**Cracking Linux Password Hashes with Hashcat**

**What You Need for This Project**

* An Ubuntu machine, Physical or virtual

*Note: Kali Linux seems to run into issues with Hashcat.*

**Part 1**

1. **Updating Hashcat**

Hashcat won't let you run an old version.

In a Terminal window, execute this command:

**ping google.com**

You should see replies, saying "64 bytes from...". If you don't, you need to troubleshoot your networking.

In a Terminal window, execute these commands:

**apt-get update**

**sudo apt install hashcat**

**sudo apt install curl**

1. **Creating a Test User**

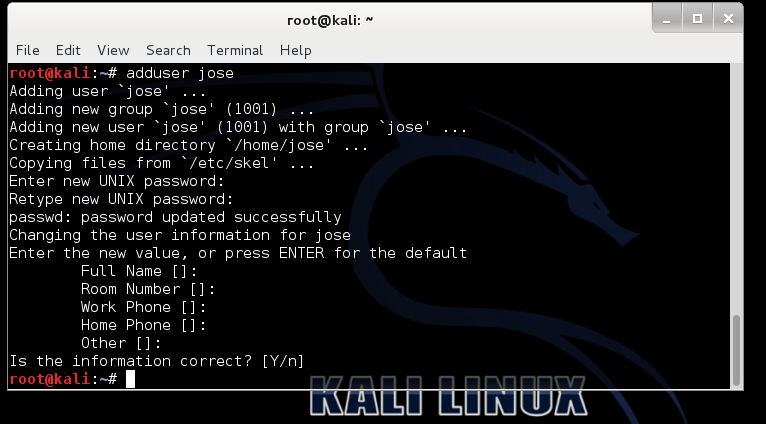
In a Terminal window, execute this command:

**sudo adduser jose**

At the "Enter new UNIX password" enter a password of **password**

At the "Retype new UNIX password" enter a password of **password**

Press Enter to accept defaults for the other options, as shown below:

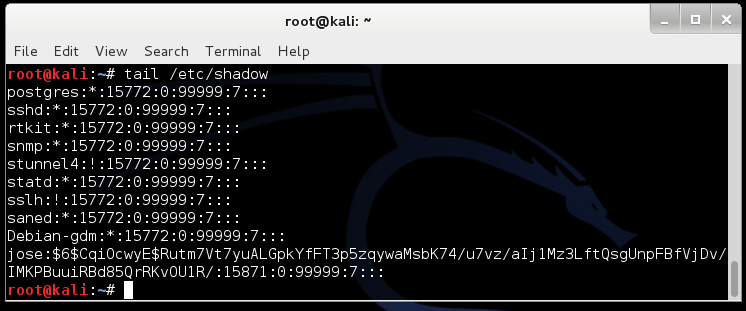


1. **Viewing the Password Hash**

In a Terminal window, execute this command:

**sudo tail /etc/shadow**

The last line shows the password hash for jose, as shown below (your hash will be different):



1. **Finding Your Salt Value**

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.

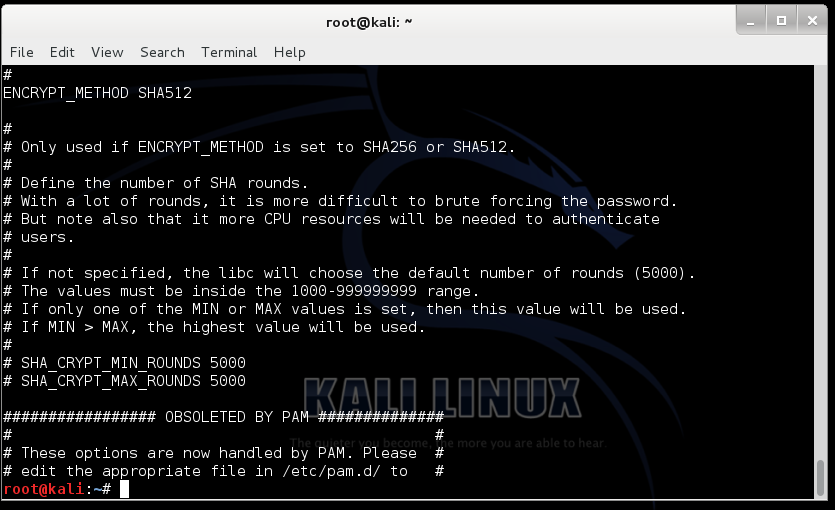
In my example, the SALT is **CqiOcwyE**

1. **Understanding the Hash Algorithm**

The hash algorithm is defined in the file /etc/login.defs. To see the portion of that file discussing the password hash algorithm, execute this grep command to see 18 lines after the line containing the string "ENCRYPT\_METHOD":

**grep -A 18 ENCRYPT\_METHOD /etc/login.defs**

As you can see, Ubuntu uses SHA-512 hashes, with the default value of 5000 rounds:



1. **Making a Hash File**

In a Terminal window, execute these commands:

**tail -n 1 /etc/shadow > crack1.hash**

**nano crack1.hash**

In the nano text editor, carefully delete the username **jose** and the colon after it, and all the text at the end of the file, including all the colons, leaving only the hash, as shown below:

Press **Ctrl+X**, **Y**, **Enter** to save the file.

1. **Dowloading a Wordlist**

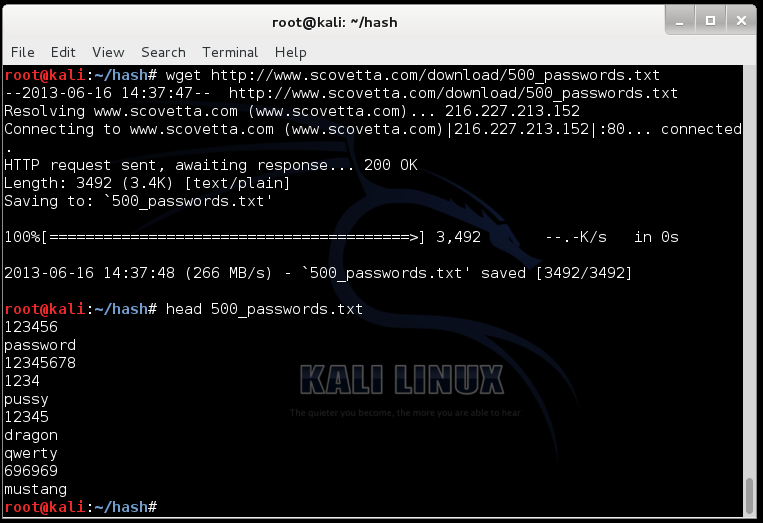
We'll use a very decent size list of over 14 million common passwords.

In a Terminal window, execute these commands:

**curl http://faculty.washington.edu/marcjd/rockyou.txt > rockyou.txt**

**head rockyou.txt**

You should see the first ten passwords, as shown below:



1. **Cracking the Hash**

In a Terminal window, execute these commands:

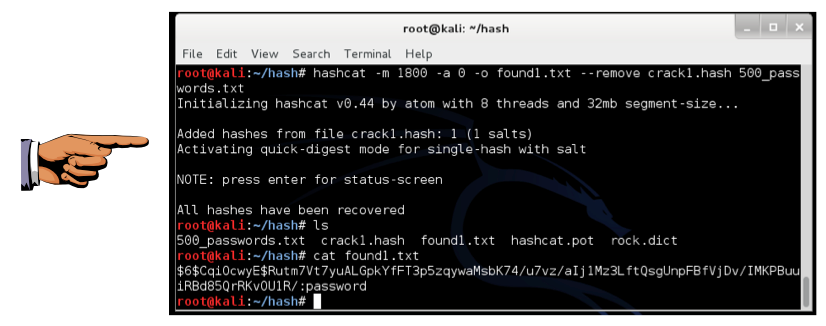
**hashcat -m 1800 -a 0 -o found1.txt --remove crack1.hash rockyou.txt --force**

**cat found1.txt**

Explanation: This uses hashcat with these options:

* Unix type 6 password hashes (-m 1800)
* Using a dictionary attack (-a 0)
* Putting output in the file **found1.txt**
* Removing each hash as it is found
* Getting hashes from **crack1.hash**
* Using the dictionary **rockyou.txt**

You should see the hash, with the cracked password of "**password**" at the end, as shown below:



1. **Saving a Screen Image**

Make sure the Terminal window is visible, showing the cracked password of "**password**".

Click on the host machine's desktop, outside the virtual machine to make the host machine's desktop active.

Press the PrintScrn key to copy the whole desktop to the clipboard.

**YOU MUST SUBMIT A FULL-SCREEN IMAGE FOR FULL CREDIT.**

In the host machine, open Paint and paste in the captured image.

Save it as "**Your Name - Hashcat.jpg**".

**PART 2**

**Getting the crack.hash List**

**Following the lessons learned from above, let’s crack the following hashes:**

**$6$NShHCRTL$lAe9dI1rtpAXQkiMPqncpCQ69gE7Y25TgKRDvtfIOdLVTlG4cMAp9LQE9eEZuboS4tO6ippBnOIFE8zgqOvGP0**

**$6$ssMb25ys$yuyoQKJaaGeRVhwsklDAvWnJLcgZxiTX7mrxH.8xCslnGcCbB3S0gLic3qlyOGWCZImFI3KW29p1Ht7ny9Jwo/**

**$6$sH2VWpHm$cEvtk3IffFilT73amGGv7/6j2LRWHQ7df4vjgoSuOSEt8QZDeDDYxCqlly.cU8/AfL/ulYmX/42QI.etA8fdV1**

**$6$E5s/79nO$HLNy0xElpbp7Dx4537KCsAlAER.wULMLLS1vzgmkVyp1ZK/fK/.td819Ea1RFhMBLfsQXvFM0HfMW3k3oF4ob.**

**To do this, we need to place the above hash values into a file. I have already done this. We just need to get it in Ubuntu.**

**Go ahead and type the following:**

**curl http://faculty.washington.edu/marcjd/crack2.hash > crack2.hash**

**Then, type the following:**

**hashcat -m 1800 -a 0 -o found2.txt --remove crack2.hash rockyou.txt --force**

**cat found2.txt**

**After cracking the passwords take a screenshot and save it as “Your Name – Hashcat - 2.jpg”. Upload your screenshots in Canvas.**

* Hashcat Wiki page with options: <https://hashcat.net/wiki/doku.php?id=hashcat>