Oscar Espinosa Curiel

Pass the Hash

Cuando un atacante logra vulnerar un sistema y de alguna manera obtiene los hashes de las contraseñas de autenticación de los usuarios, el sistema se vuelve vulnerable al ataque *Pass-the-Hash*. Dado que el tiempo necesario para romper un hash es bastante, se puede brincar este paso, haciendo con este tipo de ataque. Es común este ataque en sistemas Windows por la forma en que maneja sus sesiones, pues solo se necesita un inicio de sesión para que el usuario tenga acceso a sus recursos, ya que el hash de su contraseña se almacena en cache.

Pass-the-Hash consiste, pues, en suplantar los hashes de algún usuario por otro que el atacante conozca, haciéndose pasar finalmente por este usuario. El encargado en Windows de la administración de los hashes es *Local Security Authority Subsystem (%SystemRoot%\System32\Lsass.exe)*. Para esto es necesario para esto tener permisos administrativos, pues se requiere manipulación del archivo SAM.

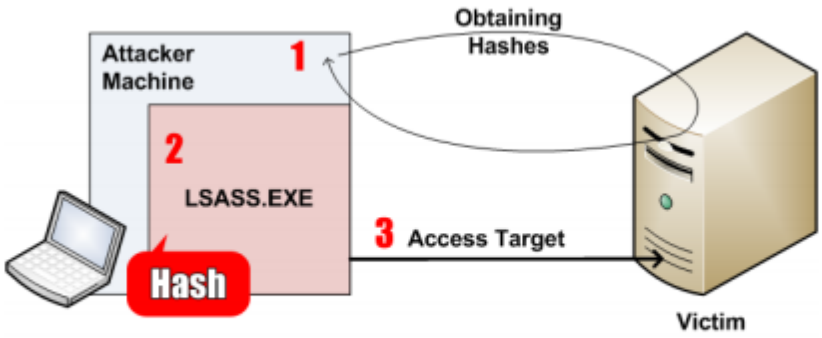

Figure 2-3: Pass-the-hash attack in action. Courtesy of Ed Skoudis. (Skoudis, 2008)

En el primer paso, el atacante obtiene los hashes de la víctima.

En el segundo paso, el atacante pone uno de los hashes que obtuvo (preferentemente de un usuario con permisos administrativos) en su Lsass local.

En el tercer paso, el sistema víctima proporcionará acceso al atacante en el servidor víctima sin necesidad de proporcionar una contraseña cada que el atacante intente acceder a la víctima.

Fuente

- Ewaida, Bashar. *Pass-the-hash attacks: Tools and Mitigation*. SANS Institute. 2010. Págs. 8-10. Recuperado de https://www.sans.org/reading-room/whitepapers/testing/pass-the-hash-attacks-tools-mitigation-33283