UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA

COS 330

September 5, 2016

Practical 3

Release Date: 05 September 2016

Due Date: 21 September 2016

Submission Deadline: 20 September 2016

Instructions

In this practical we are going to use **the Kali Linux virtual machine** and the tool '**hashcat**' provided with Kali to show how vulnerable weak passwords are when the password hash is available. Virtual box will be available to run Kali Linux on in the orange labs as of Monday 05/09/2016.

Add your own user account in Kali with the command **'adduser uxxxxxxxx'** where **xxxxxxxx** is your student number. Make the password your student number in the format xxxxxxxx. If you already have created your own account as uxxxxxxxx, you can change the password with the command **'passwd uxxxxxxxx'**.

Note: The aim of this practical is NOT to test anything other than Computer Security concepts that you are expected to know by now.

Upload a zip archive of your screenshots and your answers onto the CS website by the above-mentioned due date. If you do not demonstrate your work in one of the practical sessions, then you will not be allocated any marks (even if you did upload), i.e. you must be present in person at the demo session to be able to receive a mark. Also, you might need to re-run some of the commands during your demo should there be any uncertainties with your marker.

Note: All screenshots need to show your student number in the title to receive marks. To achieve that, you need to be logged in with your own user account.

Caution: For this exercise, do not use any of your real personal passwords. All passwords need to be newly created during this practical so as not to give away your real passwords

Everything that you submit might be checked for plagiarism. Instances of plagiarism will be dealt with in a serious manner.

Background

Using passwords to protect sensitive assets is seen as a safe practice. However, the effectiveness of this practice depends on the strength and complexity of the password as well as how long the password is kept. The following tasks will practically expose you to how weak passwords can easily be exploited.

Task 1 [5 Marks]

Retrieve the password hashes provided from the members.sql file. Place the hashes in your own file. Use hashcat to brute-force the passwords as efficiently as possible (hint - use 'hashcat -h' and online documentation, password length is 5 characters). Provide the following for your answer:

1. Hash type used by Practical 2. [1]
2. Hashcat command line with parameters used. [2]
3. Screenshot of hashcat clearly showing all the retrieved passwords (admin and all users) and time elapsed. [2]

Task 2 [5 Marks]

Find the password hash for the root account on your Kali Linux virtual machine (hint - look at '/etc/shadow' as root). Place the hash in your own file (hint - consult online documentation for shadow file format and look in '/etc/login.defs'). Use hashcat to brute-force the password as efficiently as possible. Provide the following for your answer:

1. Hash type used by Kali Linux. [1]
2. Hashcat command line with parameters used. [2]
3. Screenshot of hashcat clearly showing the retrieved password (root) and time elapsed. [2]

Task 3 [4 Marks]

Now use hashcat on the password hash of your own account. Show that the chosen password is weak if the format is known. Provide the following for your answer:

1. Hashcat command line with parameters used. [2]
2. Screenshot of hashcat running (status) with time left estimation. [2]

Task 4 [6 Marks]

Change your password to a strong password. Use hashcat to motivate that the chosen password is strong. Provide the following for your answer:

1. Your chosen password. [2]
2. Hashcat command line with parameters used. [2]
3. Screenshot of hashcat running (status) with time left estimation. [2]

Upload Instruction: Put your answers as well as your screenshots for tasks 1 to 4 into a single document and upload a zipped copy of the document.

Total Marks [20 Marks]