Volcado de los hashes «offline»

El «volcado de los hashes offline» es una práctica común en el ámbito de la seguridad informática, que consiste en obtener y almacenar los hashes de contraseñas de una base de datos fuera de línea, es decir, sin necesidad de acceder al sistema o aplicación en tiempo real.

Cuando se realiza un volcado de hashes offline, un atacante o un auditor de seguridad puede acceder a la base de datos de contraseñas de una aplicación o sistema, ya sea a través de una vulnerabilidad o mediante acceso no autorizado, y extraer los hashes de las contraseñas almacenadas en ella. Estos hashes se guardan en un archivo o base de datos separada para su posterior análisis.

Una vez obtenidos los hashes offline, un atacante puede intentar descifrar las contraseñas originales mediante diversas técnicas, como ataques de fuerza bruta, diccionario o utilizando tablas de arco iris. Estas técnicas buscan encontrar coincidencias entre los hashes obtenidos y una lista de posibles contraseñas precalculadas o generadas.

El volcado de hashes offline se utiliza en pruebas de penetración, evaluaciones de seguridad y análisis forenses para evaluar la fortaleza de las contraseñas almacenadas y la seguridad general de un sistema o aplicación. Sin embargo, también plantea riesgos significativos para la privacidad y la seguridad de los usuarios si los hashes no se protegen adecuadamente.

En el caso específico de Windows, se puede encontrar una copia de la SAM en diferentes ubicaciones, como %systemroot%\system32\config\sam y %systemroot%\winnt\system32\config\sam.bak. Además, si el

administrador ha realizado copias de seguridad, es posible encontrar una versión comprimida en %systemroot%\windows\repair\sam._. Una vez que se accede al archivo en cuestión, su contenido puede ser volcado utilizando herramientas como samdump. Sin embargo, a partir de Windows 2000, Microsoft implementa el sistema de cifrado Syskey, lo que dificulta la obtención de hashes LM y NTLM de manera directa. Aunque Syskey y los cifrados LM/NTLM se introdujeron para agregar seguridad adicional, en la práctica, la fortaleza de la contraseña elegida por el usuario sigue siendo crucial.