**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

Text

Description automatically generated

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

Text

Description automatically generated

3. Download the wordlist dictionary

Text

Description automatically generated

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

Text

Description automatically generated

Checking etc/shadow:

Text

Description automatically generated

A screenshot of a computer

Description automatically generated

5. Cracking the password for alice using john the ripper

P.T.O

A screenshot of a computer

Description automatically generated with medium confidence

Here we can see that password for alice is cracked

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

A screenshot of a computer

Description automatically generated with medium confidence

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

Text

Description automatically generated

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

Username -> tarusi

Password-> isurat

Text

Description automatically generated

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

A screenshot of a computer

Description automatically generated

Cracking the password with John The ripper:

A screenshot of a computer

Description automatically generated with medium confidence

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:

A screenshot of a computer

Description automatically generated with medium confidence

END