Colombia Hack Agent (CHackA)

[...]	Developer:	Jairo A. García H.	[...]
[...]	Version:	1.0.	[...]
[...]	Codename:	HACKLAB CRACKING HASH JOHN THE RIPPER	[...]
[...]	Report to:	chacka0101 @ gmail.com	[...]
[...]	Homepage:	https://github.com/chacka0101/HACKLABS	[...]
[...]	Publication Date:	20/Abr/2019	[...]

HACKLAB PARA CRACKING HASH CON JOHN THE RIPPER

Resumen: Realizaremos un HackLab para crackear los Hash con el software Jhon The Ripper.

John the Ripper es un programa de criptografía que aplica fuerza bruta para descifrar Hash de contraseñas. Es capaz de romper varios algoritmos de cifrado o hash, como DES, SHA-1, entre otros.

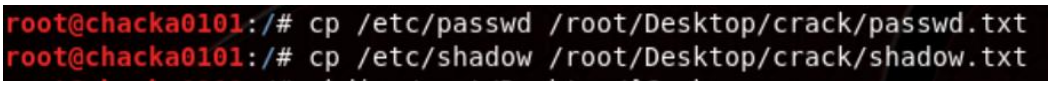
Aplica para: **KALI LINUX 2019.1**

1. Creamos un directorio para almacenar los archivos que estemos trabajando:

```
root@chacka0101:/# mkdir /root/Desktop/crack
```

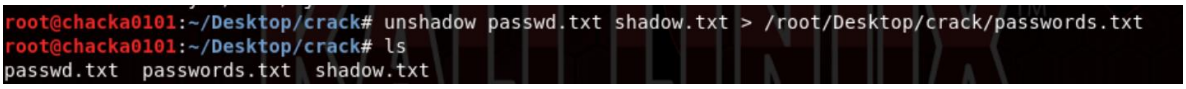
2. Copiamos los directorios de passwd y shadow, archivos los cuales contienen los HASH de las contraseñas de Kali Linux y los convertimos en .txt:

```
root@chacka0101:/# cp /etc/passwd /root/Desktop/crack/passwd.txt
root@chacka0101:/# cp /etc/shadow /root/Desktop/crack/shadow.txt
```



3. Utilizaremos Unshadow para combinar los archivos passwd y shadow en formato Jhon The Ripper. Crearemos un nuevo archivo de texto llamado passwords.txt.

```
root@chacka0101:/# unshadow passwd.txt shadow.txt > /root/Desktop/crack/passwords.txt
```

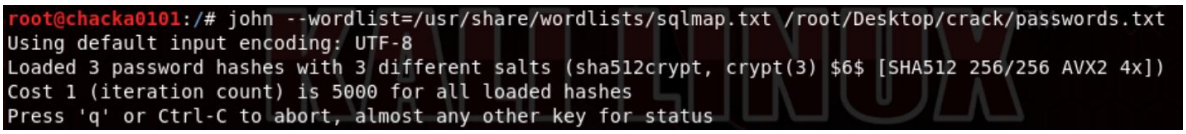


4. En Kali Linux existe un directorio llamado /usr/share/wordlists el cual contiene archivos con listas de palabras o posibles contraseñas que podemos utilizar. Para este hacklab vamos a utilizar la lista de sqlmap.txt, sin embargo, podemos crear una lista personalizada o también utilizar la que gusten.

También puede comprarlas u obtenerlas en: https://www.openwall.com/wordlists/

5. Para ejecutar el desciframiento de los Hash, ejecutamos el comando de Jhon The Ripper:

```
root@chacka0101:/#          john          --wordlist=/usr/share/wordlists/sqlmap.txt
/root/Desktop/crack/passwords.txt
```



Esperamos pacientemente, jeje.

6. Finalmente, el software Jhon The Ripper con sus algoritmos de desciframeinto logra revelar las contraseñas de las tres cuentas de usuario dentro de los archivos analizados.

7. Para consultar información de referencia:

https://www.openwall.com/john/

Agradecimientos a:

Kali Linux - https://www.kali.org/
Jhon The Ripper - https://www.openwall.com/john/

-END-