



Creación y uso de Rainbow Tables

Winrtgen es un generador gráfico de tablas arcoiris que admite LM, FastLM, NTLM, LMCHALL, HalfLMCHALL, NTLMCHALL, MSCACHE, MD2, MD4, MD5, SHA1, RIPEMD160, MySQL32, MySQLSHA1, CiscoPIX, ORACLE, SHA-2 2 (384) y SHA-2 (512) hashes.

RainbowCrack es un programa de computadora que genera tablas de arco iris para usar en el descifrado de contraseñas.

Objetivos del laboratorio

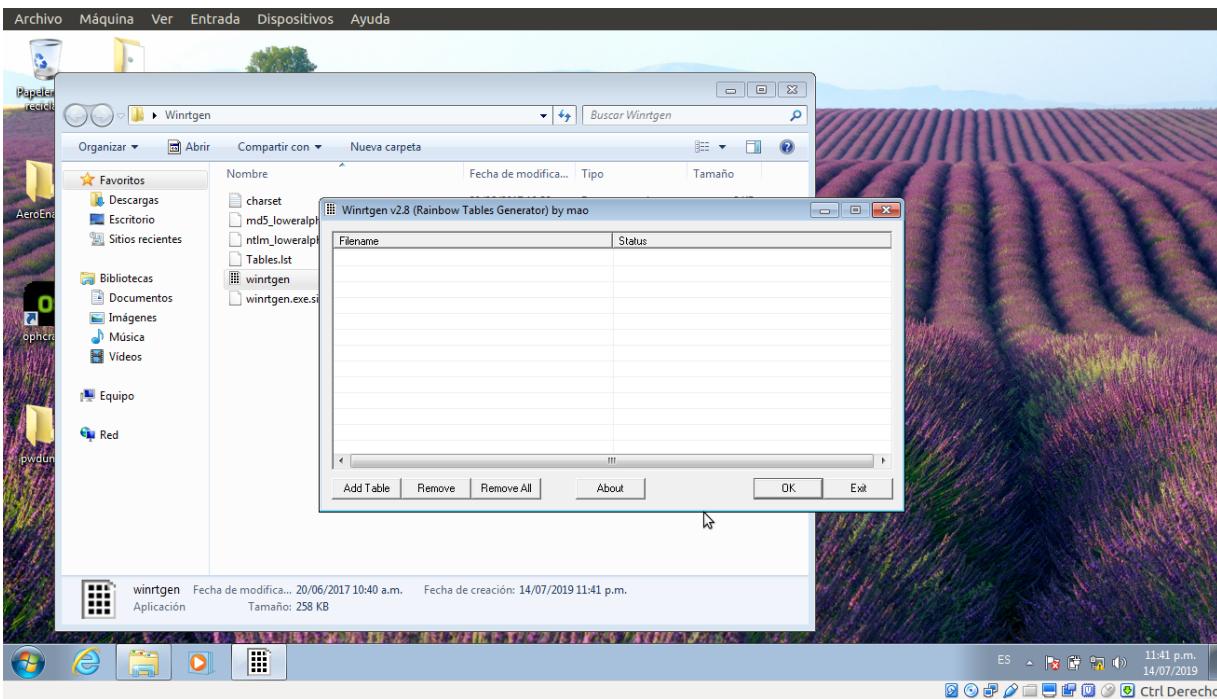
El objetivo de este laboratorio es mostrar a los estudiantes cómo crear tablas de arco iris y usarlas para descifrar los hashes y obtener contraseñas en texto plano.

Visión general del laboratorio

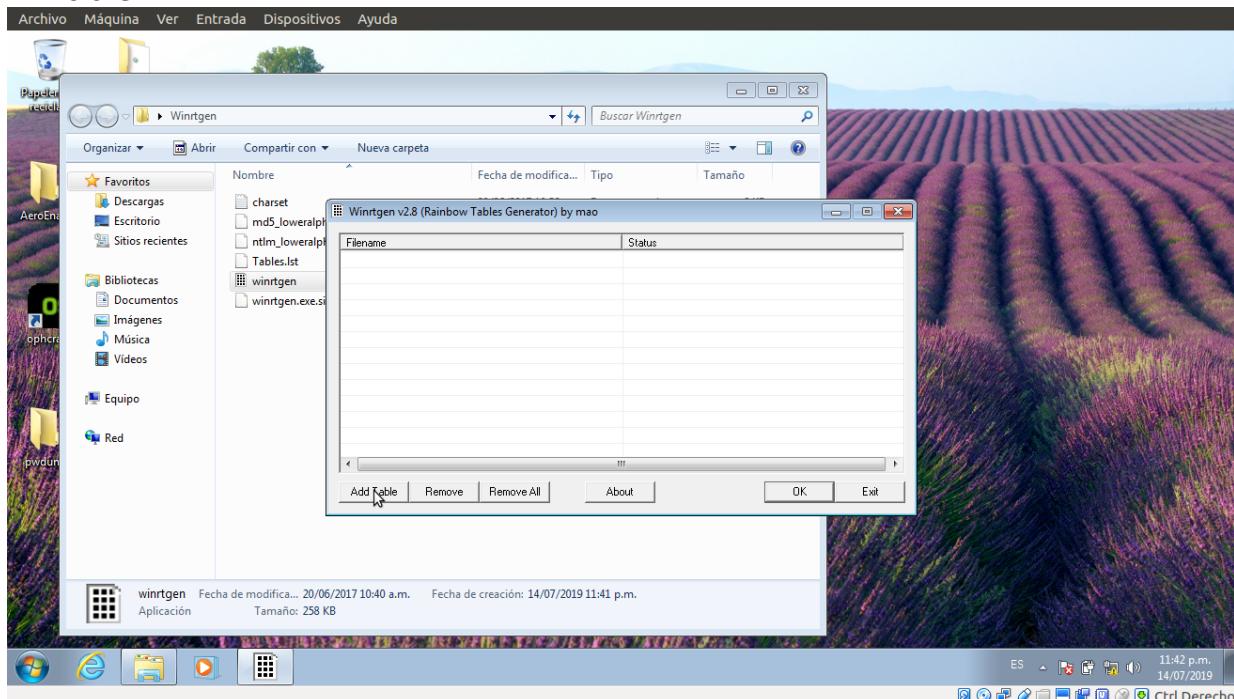
Una tabla de arco iris es una tabla precomputada para revertir las funciones criptográficas de hash, que generalmente se usa para descifrar hashes de contraseña. Las tablas se usan generalmente para recuperar la contraseña de texto simple que consiste en un conjunto limitado de caracteres, hasta una cierta longitud.

Tareas del laboratorio

1. Navega hasta el directorio donde tengas almacenado el ejecutable para **winrtgen.exe**.
2. Si aparece una ventana emergente **Abrir archivo - Advertencia de seguridad**, haga clic en **Ejecutar**.
3. Se abrirá la ventana principal de **Winrtgen**, como se muestra en la siguiente captura de pantalla.

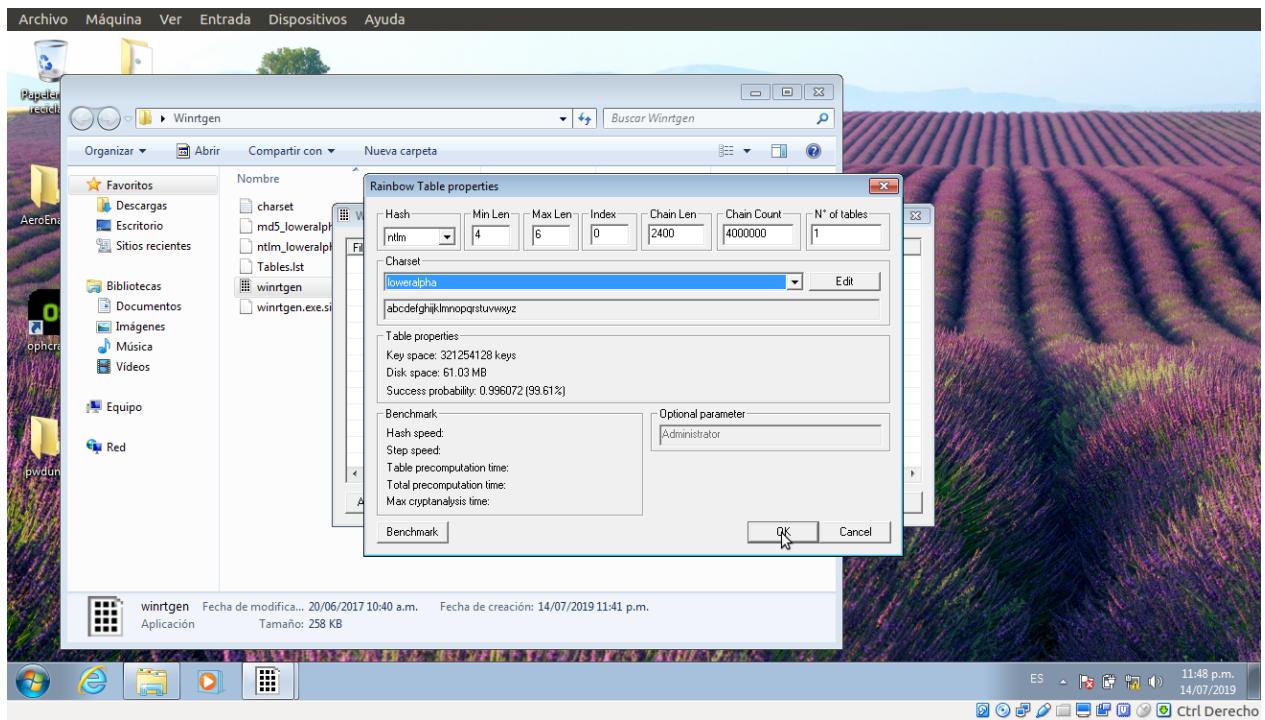


4. Haga clic en el botón **Agregar tabla** para agregar una nueva rainbow table.



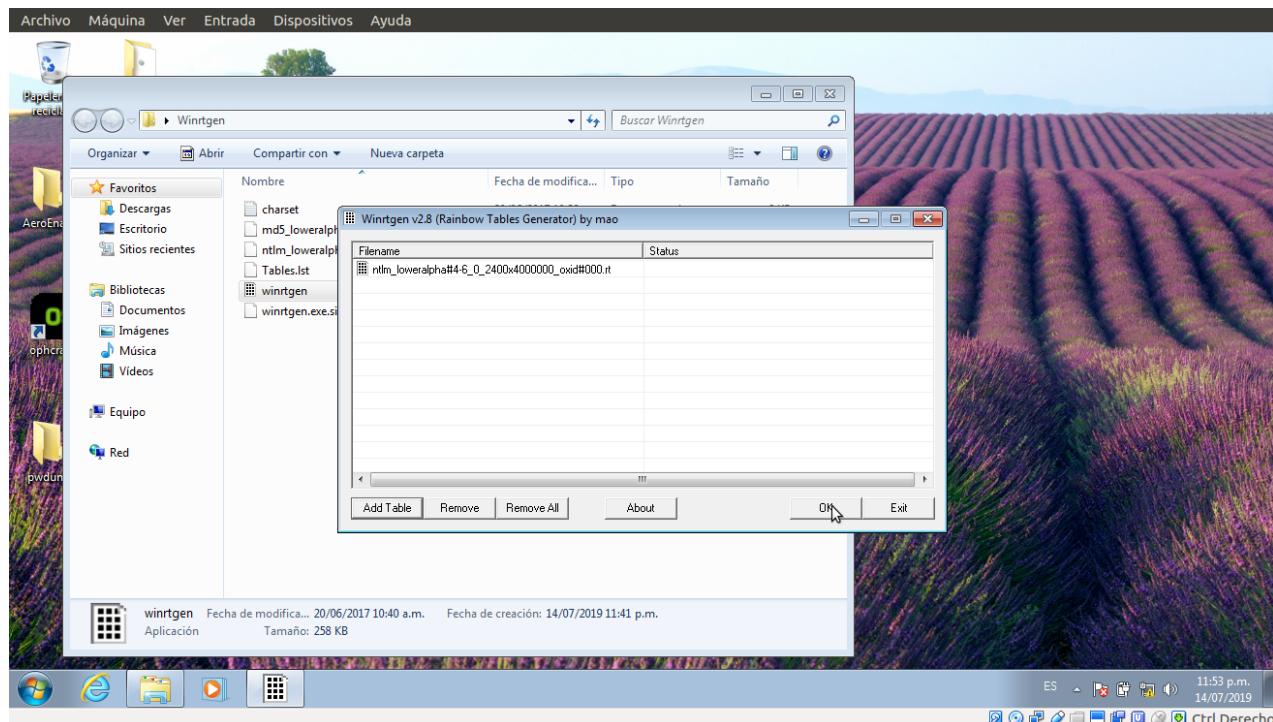
5. Aparece la ventana de propiedades de Rainbow Tables.

- Seleccione ntlm de la lista desplegable Hash.
- Establezca Min Len como 4, Max Len como 6 y Chain Count 4000000
- Seleccione loweralpha de la lista desplegable Charset (depende de la contraseña)



6. Clic en **OK**

7. Con estos ajustes, está creando una rainbow table que se puede usar para descifrar solo hashes NTLM que contienen contraseñas alfabéticas en minúsculas que varían entre 4 y 6 caracteres de longitud.
8. Se creará un archivo y se mostrará en la ventana de Winrtgen. Haga clic en Aceptar.



9. Winrtgen comienza a crear la tabla hash.

Nota: Winrtgen toma mucho tiempo para generar hashes. Por lo tanto, para ahorrar tiempo para la demostración de laboratorio, una tabla hash generada previamente se mantiene en la ubicación de los archivos descargados.

10. La tabla hash creada se guarda automáticamente en la ruta actual.

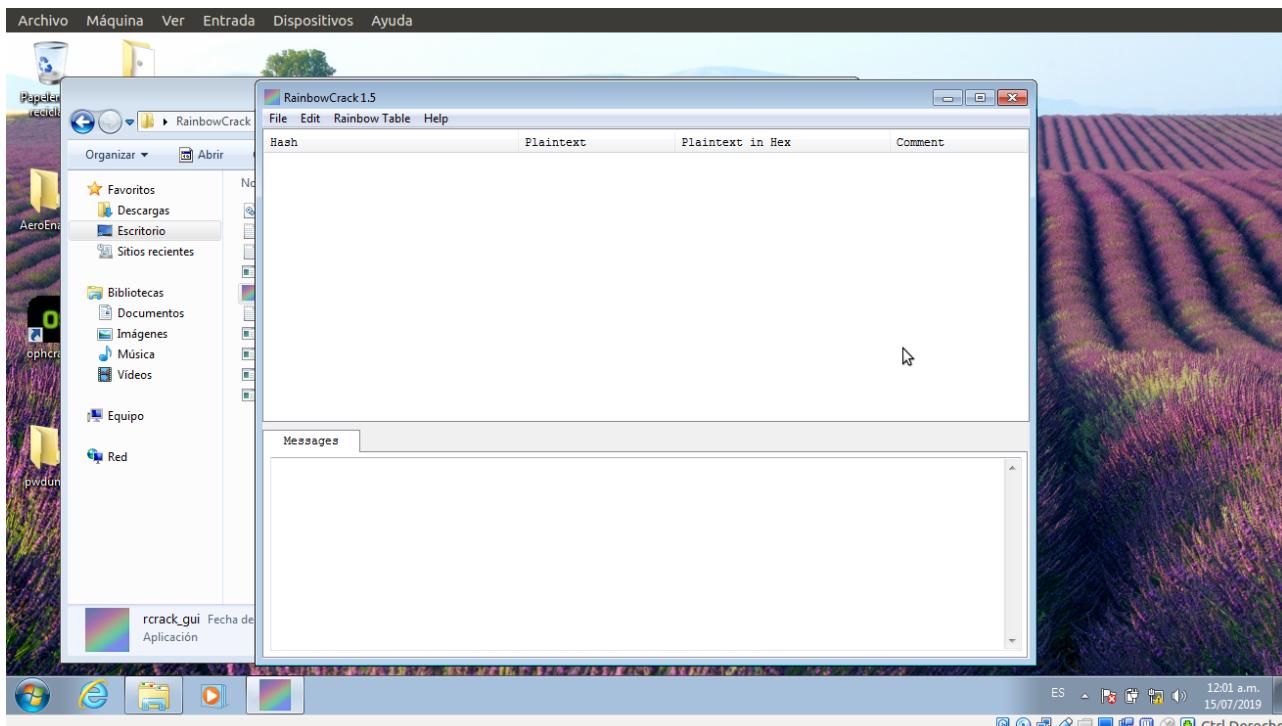
11. Esta tabla generada se usa en herramientas como RainbowCrack para descifrar contraseñas de varias longitudes, dependiendo de los hashes que genere usando Winrtgen.

12. Ahora, trataremos de usar estas tablas y descifrar los hashes de contraseña usando la herramienta RainbowCrack.

13. Navega hasta el directorio donde tengas almacenado el ejecutable para **rcrack_gui.exe**

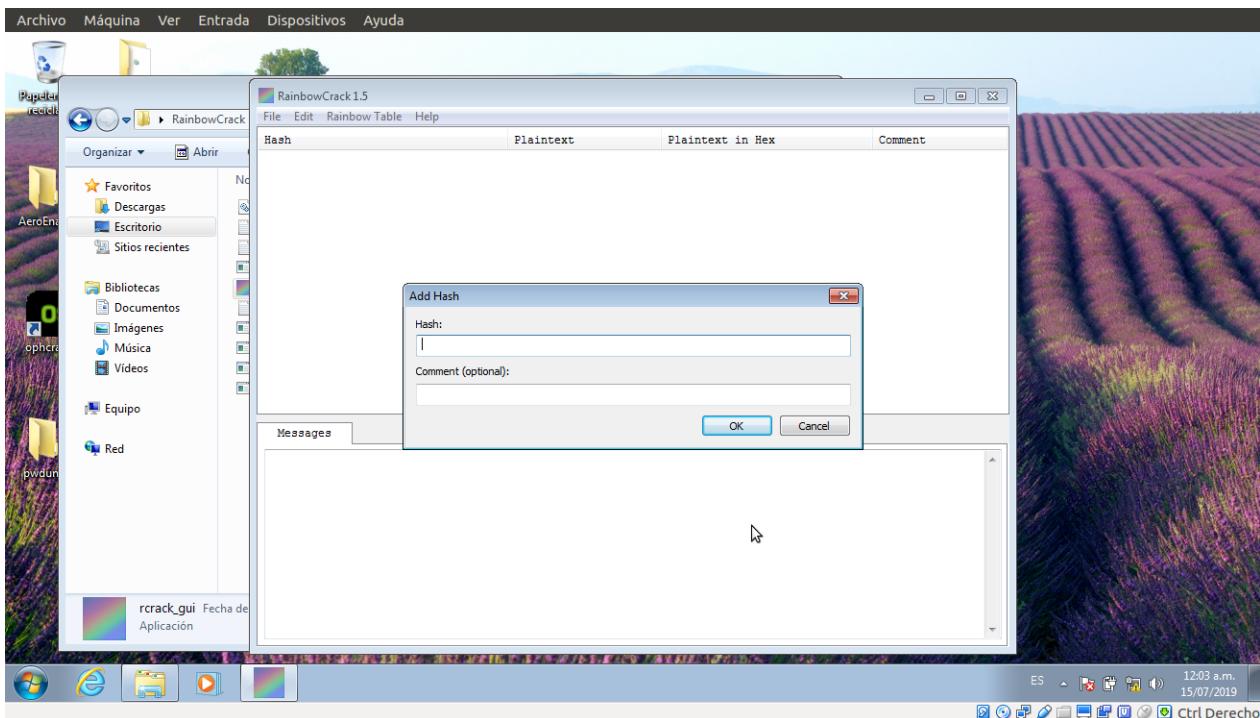
14. Si aparece una ventana emergente Abrir archivo - Advertencia de seguridad, haga clic en Ejecutar

15. Se abrirá la ventana principal de RainbowCrack, como se muestra en la siguiente captura de pantalla.



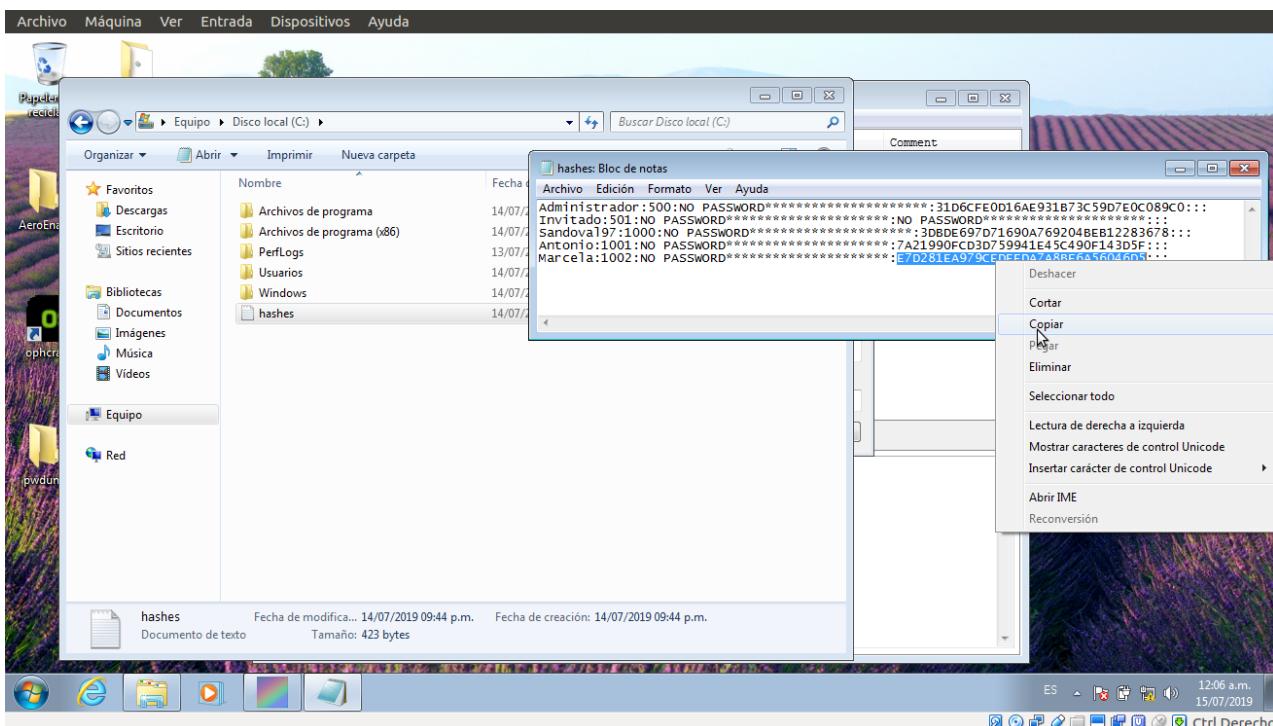
16. Para agregar un hash de contraseña en RainbowCrack, haga clic en el menú Archivo y haga clic en Agregar hash.

17. Aparece el cuadro de diálogo Agregar hash, como se muestra en la siguiente captura de pantalla.

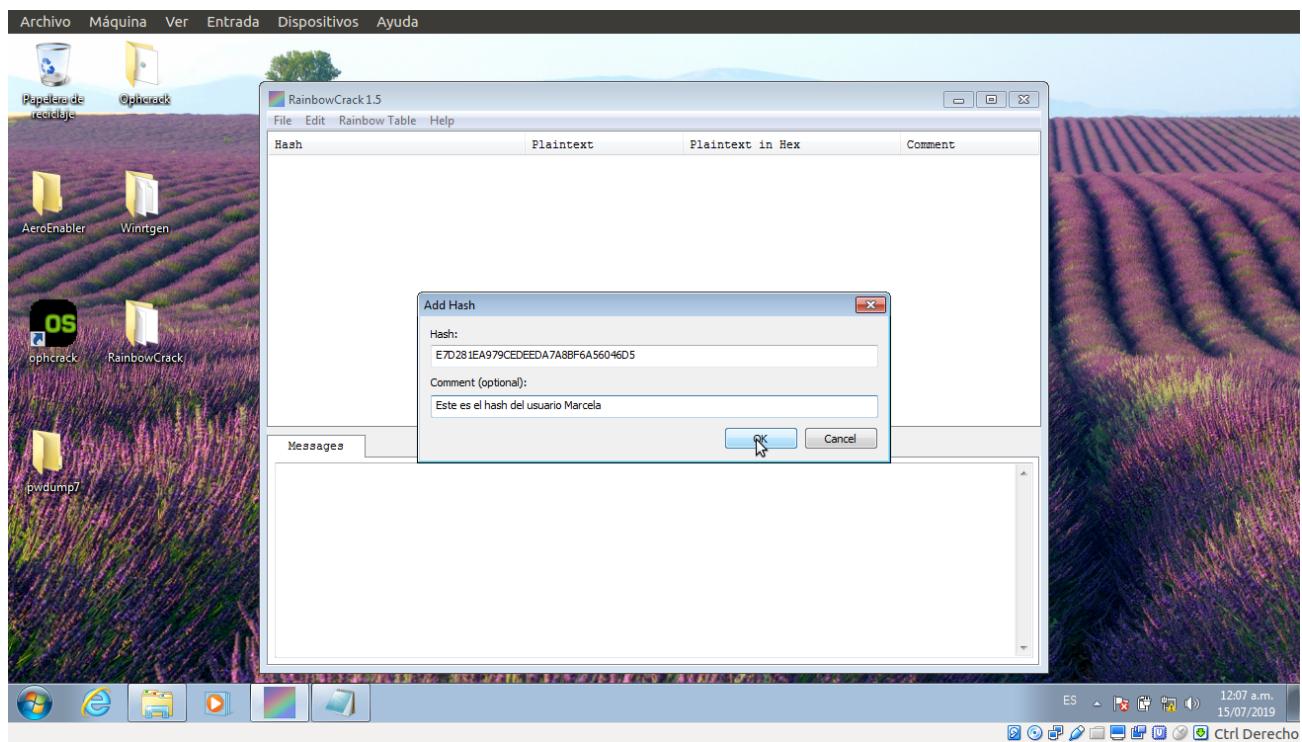


18. Navegue a C:\ y abra el archivo hashes.txt (que ya se generó usando Pwdump7 en un laboratorio anterior).

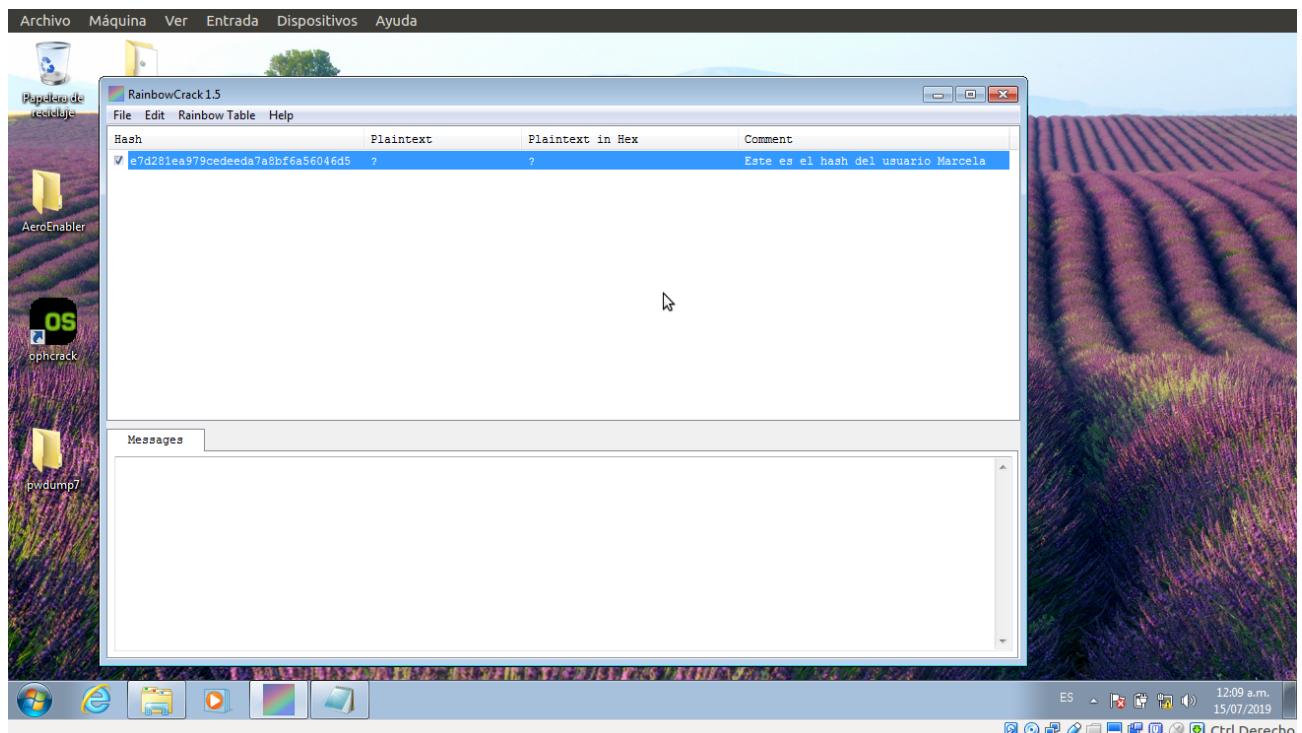
19. Copia un hash de contraseña del archivo hashes.txt



20. Péguelo en el campo Hash en RainbowCrack, proporcione un comentario (opcional) y haga clic en Aceptar.

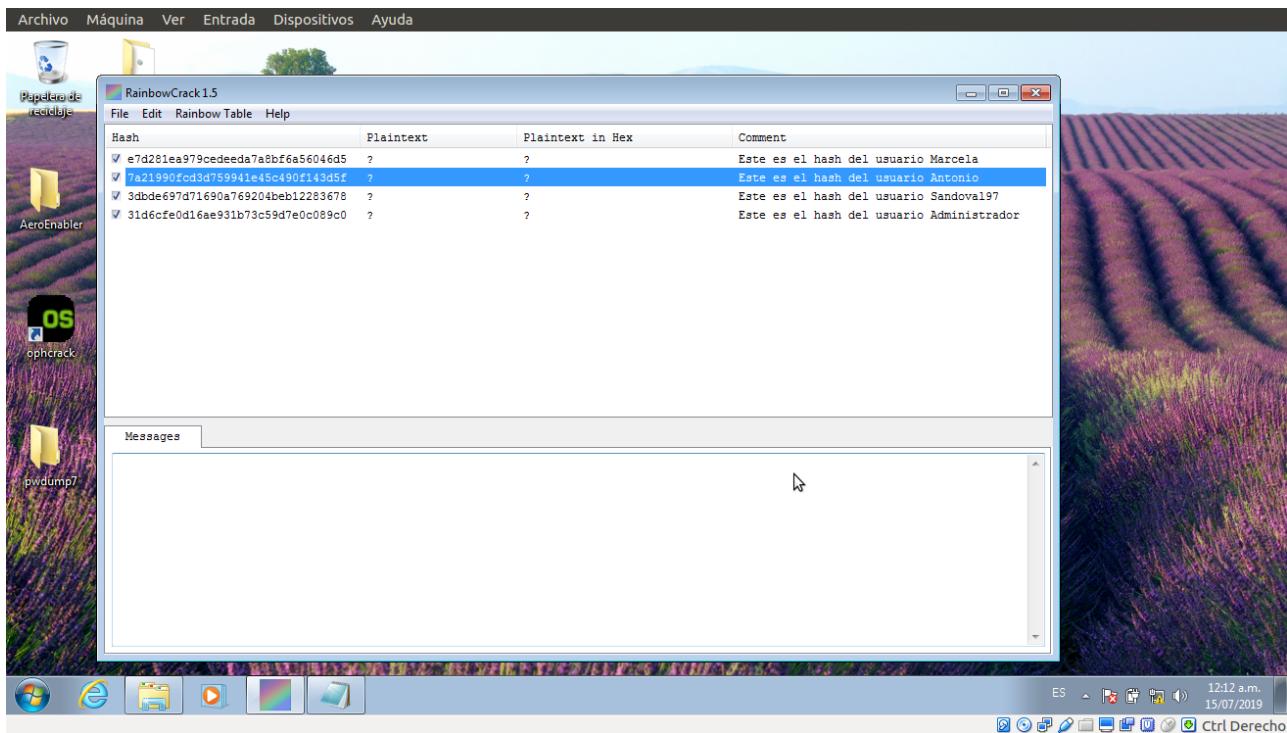


21. El hash seleccionado se agrega a RainbowCrack, como se muestra en la siguiente captura de pantalla.



22. Para agregar más hashes, repita en los pasos anteriores 16-20

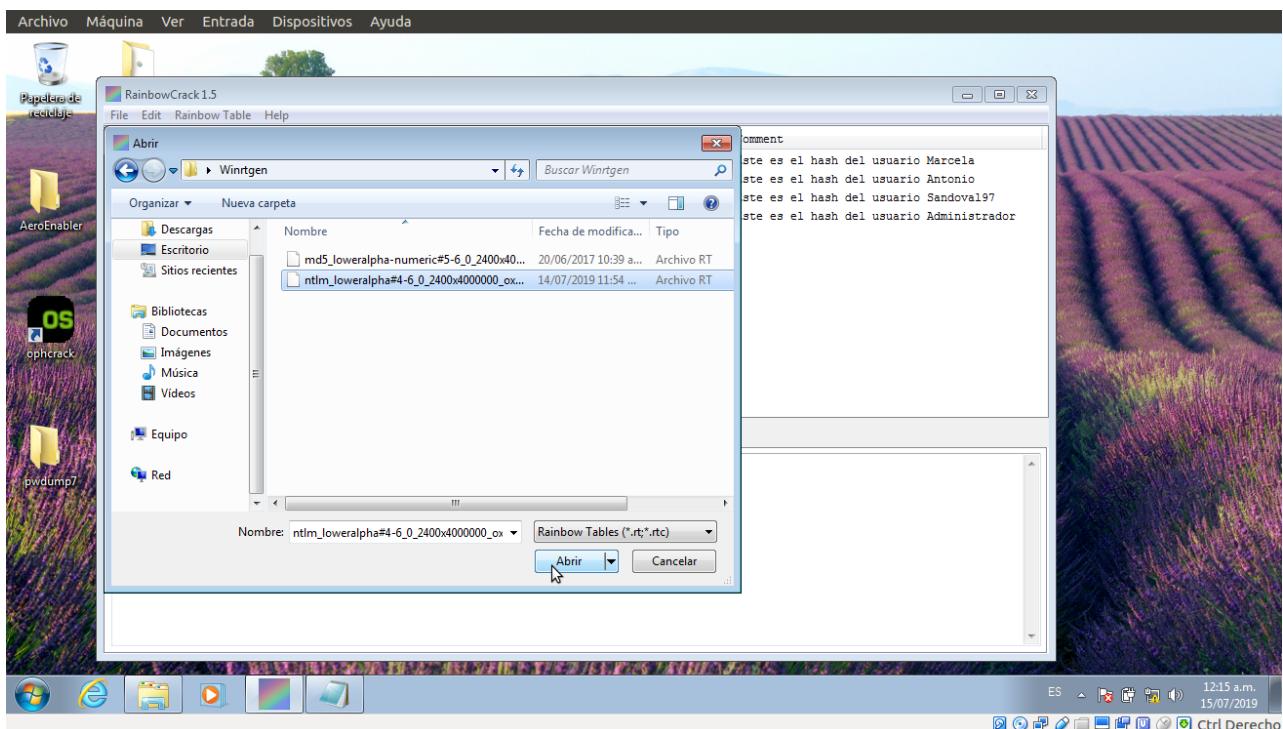
23. Los hashes agregados se muestran en la siguiente captura de pantalla.



24. Haga clic en el menú Rainbow Table y haga clic en buscar rainbow tables.

25. Navega hasta la Rainbow table, ubicada en Escritorio/Winrtgen

26. Clic Abrir.



27. Tan pronto como haga clic en Abrir RainbowCrack, se abrirá el hash de la contraseña y se mostrarán las contraseñas en texto plano, como se muestra en la siguiente captura de pantalla

