Secure System Design: Threats and Countermeasures
CS392

`Date: 26th Mar 2019` — `Assignment 5`

`Submission Filename: assign5.pdf` — `Due Date: 30th Mar 2019`

`Full Marks 40`

1 Assignment 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.

For this experiment, you can use *John The Ripper*[1] tool, also known as `john`. This tool uses a dictionary or a search pattern to check for passwords. To install this tool, you may use the folwoing command

```
$sudo apt-get install john
```

Now, use *su* command and change to root. After then, create a folder named *test*. Change its permission to 777 by using *chmod* command.

Now, goto *test* folder and get a *wordlist* dictionary. You can use the following command to get a dictionary of *wordlist*.

```
#wget http://scrapmaker.com/data/wordlists/dictionaries/rockyou.txt
```

Once the *wordlist* file is downloaded then you can add user using *adduser* command and create an account for a new user. Let's create an account with username `alice` and password `alice`. You can check */etc/shadow* file to check the entry of that new user's account. The password of that new user is now stored using salted hash function. Now, we can use `john` to find whether the password can be cracked or not. If it is available in the *wordlist* file then it should show the corresponding password against the username. For this following command can be used-

```
#john --wordlist=rockyou.txt /etc/shadow
```

This will try to explore all the hashed entries of */etc/shadow* with specified *rockyou wordlist*. Please note that it is a time taking task. If no *wordlist* is specified then system will use the default *wordlist*. Also, if you want to check the already cracked passwords from a password file then the following command can be used

```
$sudo john --show passwordFilename
```

Now, add 5 users as per followings-

- Add two users and their passwords will be chosen from the *rockyou wordlist* file.
- Add one user with password as the reverse of the *username*.
- Add one user with password as the 123 extension of the *username*. So if the *username* is *bob* then password will be *bob123*
- Add one user with randomly generated strong password

Now your task is to crack the passwords using `john` tool. Report whether you can crack all the passwords and also the time needed to crack them. To check time requirement, you can use the *time* command.

2 Submission

You need to submit a detailed report to describe what you have done and what you have observed; you also need to provide explanation to the observations that are interesting or surprising. Attach supporting snapshots wherever possible.

[1] http://www.openwall.com/john/