Leal González Ignacio

Ataque pass-the-hash

Un ataque pass-the-hash es un exploit en la que un atacante roba una credencial de usuario hash y, sin descifrarla, la reutiliza para engañar a un sistema de autenticación y crear una nueva sesión autenticada en la misma red.

Para ejecutar un pass-the-hash, el atacante primero obtiene los hashes del sistema objetivo utilizando cualquier número de herramientas de hash-dumping. Luego, se utiliza una herramienta pass-the-hash para colocar los hashes obtenidos en un servicio de subsistema de autoridad de seguridad local. Esto a menudo engaña a un sistema de autenticación basado en Windows para que crea que el punto final del atacante es el del usuario legítimo, y proporcionará automáticamente las credenciales necesarias cuando el atacante intente acceder al sistema de destino. Todo esto se puede lograr sin necesidad de la contraseña original.

Para mitigar la amenaza de un ataque pass-the-hash, las organizaciones deben garantizar que solo se pueda acceder a los controladores de dominio desde sistemas de confianza sin acceso a Internet. La autenticación de dos factores que utiliza tokens también debe aplicarse, así como el principio de privilegio mínimo. Las organizaciones deben monitorear de cerca los hosts y el tráfico dentro de sus redes para detectar actividades sospechosas.

Por lo general, los ataques de hash se dirigen a sistemas Windows, pero también pueden funcionar contra otros sistemas operativos en algunos casos y cualquier protocolo de autenticación como Kerberos. Windows es especialmente vulnerable a estos ataques debido a su función de inicio de sesión único (SSO) que permite a los usuarios ingresar la contraseña una vez para acceder a todos los recursos. El SSO requiere que las credenciales de los usuarios se almacenen en caché dentro del sistema, lo que facilita el acceso de los atacantes.

Un informe de 2009 de SANS muestra cómo los atacantes podrían emplear el uso de ataques de hash combinados con la explotación del lado del cliente para comprometer la red interna de una organización y robar datos importantes.

Referencias

https://searchsecurity.techtarget.com/definition/pass-the-hash-attack