

Práctica: Auditoría de contraseñas en Windows

Objetivos

Aprender a auditar como administrador, la fortaleza de las contraseñas de los usuarios en un sistema Windows.

Preparación

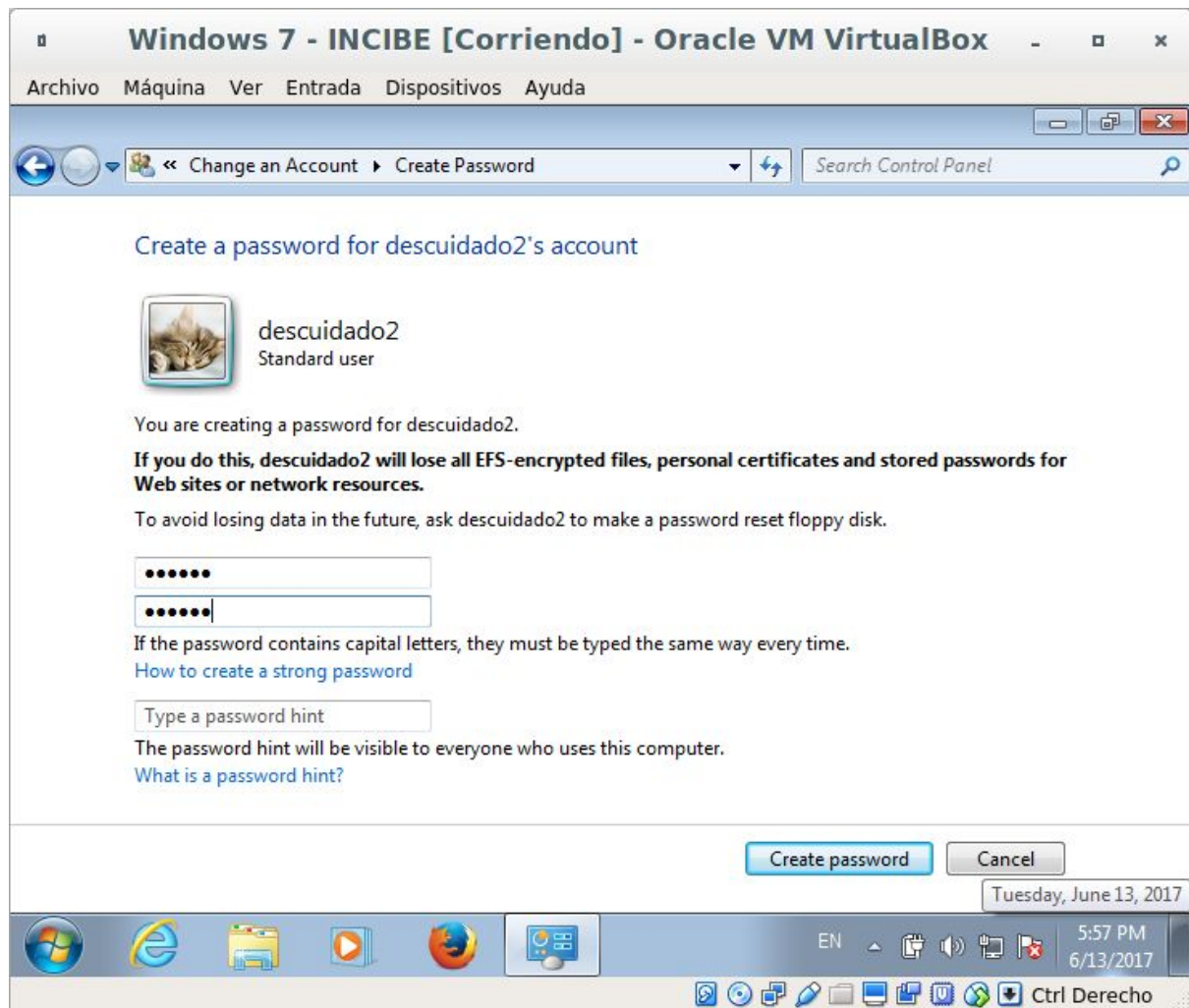
Descargar la herramienta **Pwdump7**. Necesitarás también un sistema **Windows inferior a Windows 10**, debido a que a partir de Windows 10 con la Anniversary Update instalada, se cambia el sistema de cifrado de los hashes en la SAM, que pasa a usar AES en vez de RC4, por lo que de momento pwdump7 no funciona con Windows 10

Enunciado

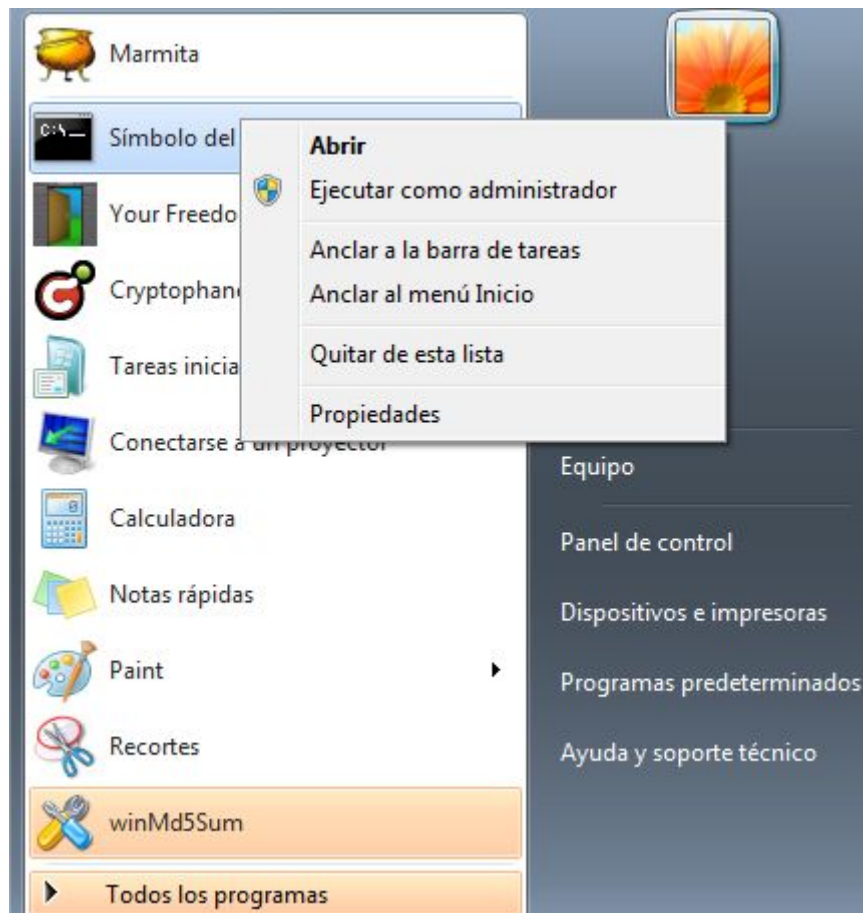
Utiliza la herramienta **pwdump7** para obtener los hashes de los usuarios de tu sistema con Windows (si no usas Windows, puedes hacerlo con una máquina virtual o un ordenador con Windows de tu centro). El objetivo es auditar la fortaleza de las contraseñas de tu sistema.

Instrucciones:

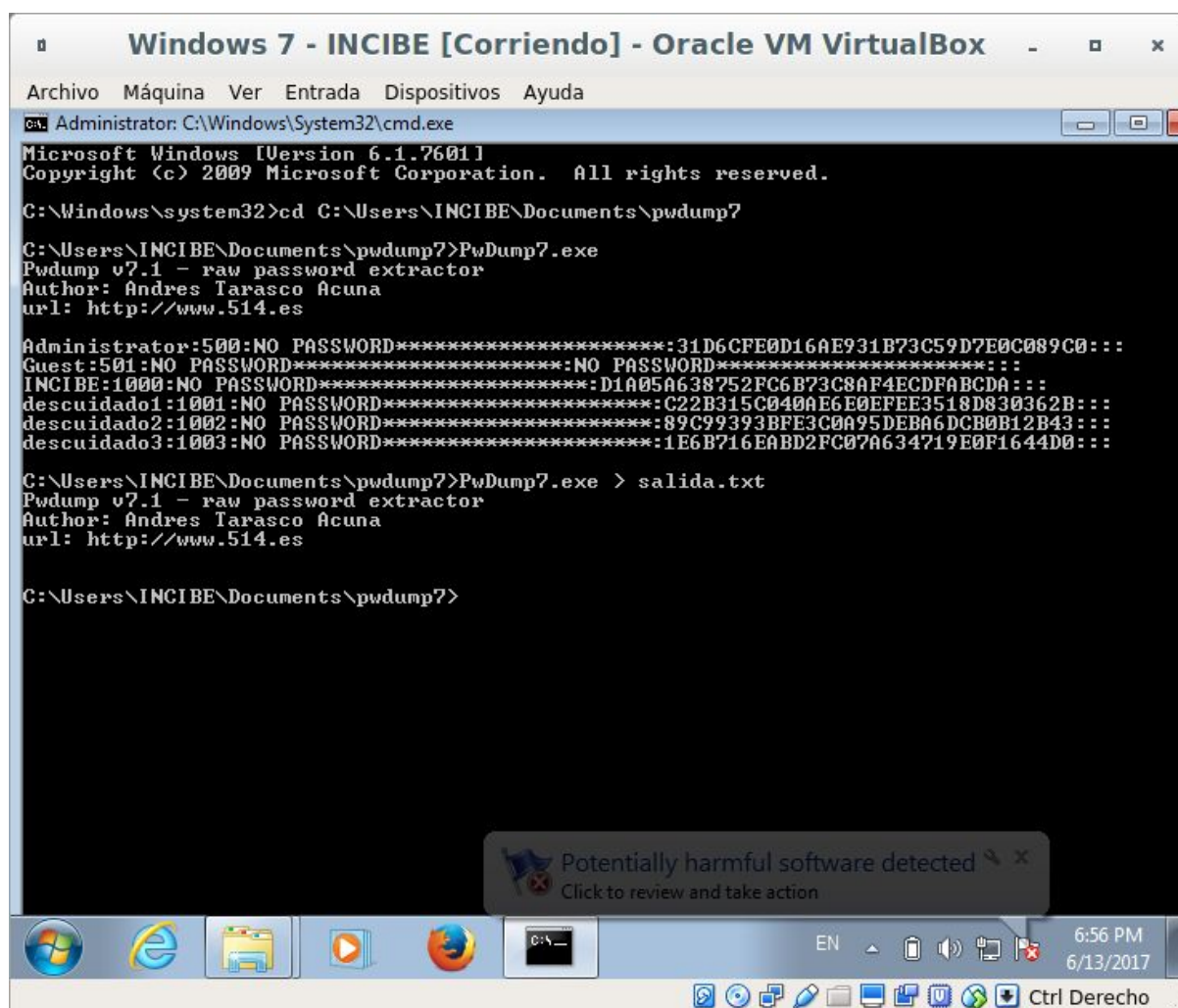
1. Debes acceder a Windows con un usuario que pertenezca a Administradores del equipo. Crea unos cuantos usuarios en tu sistema con contraseñas débiles del tipo 0123456789 o abc123, etc. Lo puedes hacer desde clic con el botón derecho en Equipo o Mi PC -> Administrar -> Usuarios y grupos locales -> botón derecho en carpeta Usuarios -> Usuario nuevo...



2. Ejecuta CMD (línea de comandos de Windows) como administrador haciendo clic con el botón derecho y haciendo clic en "Ejecutar como administrador":



3. Lanza pwddump7 desde la ruta donde lo hayas descomprimido. Puedes usar el comando `cd` para cambiar al directorio correspondiente, como en el siguiente ejemplo:



```
Windows 7 - INCIBE [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
ca. Administrator: C:\Windows\System32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Windows\system32>cd C:\Users\INCIBE\Documents\pwdump7

C:\Users\INCIBE\Documents\pwdump7>Pwdump7.exe
Pwdump v7.1 - raw password extractor
Author: Andres Tarasco Acuna
url: http://www.514.es

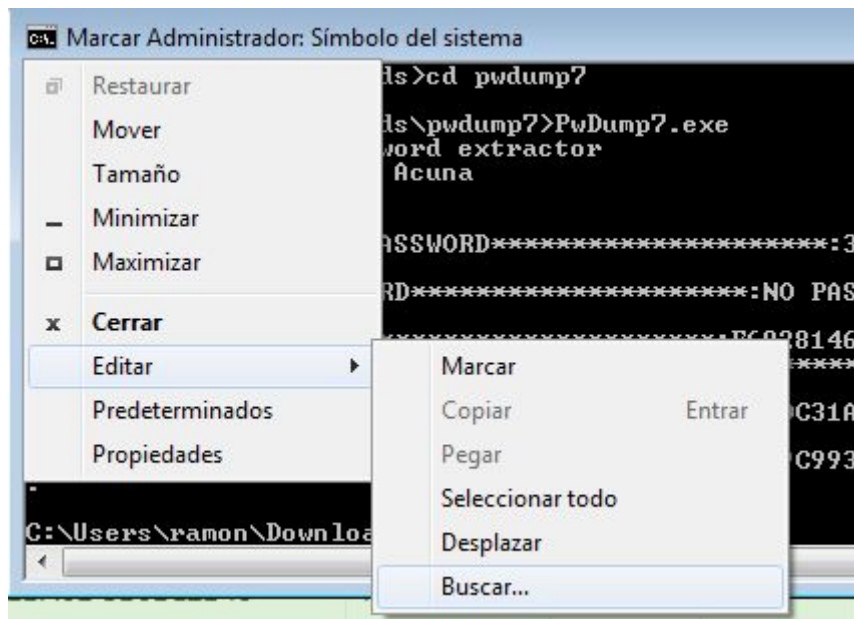
Administrator:500:NO PASSWORD*****:31D6CFE0D16AE931B73C59D7E0C089C0:::
Guest:501:NO PASSWORD*****:NO PASSWORD*****:
INCIBE:1000:NO PASSWORD*****:D1A05A638752FC6B73C8AF4ECDFABCD:::
descuidado1:1001:NO PASSWORD*****:C22B315C040AE6E0EFEE3518D830362B:::
descuidado2:1002:NO PASSWORD*****:89C99393BFE3C0A95DEBA6DCB0B12B43:::
descuidado3:1003:NO PASSWORD*****:1E6B716EABD2FC07A634719E0F1644D0:::

C:\Users\INCIBE\Documents\pwdump7>Pwdump7.exe > salida.txt
Pwdump v7.1 - raw password extractor
Author: Andres Tarasco Acuna
url: http://www.514.es

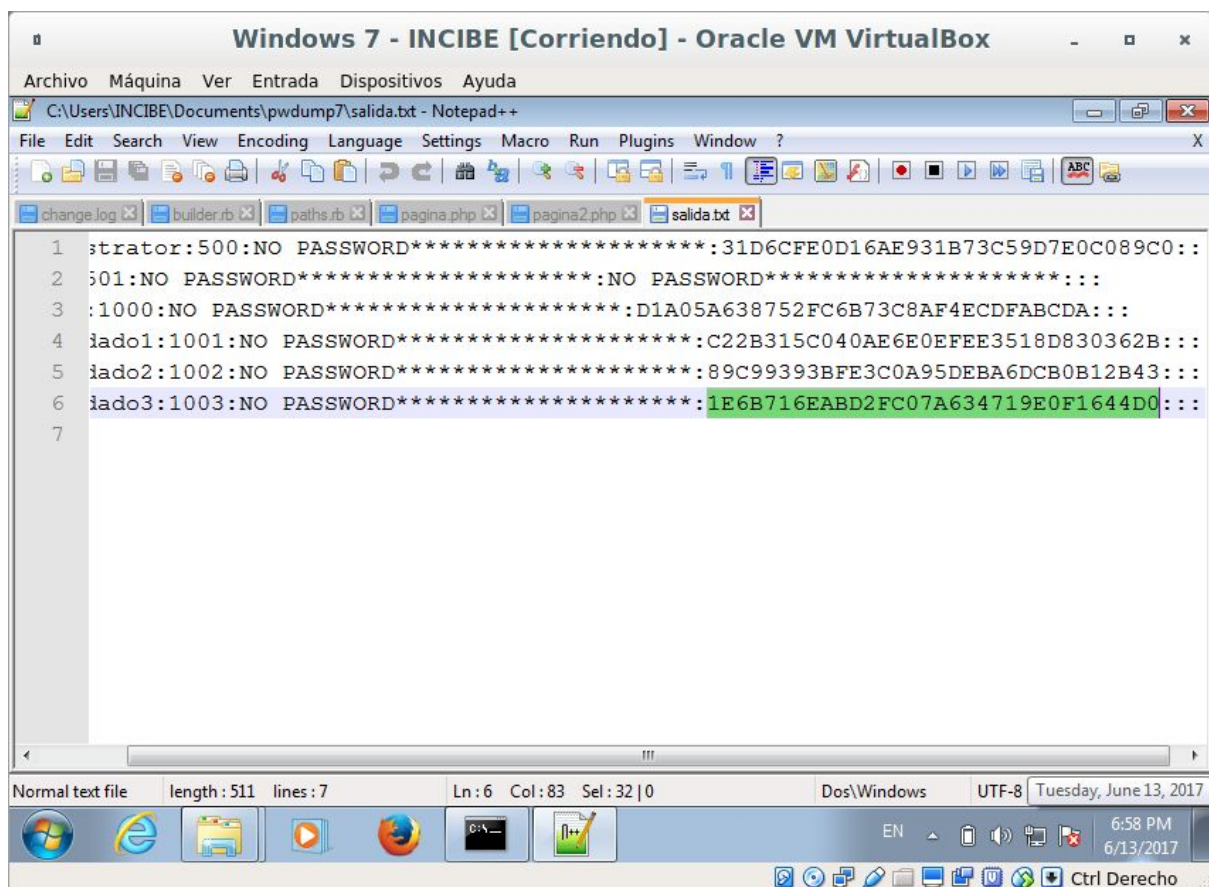
C:\Users\INCIBE\Documents\pwdump7>
```

Esto saca por pantalla los hashes de las contraseñas de los usuarios del sistema. Si lo prefieres puedes guardarlo en un fichero redirigiendo la salida del comando a un archivo para después poder copiar los hashes más fácilmente desde un fichero de texto que desde la consola de Windows. Esto se haría así: Pwdump7.exe > salida.txt, como has podido ver en la captura anterior

4. Copia el hash NTLM del usuario que quieras auditar, desde la consola o desde el bloc de notas con el fichero de salida (depende de como lo hayas hecho). Desde la consola hay que hacerlo haciendo clic en la esquina superior izquierda de la ventana de la consola -> Marcar -> Seleccionar con el ratón -> Pulsar enter:



5. El hash NTLM es el que aparece en último lugar, tal y como ves en la siguiente captura:

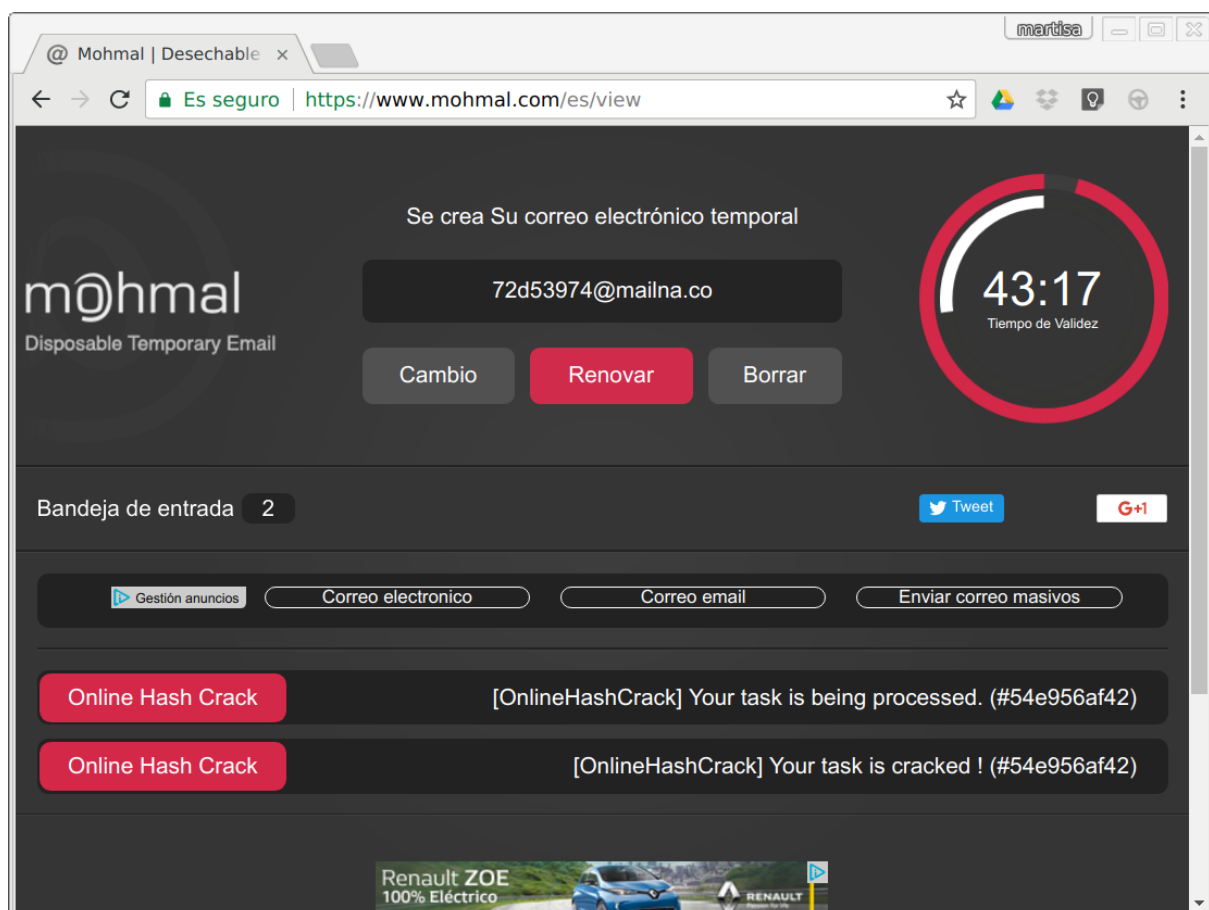


Los campos del formato de salida se separan con dos puntos (:). Como puedes ver, el primero es el usuario, después es el identificador del usuario y el tercer y cuarto parámetro son los hashes LM y NTLM respectivamente, que son los dos resúmenes criptográficos con

los que Windows guarda el resumen de la contraseña. LM es el que se usaba en las primeras versiones de Windows y es altamente inseguro. Como puedes ver, los sistemas operativos actuales a partir de Vista, ya no guardan el hash LM por su debilidad. Es por eso que aparece el texto NO PASSWORD en el campo del hash LM.

6. Cópialo en la url <http://www.onlinehashcrack.com/> indicando un email donde se te enviará el resultado. Esta página intenta descubrir las contraseñas asociadas a los hashes mediante técnicas como diccionarios de palabras o fuerza bruta (probar todas las combinaciones posibles). Si la contraseña elegida es fuerte, tardará muchísimo en romperla (pueden ser años). Además, si tiene más de 8 caracteres o más, hay que pagar para que la descifren. Si es débil, como la de los usuario de prueba que has creado, verás que en pocos minutos obtiene la contraseña.

Si te da miedo ir poniendo por ahí tu correo electrónico personal (deberías tenerlo, aunque sólo sea por no fomentar tu spam), puedes usar un correo temporal como éste:



Donde como ves, puedes leer los correos que te envíen durante un tiempo. Debes tener éxito sin problemas:

My Dashboard : Hashes / WPA / Office | Online Hash Crack - Mozilla Firefox

Archivo Editar Ver Historial Marcadores Herramientas Ayuda

My Dashboard : Ha x +

https://www.onlinehashcrack.com/433d6dbf7b

OnlineHashCrack Professional Password Recovery

HOME HASHES WIFI OFFICE HOW TO? ABOUT CONTACT

Your Hashes (2)

#	Date	Hash	Algorithm	Status	Length	Password	Actions
1	2017-06-17	89C993938FE3C0A95DEBA6DCB0B12B43	NTLM	Found !	6	123abc	✕ ✎ ⬇
2	2017-06-17	1E6B716EABD2FC07A634719E0F1644D0	NTLM	Found !	4	easy	✕ ✎ ⬇
3	2017-06-17	QUICK ADD / NEW HASH HERE ..					ADD !

Your WPA dumps (0)

#	Date	ESSID	BSSID	Station	Status	Password	Actions
1	2017-06-17	Add a new WPA dump file :					ADD !

Examinar... No se ha seleccionado ningún archivo.

Proactive cyber security mgmt - securiCAD

Take control over risks, make better investments, and become more effective

foreseet.com

>

7. Sube a la plataforma en la actividad correspondiente una memoria con capturas describiendo el proceso realizado.

También es posible romper los hashes mediante herramientas locales instaladas en el sistema, en vez de páginas web como la citada en la práctica. De esta forma preservamos la privacidad de las contraseñas. Algunas de estas herramientas son L0phtCrack, Cain & Abel, John The Ripper y menciono especial tiene personalmente, la herramienta [Ophcrack](#). Esta herramienta, disponible para Windows, Mac y GNU/Linux, permite usar tablas rainbow, que son ficheros enormes con millones de combinaciones de hashes de contraseñas ya calculados, de forma que el proceso se acelera enormemente produciendo resultados espectaculares. Desde la página web de Ophcrack se pueden descargar también las tablas, algunas de ellas de varios gigas de tamaño.

Puedes investigar estas herramientas y hacer uso de ellas para intentar romper o averiguar otras contraseñas. Si lo haces, **puedes ampliar la memoria documentando el proceso de uso de estas herramientas, lo que supondría una parte voluntaria de la práctica que serviría para subir nota.**