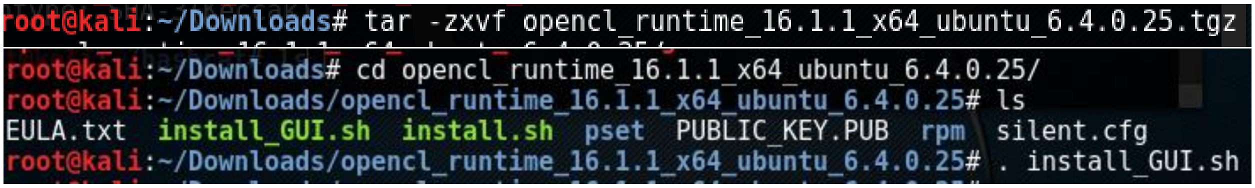
Rainbow Table Attack: Cracking UNIX Passwords

Lab Environment

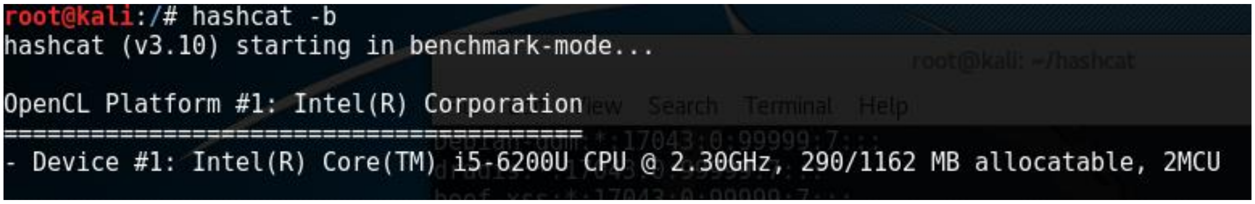
1. Following the tutorial to install Kali Linux. https://www.youtube.com/watch?v=GpTIM9OroIY
2. You can set the root as:
    - Username: root
    - Password: dees
3. Prerequisite

    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!!



```
root@kali:~/Downloads# tar -zxvf opencl_runtime_16.1.1_x64_ubuntu_6.4.0.25.tgz
root@kali:~/Downloads# cd opencl_runtime_16.1.1_x64_ubuntu_6.4.0.25/
root@kali:~/Downloads/opencl_runtime_16.1.1_x64_ubuntu_6.4.0.25# ls
EULA.txt  install_GUI.sh  install.sh  pset  PUBLIC_KEY.PUB  rpm  silent.cfg
root@kali:~/Downloads/opencl_runtime_16.1.1_x64_ubuntu_6.4.0.25# . install_GUI.sh
```

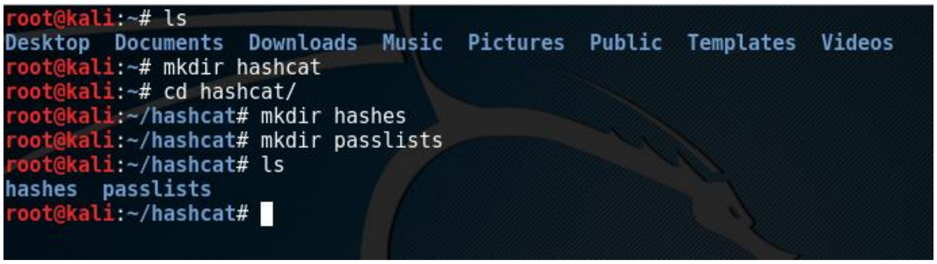
4. Type to check the configuration: hashcat –b



```
root@kali:/# hashcat -b
hashcat (v3.10) starting in benchmark-mode...

OpenCL Platform #1: Intel(R) Corporation
========================================
- Device #1: Intel(R) Core(TM) i5-6200U CPU @ 2.30GHz, 290/1162 MB allocatable, 2MCU
```

Task 1: Crack Password Using Brute Force

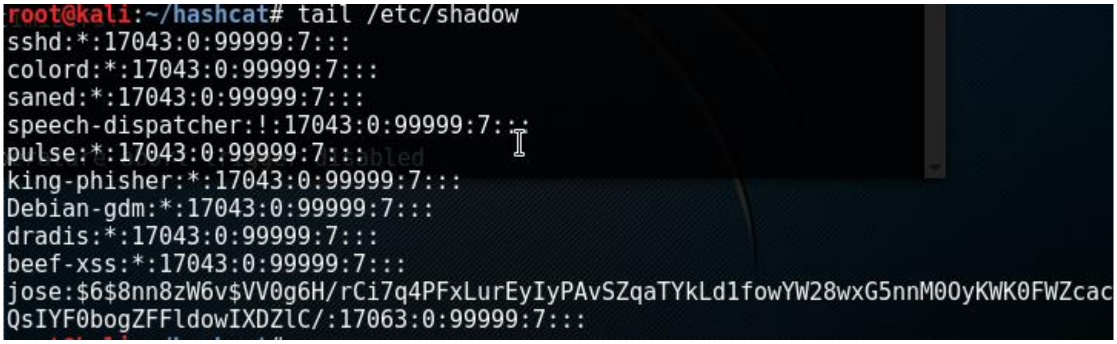
1. Create folders.
    1.1. mkdir hashcat
    1.2. mkdir hashes



```
root@kali:~# ls
Desktop  Documents  Downloads  Music  Pictures  Public  Templates  Videos
root@kali:~# mkdir hashcat
root@kali:~# cd hashcat/
root@kali:~/hashcat# mkdir hashes
root@kali:~/hashcat# mkdir passlists
root@kali:~/hashcat# ls
hashes  passlists
root@kali:~/hashcat# 
```

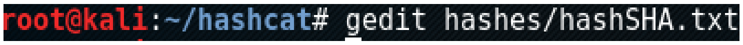
2. Create a new user Jose with a password (e.g., 12345)
   2.1 adduser –m jose
   2.2 passwd jose

3. 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 $, are the SALT. In my example, the SALT is 8nn8zW6v$VV0g6H

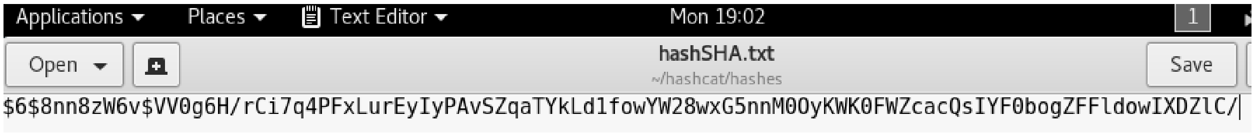


```
root@kali:~/hashcat# tail /etc/shadow
sshd:*:17043:0:99999:7:::
colord:*:17043:0:99999:7:::
saned:*:17043:0:99999:7:::
speech-dispatcher:!:17043:0:99999:7:::
pulse:*:17043:0:99999:7:::
king-phisher:*:17043:0:99999:7:::
Debian-gdm:*:17043:0:99999:7:::
dradis:*:17043:0:99999:7:::
beef-xss:*:17043:0:99999:7:::
jose:$6$8nn8zW6v$VV0g6H/rCi7q4PFxLurEyIyPAvSZqaTYkLd1fowYW28wxG5nnM0OyKWK0FWZcac
QsIYF0bogZFFldowIXDZlC/:17063:0:99999:7:::
```

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

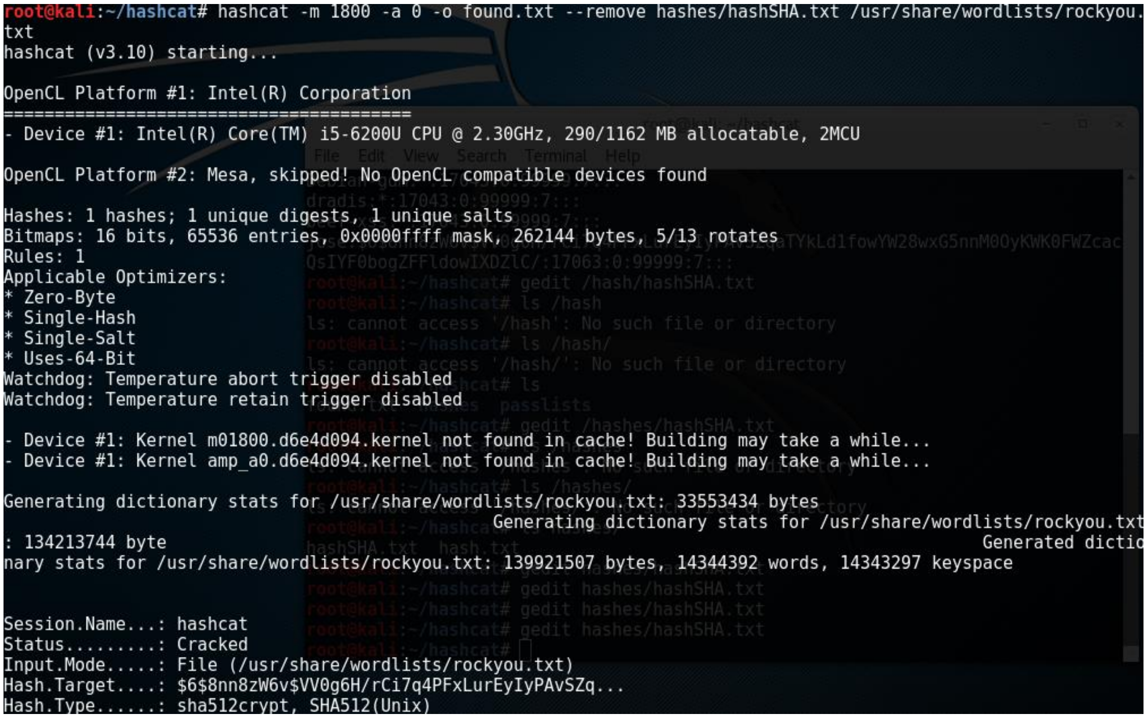


```
root@kali:~/hashcat# gedit hashes/hashSHA.txt
```



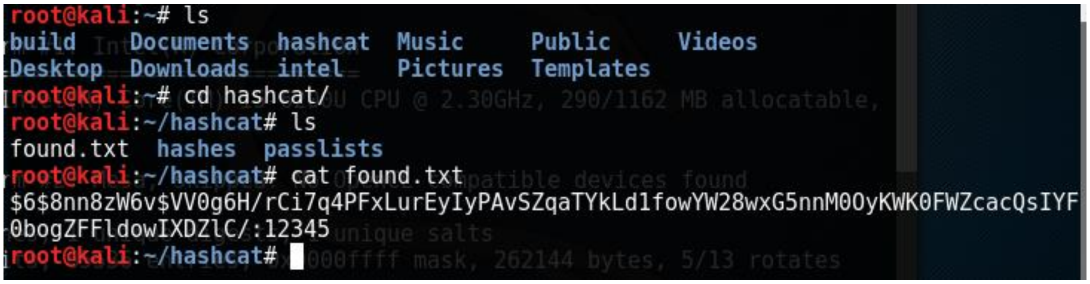
```
$6$8nn8zW6v$VV0g6H/rCi7q4PFxLurEyIyPAvSZqaTYkLd1fowYW28wxG5nnM0OyKWK0FWZcacQsIYF0bogZFFldowIXDZlC/
```

5. Type following command to decryption
   5.1. Rockyou.txt is a password dictionary
   5.2. You need to check if the password dictionary exists.
      5.2.1. find –iname rockyou.*
      5.2.2. if the file ends with .gz, you need to unzip it



```
root@kali:~/hashcat# hashcat -m 1800 -a 0 -o found.txt --remove hashes/hashSHA.txt /usr/share/wordlists/rockyou.
txt
hashcat (v3.10) starting...

OpenCL Platform #1: Intel(R) Corporation
========================================
- Device #1: Intel(R) Core(TM) i5-6200U CPU @ 2.30GHz, 290/1162 MB allocatable, 2MCU

OpenCL Platform #2: Mesa, skipped! No OpenCL compatible devices found

Hashes: 1 hashes; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1
Applicable Optimizers:
* Zero-Byte
* Single-Hash
* Single-Salt
* Uses-64-Bit
Watchdog: Temperature abort trigger disabled
Watchdog: Temperature retain trigger disabled

- Device #1: Kernel m01800.d6e4d094.kernel not found in cache! Building may take a while...
- Device #1: Kernel amp_a0.d6e4d094.kernel not found in cache! Building may take a while...

Generating dictionary stats for /usr/share/wordlists/rockyou.txt: 33553434 bytes
                                                 Generating dictionary stats for /usr/share/wordlists/rockyou.txt
: 134213744 byte                                                                                  Generated dictio
nary stats for /usr/share/wordlists/rockyou.txt: 139921507 bytes, 14344392 words, 14343297 keyspace


Session.Name...: hashcat
Status.........: Cracked
Input.Mode.....: File (/usr/share/wordlists/rockyou.txt)
Hash.Target....: $6$8nn8zW6v$VV0g6H/rCi7q4PFxLurEyIyPAvSZq...
Hash.Type......: sha512crypt, SHA512(Unix)
```

6. Questions: Explain the following parameters
   - m
   - 1800
   - a
   - 0
   - remove
   - o



```
root@kali:~# ls
build    Documents  hashcat  Music     Public     Videos
Desktop  Downloads  intel    Pictures  Templates
root@kali:~# cd hashcat/
root@kali:~/hashcat# ls
found.txt  hashes  passlists
root@kali:~/hashcat# cat found.txt
$6$8nn8zW6v$VV0g6H/rCi7q4PFxLurEyIyPAvSZqaTYkLd1fowYW28wxG5nnM0OyKWK0FWZcacQsIYF
0bogZFFldowIXDZlC/:12345
root@kali:~/hashcat# 
```

Reference

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