

Práctica de laboratorio: decodificación de contraseñas

Objetivos

Utilice una herramienta de decodificación de contraseñas para recuperar la contraseña de un usuario.

Aspectos básicos/situación

Existen cuatro cuentas de usuario: Alice, Bob, Eve y Eric, en un sistema Linux. Usted recuperará estas contraseñas mediante el uso de John el Destripador, una herramienta de decodificación de contraseñas de código abierto.

Recursos necesarios

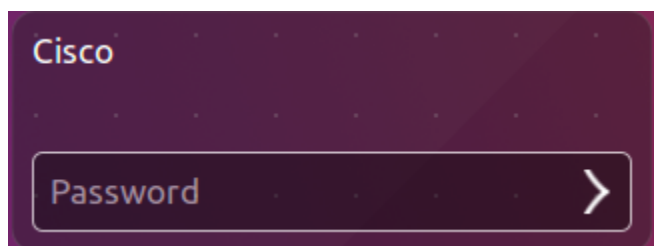
- Computadora con sistema Ubuntu 16.04.4 Desktop LTS instalado en una máquina virtual de VirtualBox o VMware.

Paso 1: Abra una ventana del terminal en Ubuntu.

- Inicie sesión en Ubuntu con las siguientes credenciales:

Usuario: **cisco**

Contraseña: **password**



- Haga clic en el icono de terminal para abrir el terminal.



Paso 2: Ejecutar John el Destripador.

- En la petición de ingreso de comandos, ingrese el siguiente comando para cambiar el directorio donde se encuentra John el Destripador:

```
cisco@ubuntu:~$ cd ~/Downloads/john-1.8.0/run
```

- En la petición de ingreso de comando, introduzca el siguiente comando:

```
cisco@ubuntu:~/Downloads/john-1.8.0/run$ sudo ./unshadow /etc/passwd  
/etc/shadow > mypasswd
```

```
cisco@ubuntu:~/Downloads/john-1.8.0/run$ sudo ./unshadow /etc/passwd /etc/shadow > mypasswd
```

Este comando combinará el archivo `/etc/passwd` donde se almacenan las cuentas de usuario, con el archivo `/etc/shadow` donde se almacenan las contraseñas de usuarios, en un nuevo archivo denominado "mypasswd".

Paso 3: Recuperar contraseñas.

- Escriba el siguiente comando en el terminal.

```
cisco@ubuntu:~/Downloads/john-1.8.0/run$ ./john --show mypasswd
```

```
cisco@ubuntu:~/Downloads/john-1.8.0/run$ ./john --show mypasswd  
0 password hashes cracked, 5 left
```

Como se muestra arriba, no existen contraseñas de decodificación en este punto.

- En la petición de ingreso de comando, introduzca el siguiente comando:

```
cisco@ubuntu:~/Downloads/john-1.8.0/run$ ./john --wordlist=password.lst --  
rules mypasswd --format=crypt
```

```
cisco@ubuntu:~/Downloads/john-1.8.0/run$ ./john --wordlist=password.lst --rules mypasswd --format=crypt
```

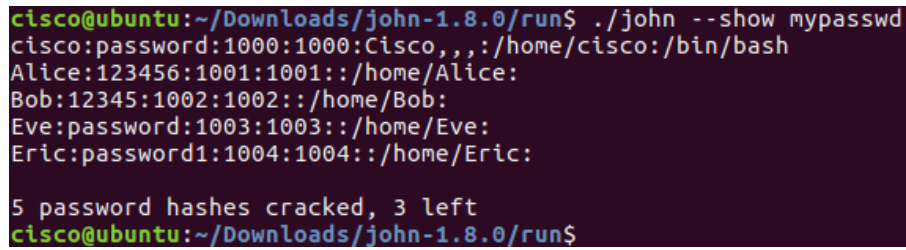
El programa, John el Destripador, utiliza un diccionario predefinido llamado **password.lst** con un conjunto estándar de «reglas» predefinidas para administrar el diccionario y recupera todos los hashes de la contraseña de md5crypt y el tipo de cifrado.

Los resultados a continuación muestran las contraseñas de cada cuenta.

```
Loaded 8 password hashes with 8 different salts (crypt, generic crypt(3) [?/64])  
Press 'q' or Ctrl-C to abort, almost any other key for status  
password1      (Eric)  
12345          (Bob)  
123456         (Alice)  
password       (cisco)  
password       (Eve)  
5g 0:00:20:50 100% 0.003998g/s 125.4p/s 376.6c/s 376.6C/s Tnting..Sssing  
Use the "--show" option to display all of the cracked passwords reliably  
Session completed
```

- c. En la petición de ingreso de comando, introduzca el siguiente comando:

```
cisco@ubuntu:~/Downloads/john-1.8.0/run$ ./john --show mypasswd
```



```
cisco@ubuntu:~/Downloads/john-1.8.0/run$ ./john --show mypasswd
cisco:password:1000:1000:Cisco,,,:/home/cisco:/bin/bash
Alice:123456:1001:1001:./home/Alice:
Bob:12345:1002:1002:./home/Bob:
Eve:password:1003:1003:./home/Eve:
Eric:password1:1004:1004:./home/Eric:

5 password hashes cracked, 3 left
cisco@ubuntu:~/Downloads/john-1.8.0/run$
```

¿Cuántas contraseñas se decodificaron?

Referencias

John el Destripador: <http://www.openwall.com/john/>