102.7c/s 102.7C/s daniela..november
0g 0:00:00:10 0% 0g/s 9.266p/s 101.9c/s 101.9C/s daniela..november
diana (person1)
oliver (person2)
bob123 (bob)
3g 0:00:05:41 0% 0.008780g/s 26.41p/s 117.7c/s 117.7C/s jasons..okokok
3g 0:00:05:45 0% 0.008679g/s 26.38p/s 117.4c/s 117.4C/s notredame..rubberducky
3g 0:00:05:46 0% 0.008646g/s 26.28p/s 117.3c/s 117.3C/s notredame..rubberducky
3g 0:00:05:48 0% 0.008615g/s 26.19p/s 117.1c/s 117.1C/s notredame..rubberducky
3g 0:00:05:50 0% 0.008565g/s 26.31p/s 117.0c/s 117.0C/s robinhood..Jonathan
3g 0:00:05:52 0% 0.008516g/s 26.16p/s 116.9c/s 116.9C/s robinhood..Jonathan
3g 0:00:05:53 0% 0.008490g/s 26.08p/s 116.8c/s 116.8C/s robinhood..Jonathan
3g 0:00:06:01 0% 0.008292g/s 26.27p/s 116.4c/s 116.4C/s 101086..juandiego
3g 0:00:06:36 0% 0.007564g/s 26.62p/s 116.9c/s 116.9C/s speed..jesuslives
3g 0:00:06:37 0% 0.007542g/s 26.54p/s 116.8c/s 116.8C/s speed..jesuslives
3g 0:00:06:38 0% 0.007520g/s 26.47p/s 116.7c/s 116.7C/s speed..jesuslives
3g 0:00:06:39 0% 0.007501g/s 26.40p/s 116.6c/s 116.6C/s speed..jesuslives
3g 0:00:06:40 0% 0.007481g/s 26.57p/s 116.5c/s 116.5C/s jesus77..bimbim
3g 0:00:06:42 0% 0.007459g/s 26.49p/s 116.4c/s 116.4C/s jesus77..bimbim
3g 0:00:06:43 0% 0.007438g/s 26.42p/s 116.3c/s 116.3C/s jesus77..bimbim
3g 0:00:06:44 0% 0.007416g/s 26.34p/s 116.2c/s 116.2C/s jesus77..bimbim
```

The other two passwords were not cracked even when the server was running for over 1 hour 30 minutes.

We can infer that the reverse username password can be cracked since there is a possibility that it might be present in the wordlist. But the next password which is the combination of special characters, uppercase, lowercase and numbers is not a surety since its hard to say that this type of password is present in the wordlist.

Also we can check the number of passwords cracked:

```
root@VM:~/test# sudo john --show /etc/shadow
alice:alice:19087:0:99999:7:::
person1:diana:19087:0:99999:7:::
person2:oliver:19087:0:99999:7:::
bob:bob123:19087:0:99999:7:::

4 password hashes cracked, 4 left
root@VM:~/test#
```

END
