



Volcando y rompiendo hash SAM para extraer la contraseña de texto simple

Pwdump7 se puede utilizar para volcar archivos protegidos. Ophcrack es un programa gratuito de código abierto (licencia GPL) que se agrieta. Contraseñas de Windows utilizando hashes LM a través de rainbow tables.

Objetivos del laboratorio

El objetivo de este laboratorio es ayudar a los estudiantes a aprender cómo:

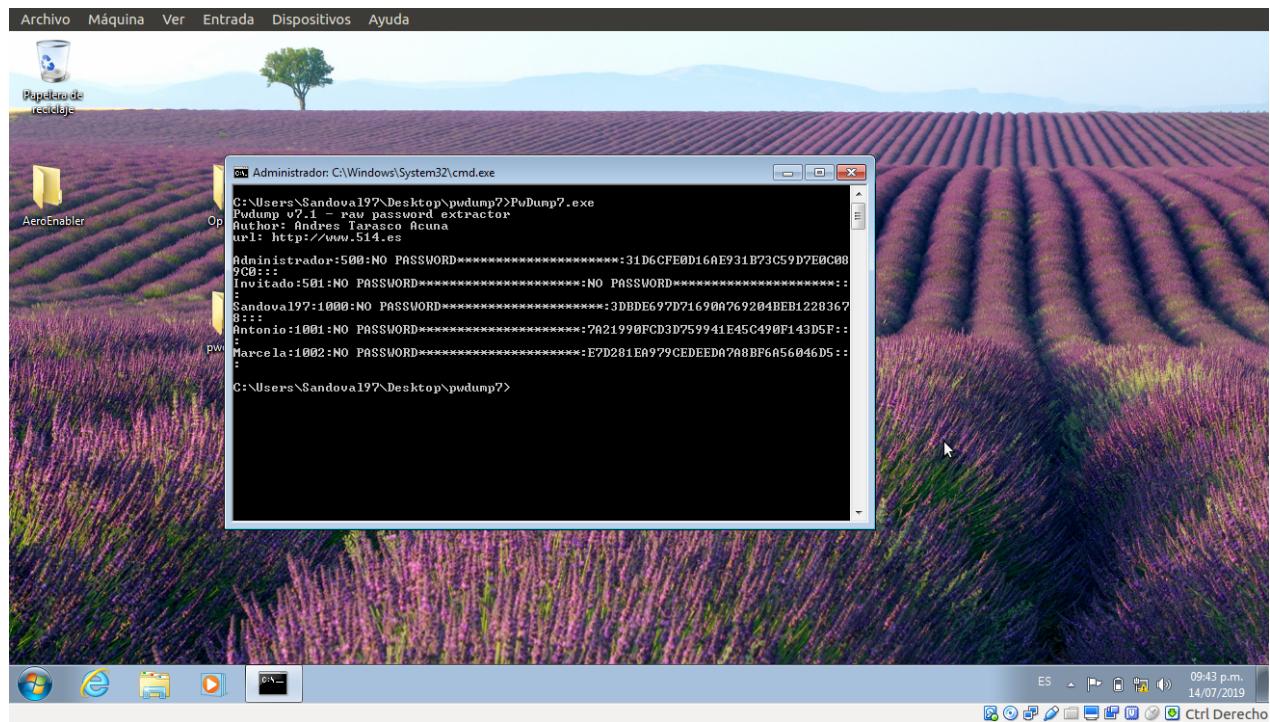
- Utilice la herramienta pwdump7 para extraer hashes de contraseña
- Utilice la herramienta Ophcrack para descifrar las contraseñas y obtener una contraseña de texto plano.

Visión general del laboratorio

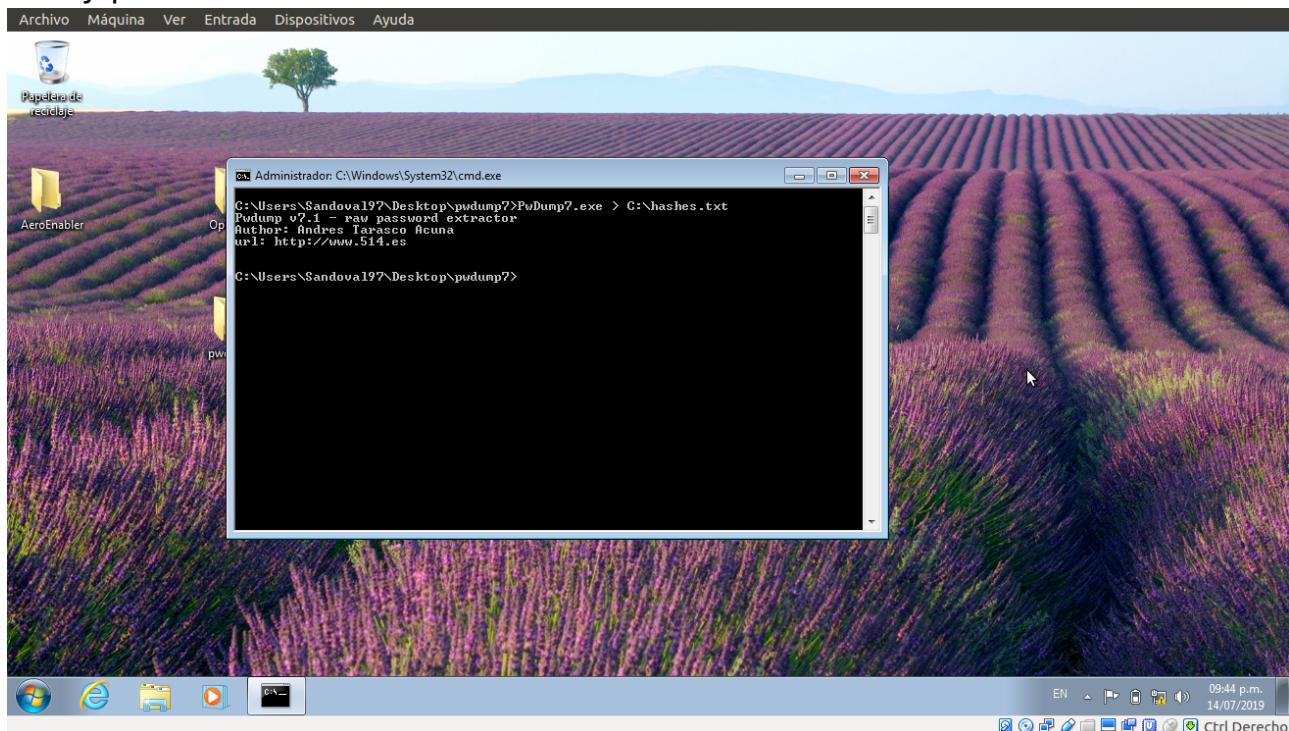
Pwdump7 también se puede utilizar para volcar archivos protegidos. Siempre puede copiar un archivo usado ejecutando `pwdump7.exe -d C:\lockedfile.dat backup-lockedfile.dat`. Las Rainbow tables para hash LM de contraseñas alfanuméricas se proporcionan de forma gratuita por los desarrolladores. De forma predeterminada, Ophcrack está empaquetado con tablas que le permiten descifrar contraseñas de no más de 14 caracteres utilizando solo caracteres alfanuméricos.

Tareas del laboratorio

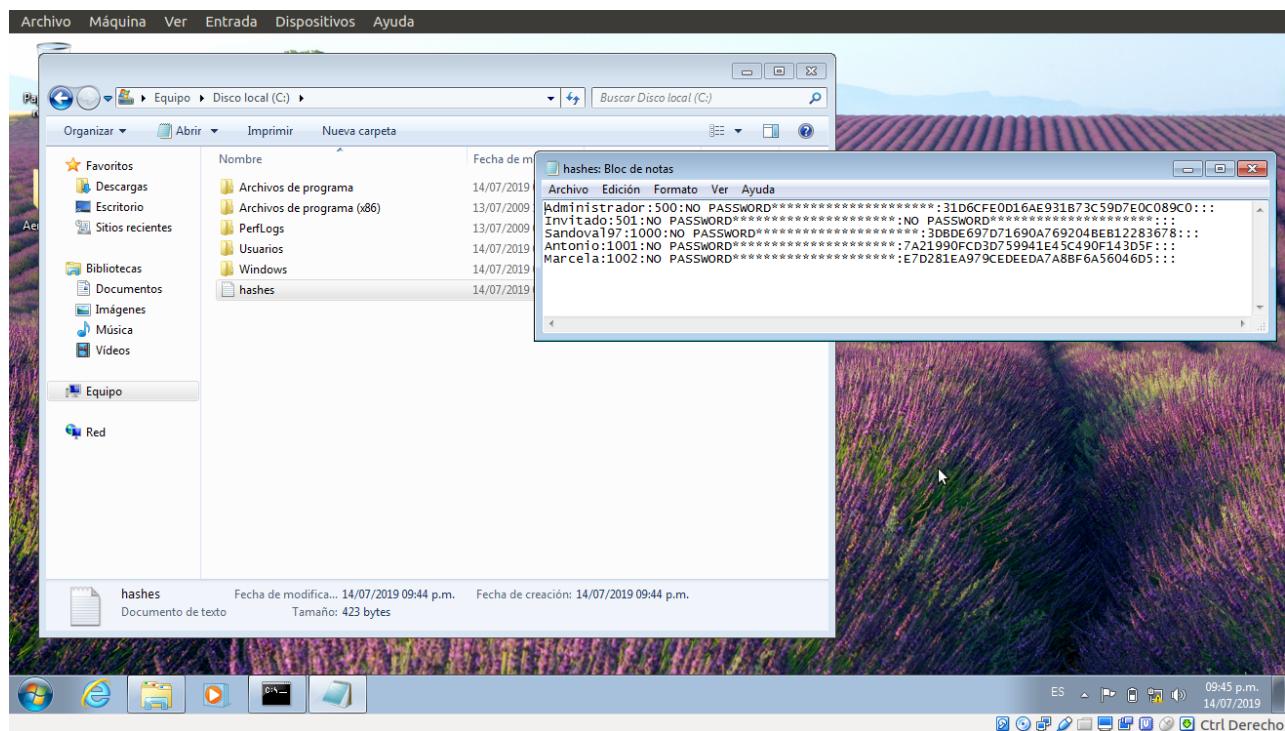
1. Abra el símbolo del sistema y navegue donde tengas almacenado el ejecutable de pwdump7.
2. Escriba **pwdump7.exe** y presione **Enter**. Esto muestra todos los hashes de contraseña, como se muestra en la siguiente captura de pantalla.



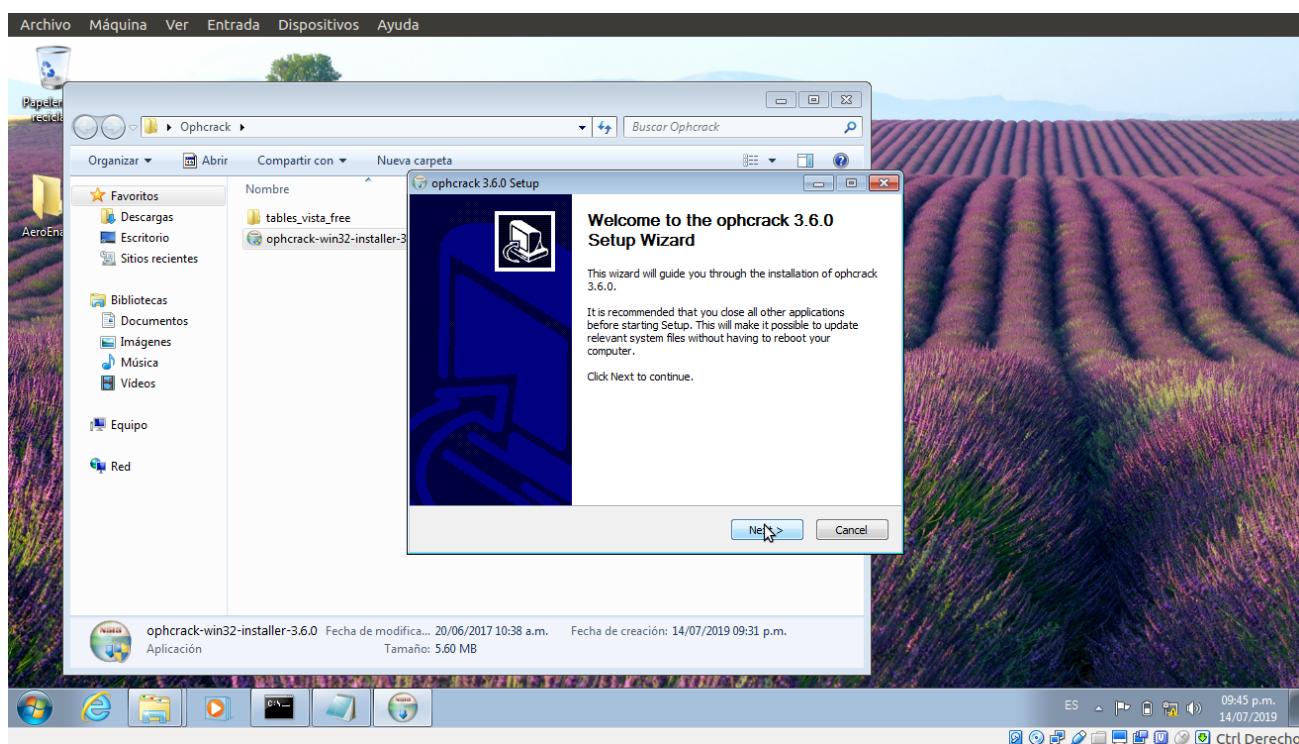
3. Ahora, en el símbolo del sistema, escriba **pwdump7.exe > C:\hashes.txt** y presione **Enter**.



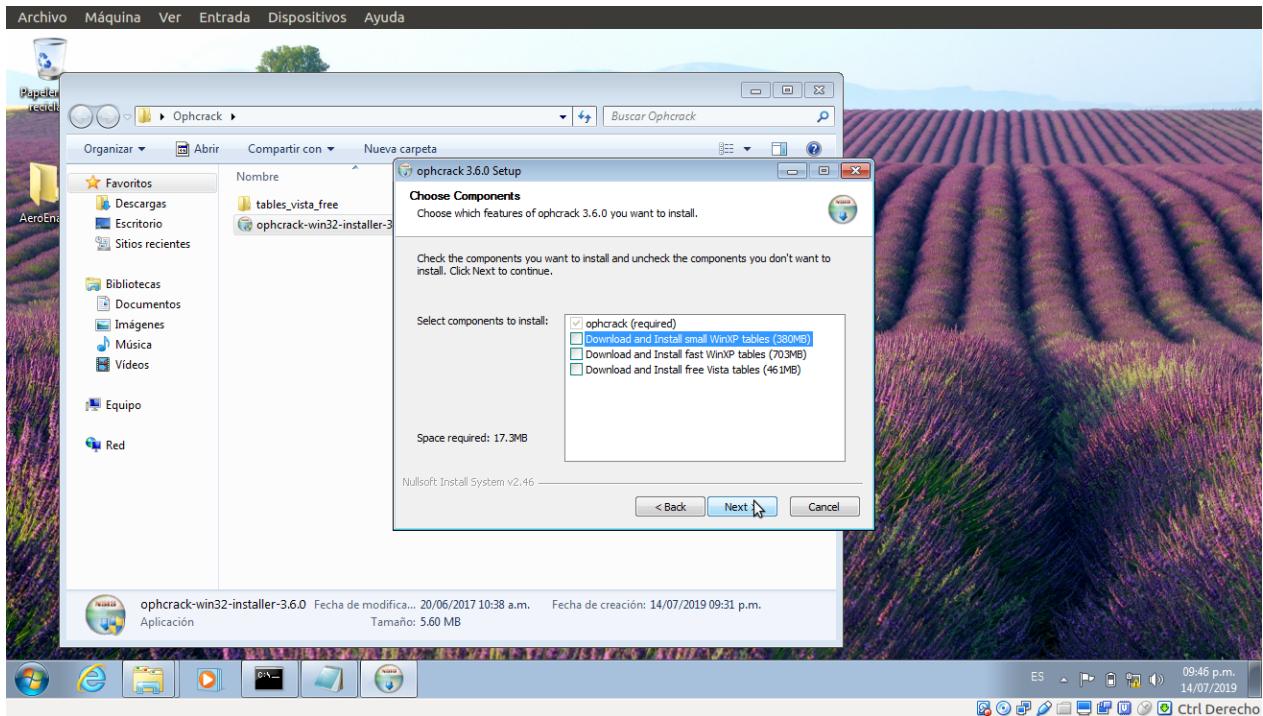
4. El comando anterior copiará todos los datos de **pwdump7.exe** en el archivo **C:\hashes.txt**.
5. Para verificar los hashes generados, navegue a **C:** y abra el archivo **hashes.txt** con el Bloc de notas.



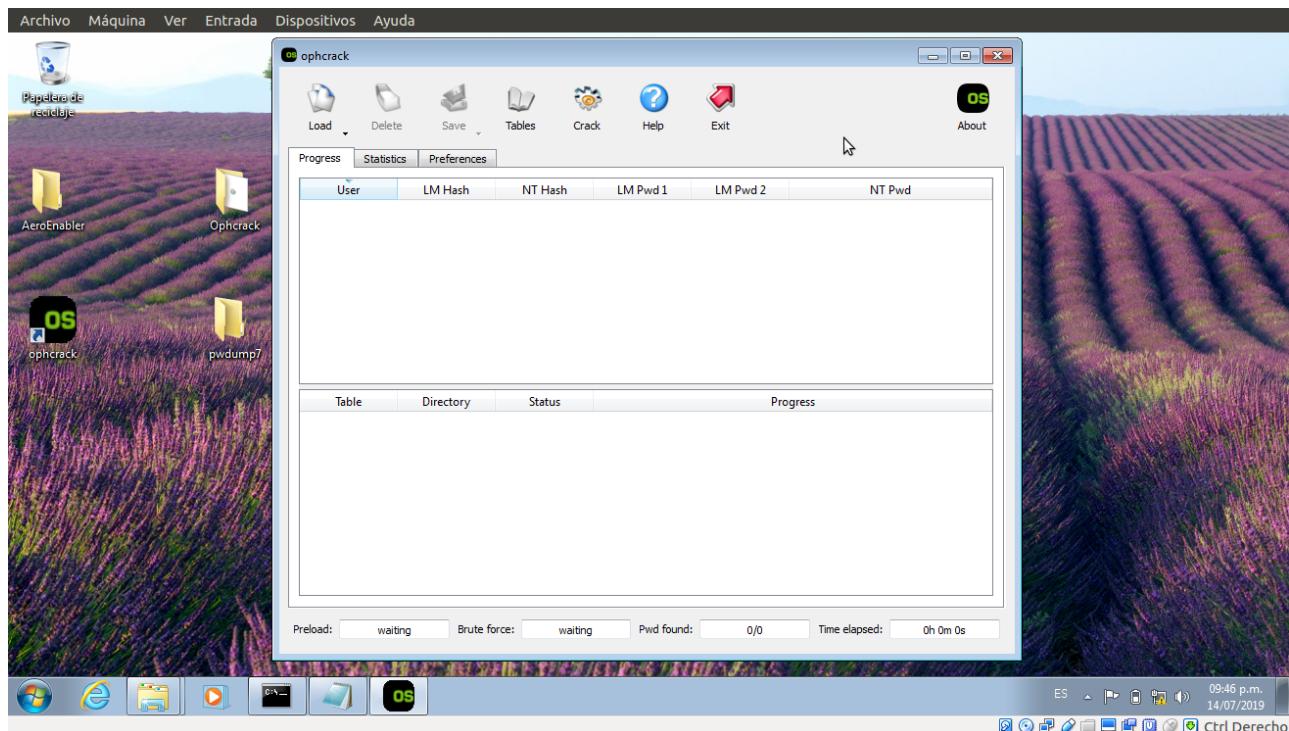
6. Ahora, intentaremos verificar estos hashes de contraseña con la herramienta **Ophcrack**.
7. Desplázate donde tengas el ejecutable de Ophcrack y haz doble clic en el.
8. Si aparece una ventana emergente de advertencia de seguridad en **Abrir archivo**, haga clic en **Siguiente**.
9. Aparece el asistente de instalación de **ophcrack**, haga clic en **Siguiente**.



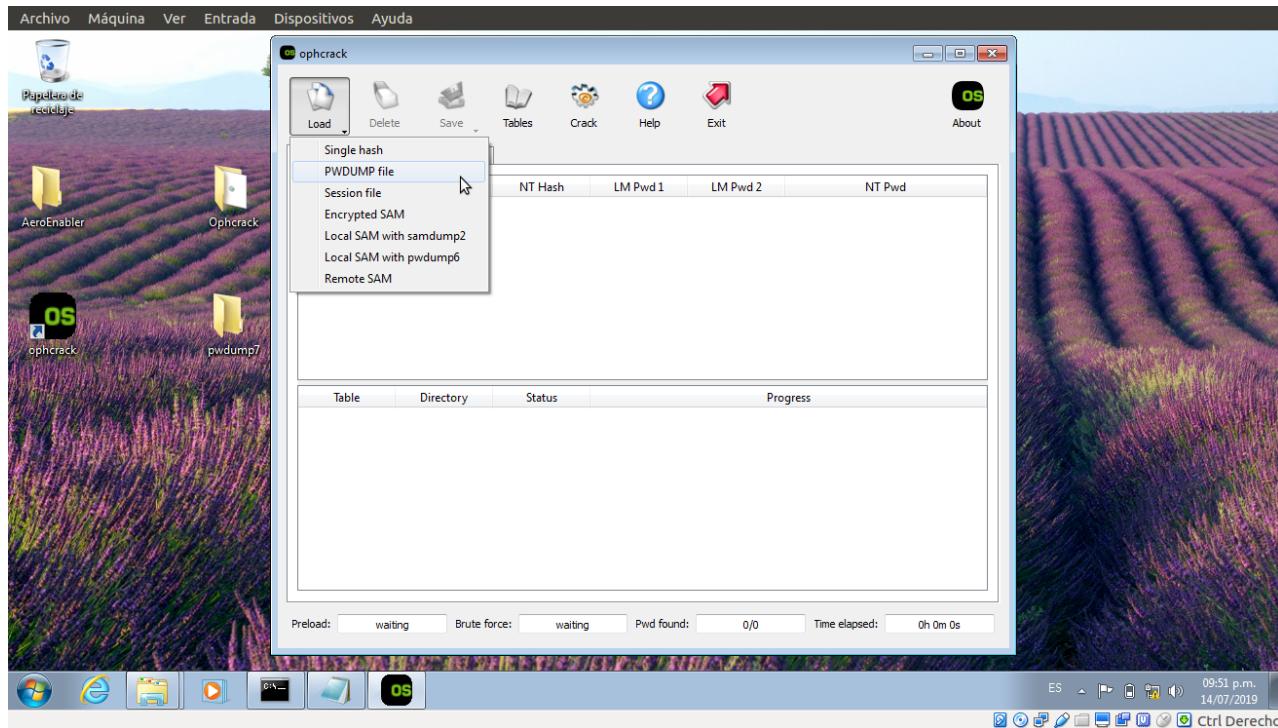
10. En la sección Elegir componentes, desmarque todas las opciones y haga clic en Siguiente.



11. Una vez hecho esto con la instalación, inicie OpenStego desde la pantalla de aplicaciones.
12. La ventana principal de **Ophcrack** aparece, como se muestra, como se muestra en la siguiente captura de pantalla.

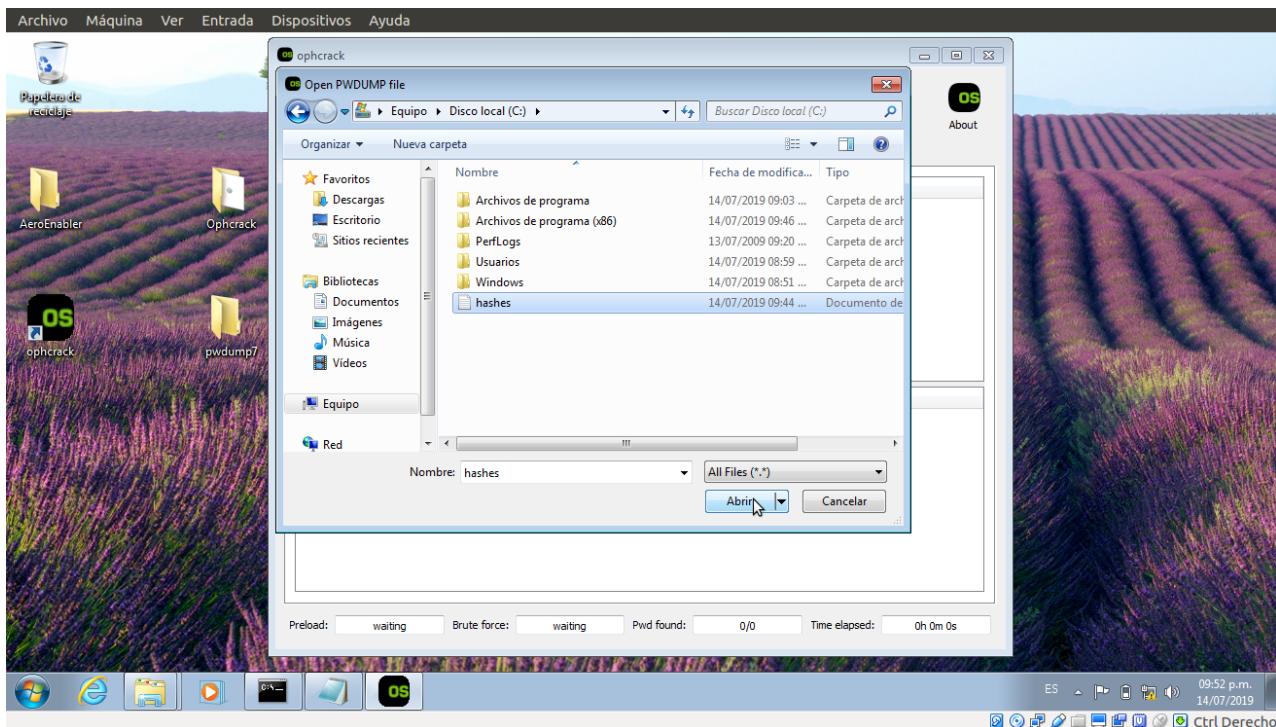


13. Haga clic en el menú de **load**, y seleccione el archivo **PWDUMP**.

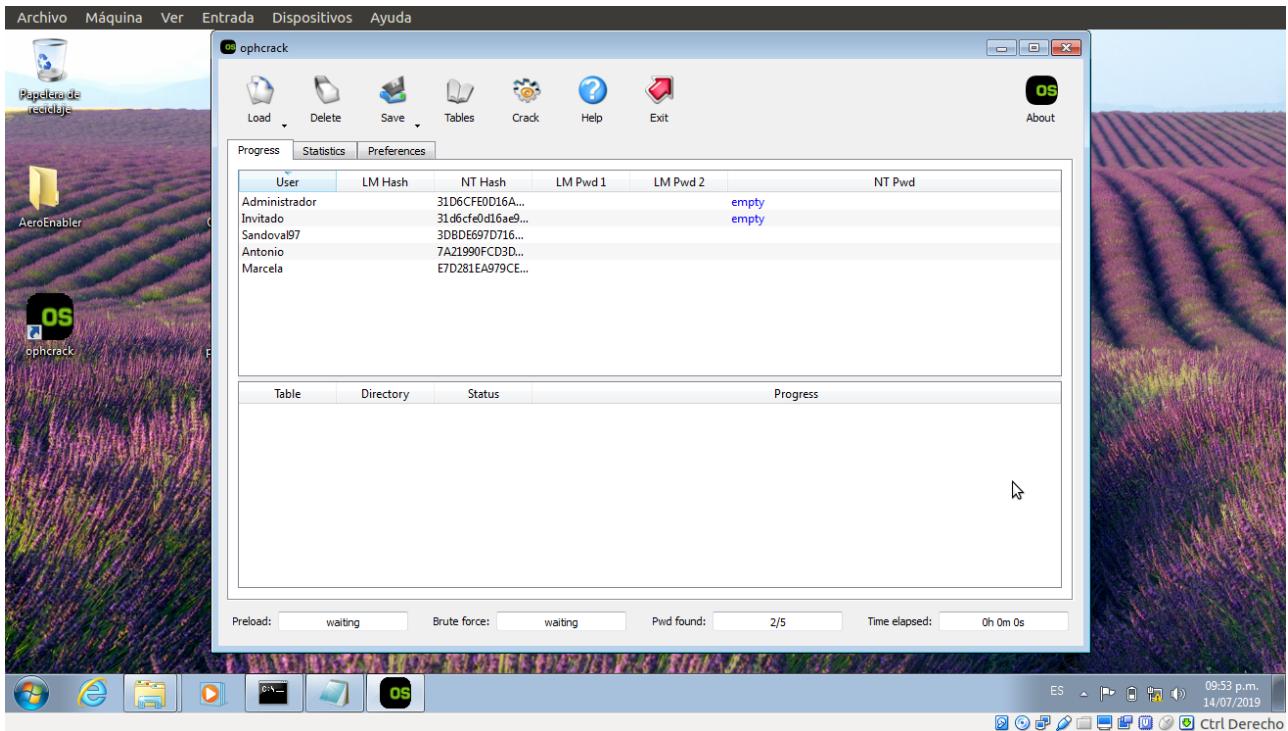


14. Aparece la ventana **Open PWDUMP file**. Examine el archivo PWDUMP (**hashes.txt** ubicado en **C:**), que ya se generó utilizando PWDUMP7 en los pasos anteriores.

15. Seleccione el archivo **hashes.txt**, ubicado en **C:**, y haga clic en **Open**.



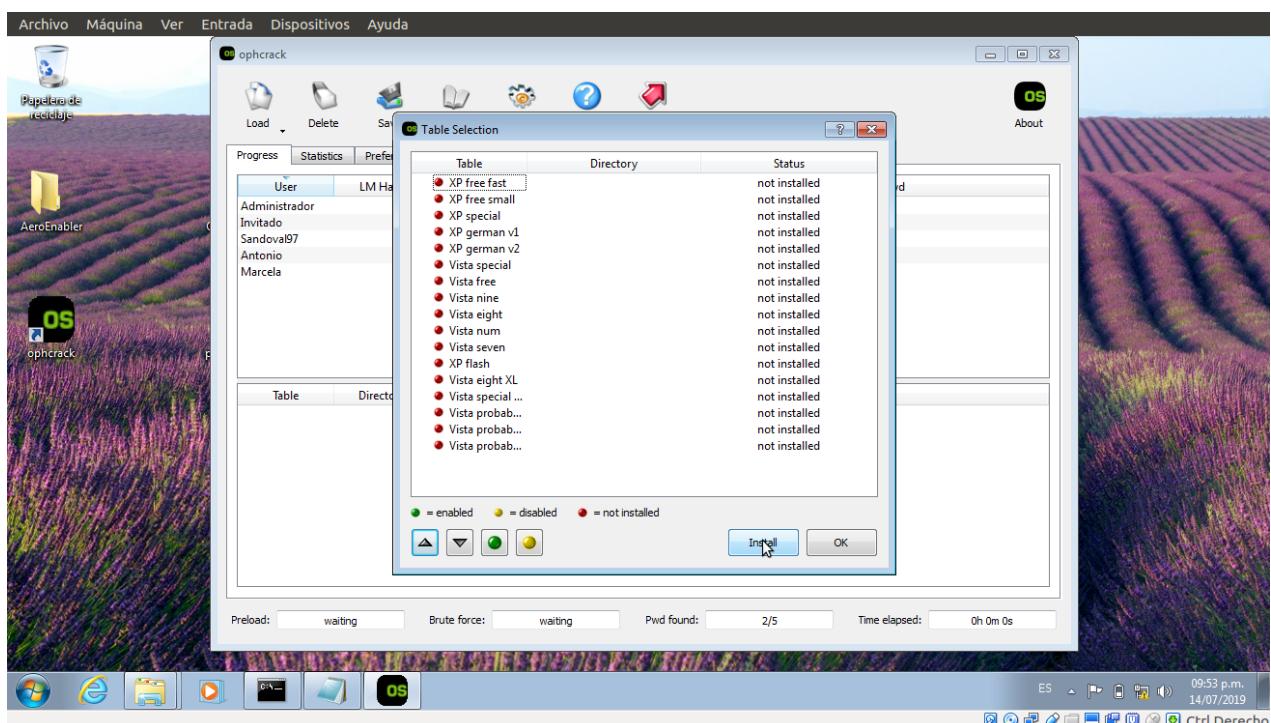
16. Los hash se cargan en Ophcrack, como se muestra en la siguiente captura de pantalla.



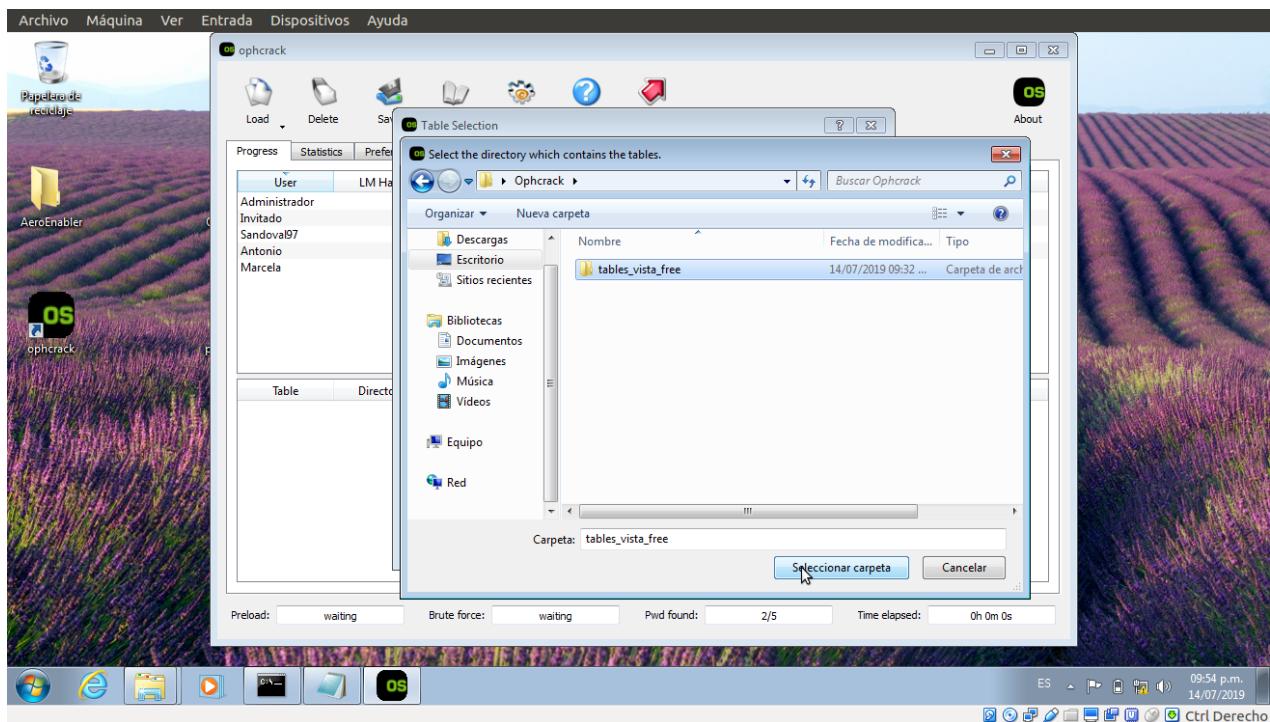
17. Haga clic en el menú **Tables**

Nota: puede descargar las tablas gratuitas de XP y Vista desde <http://Ophcrack.sourceforge.net/tables.php>

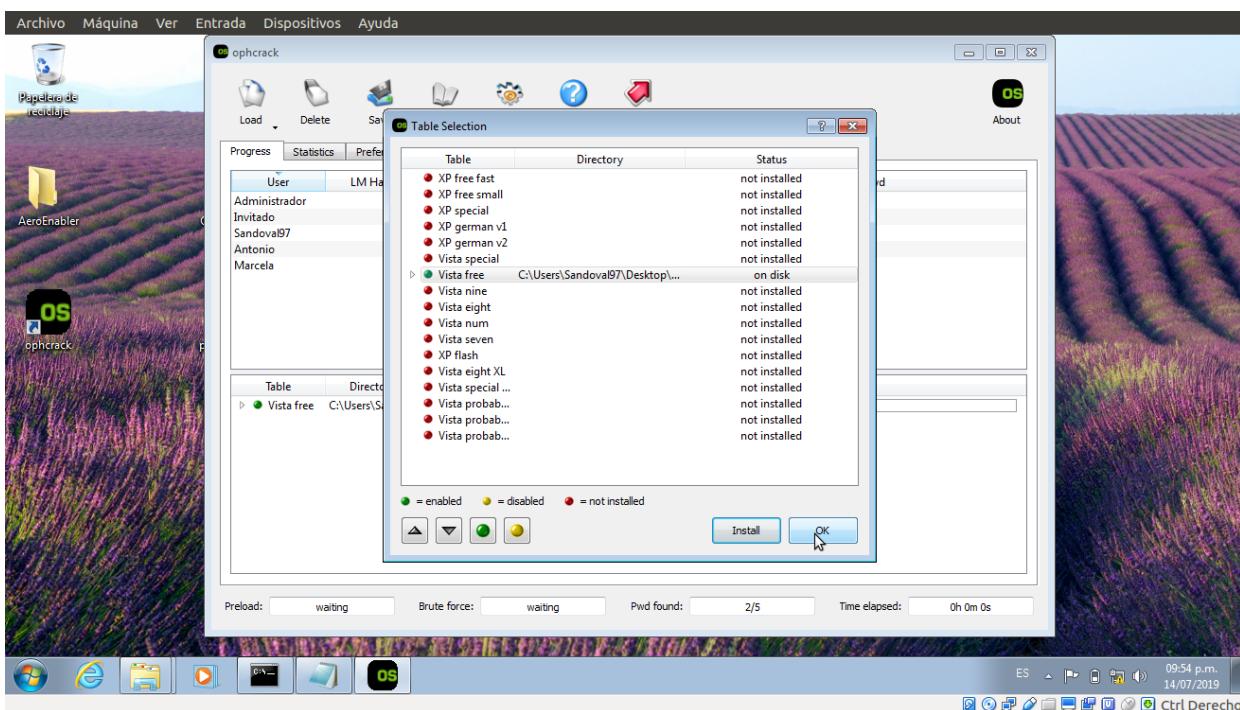
18. Aparece la ventana de selección de tabla; Seleccione **Vista free** y haga clic en install.



19. Aparece la ventana **Seleccionar el directorio que contiene las tablas**. Seleccione la carpeta **table_vista_free**, que ya está descargada y guardada, y haga clic en **Seleccionar carpeta**.

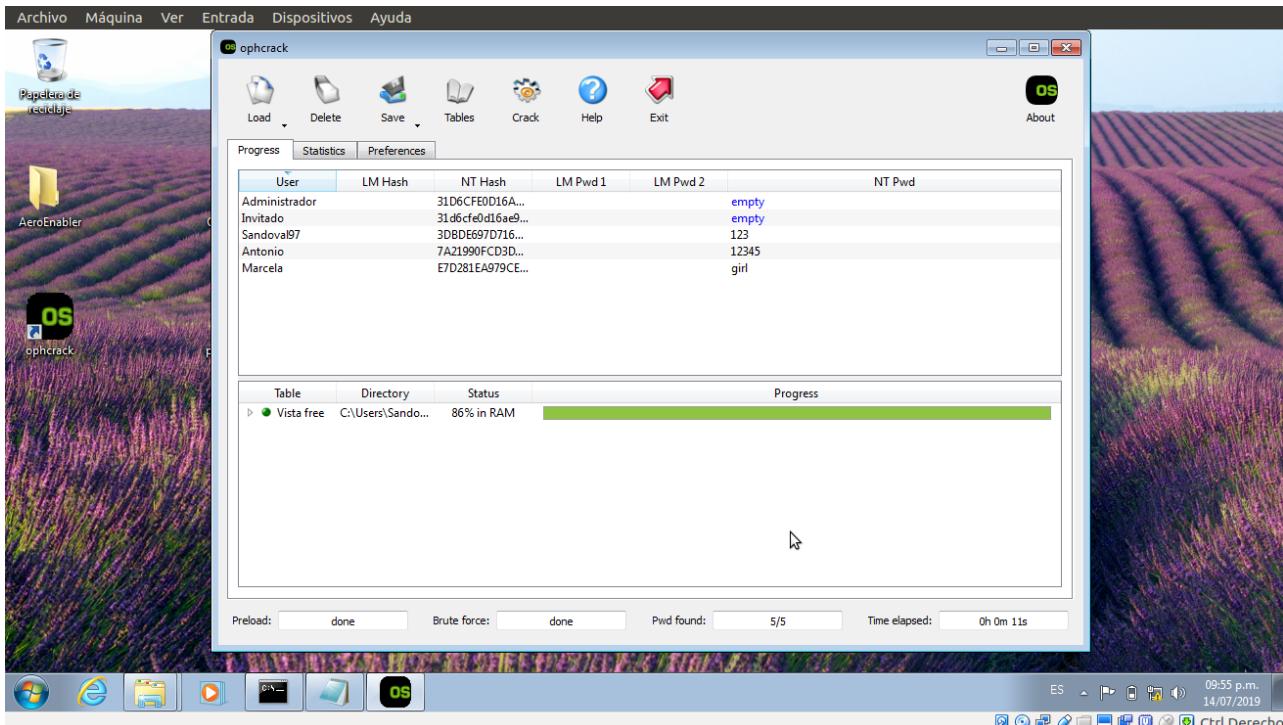


20. Esta **tables_vista_free** es una tabla precalculada para revertir las funciones criptográficas de hash y recuperar contraseñas de texto simple hasta cierta longitud.
21. El **table_vista_free** seleccionado se instala con el nombre **Vista free**, que se representa con una viñeta de color verde. Seleccione la tabla, y haga clic en **Ok**.



22. Haga clic en **Crack** en la barra de menú. Ophcrack comienza a descifrar contraseñas.

23. Se muestran las contraseñas agrietadas, como se muestra en la siguiente captura de pantalla.



En tiempo real, si un atacante intenta explotar una máquina y escalar los privilegios, puede obtener hashes de contraseña usando herramientas como Pwdump7. Al hacerlo, pueden usar herramientas de decodificación como Ophcrack para adquirir contraseñas de texto plano.