Rainbow Table Attack: Cracking UNIX Passwords

|  |
| --- |
| Copyrights 2016-2017 Frank Xu, Bowie State University.  The lab manual is developed for teaching cyber-related courses. Comments and suggestions can be sent to wxu@bowiestate.edu |

**Lab Environment**

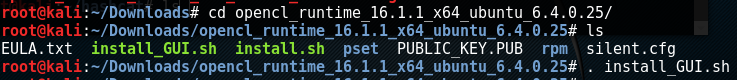
1. Following the tutorial to install Kali Linux. <https://www.youtube.com/watch?v=GpTIM9OroIY>
2. You can set the root as:

* Username: root
* Password: dees

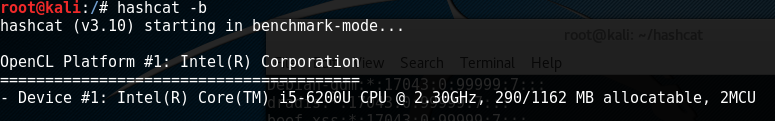
1. Prerequisite

You need the OpenCL Intel runtime. http://registrationcenter-download.intel.com/akdlm/irc\_nas/9019/opencl\_runtime\_16.1.1\_x64\_ubuntu\_6.4.0.25.tgz. The main page is https://software.intel.com/en-us/articles/opencl-drivers, Just use the Ubuntu version for Kali, It will say its unsupported but will install anyways. And it works!!



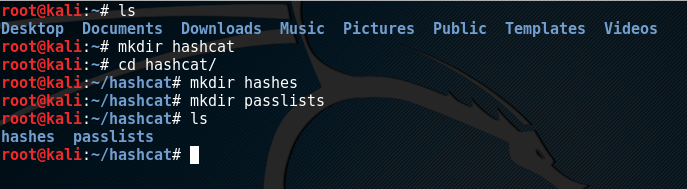


1. Type to check the configuration: hashcat –b

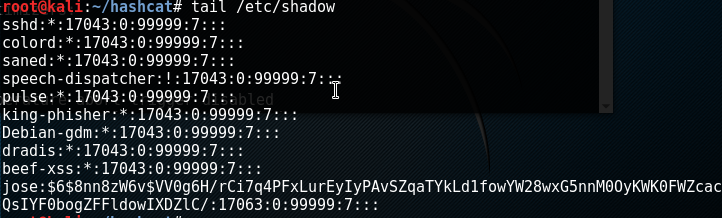


**Task 1: Crack Password Using Brute Force**

1. Create folders.
   1. mkdir hashcat
   2. mkdir hashes

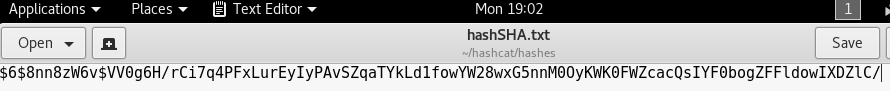


1. Create a new user Jose with a password (e.g., 12345)
   1. adduser –m jose
   2. passwd jose
2. Viewing the Password Hash. Look at the salt following the username "jose". The $6$ value indicates a type 6 password hash (SHA-512, many rounds). The characters after $6$, up to the next $, are the SALT. In my example, the SALT is

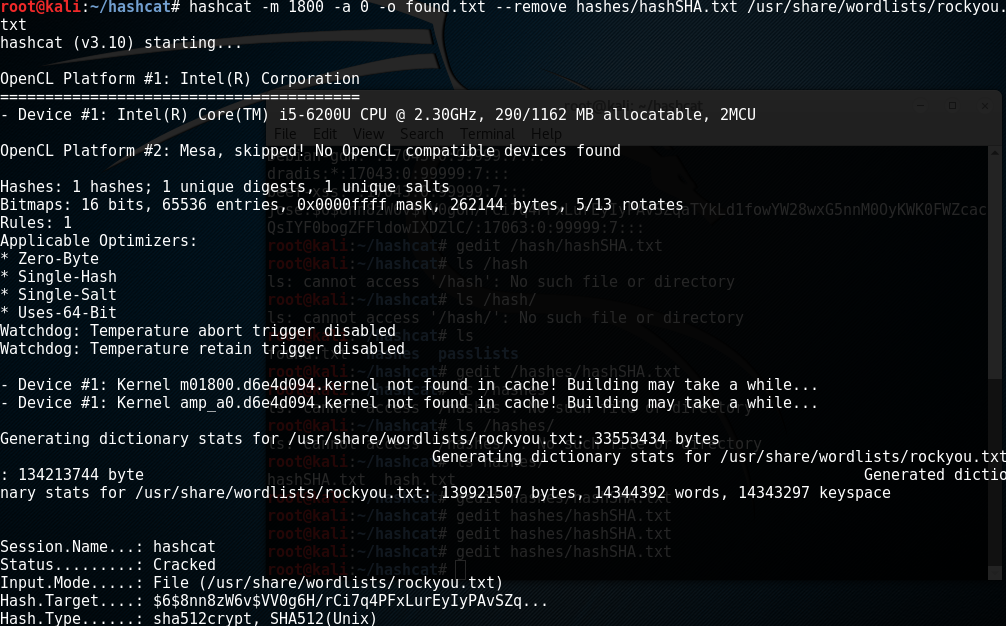


1. Save the hashed password to a file: hashes/hashSHA.txt

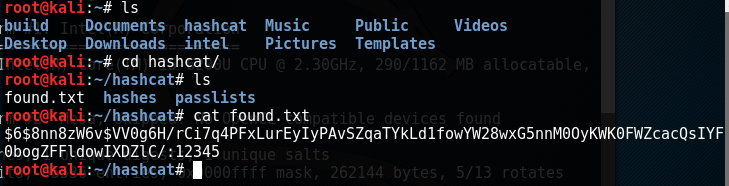




1. Type following command to decryption
   1. Rockyou.txt is a password dictionary
   2. You need to check if the password dictionary exists.
      1. find –iname rockyou.\*
      2. if the file ends with .gz, you need to unzip it



1. Questions: Explain the following parameters
   * m
   * 1800
   * a
   * 0
   * remove
   * o



Reference

* <https://bugs.kali.org/view.php?id=3432>
* https://samsclass.info/123/proj10/px16-hashcat-win.htm