López Fernández Servando Miguel

Pass the Hash Attack

Un ataque Pass-the-Hash (PtH) es una técnica mediante la cual un atacante captura un hash de contraseña y luego simplemente lo pasa a través de la autenticación El actor de amenazas no necesita descifrar el hash para obtener una contraseña en texto claro. Los ataques de PtH explotan el protocolo de autenticación, ya que el hash de las contraseñas permanece estático para cada sesión hasta que se gira la contraseña. Los atacantes comúnmente obtienen hashes exfiltrando la memoria activa de un sistema y otras técnicas.

Si bien los ataques Pass-the-Hash (PtH) pueden ocurrir en Linux, Unix y otras plataformas, son más frecuentes en los sistemas Windows. En Windows, PtH explota el inicio de sesión único (SS0) a través de NT Lan Manager (NTLM), Kerberos y otros protocolos de autenticación. Cuando se crea una contraseña en Windows, se almacena en el administrador de cuentas de seguridad (SAM), en la memoria del proceso del subsistema de autoridad de seguridad local (LSASS), en el almacén del administrador de credenciales (CredMan), en una base de datos ntds.dit en Active Directory. Por lo tanto, cuando un usuario inicia sesión en una estación de trabajo o servidor de Windows, esencialmente deja atrás sus credenciales de contraseña. Por esta razón es más común encontrar ataques del tipo Pass de Hash en sistemas operativos windows.

A continuación se describirán de manera general los pasos a seguir para realizar un ataque PtH.

1. Un atacante gana acceso a un equipo de la red mediante técnicas como phishing, contraseñas débiles, o explotando vulnerabilidades sin parche. A partir de este momento utiliza este equipo como pivote.

2. Una vez que se obtiene derecho administrativo, el atacante puede capturar las credenciales de las cuentas y usarlas para autenticarse en otros equipos de la red.

3. Si el atacante es capaz de tener acceso al controlador de dominio, obtendrá el control y acceso completo a todos los activos de la organización.

Para dejar más concreta la definición, un PtH es un método para autenticarse como un usuario sin tener una contraseña en texto claro. Este método pasa por alto los pasos de autenticación estándar que requieren una contraseña de texto claro, moviéndose directamente a la parte de la autenticación que utiliza el hash de contraseña. En esta técnica, los hashes de contraseña válidos para la cuenta que se está utilizando se capturan utilizando una técnica de acceso de credenciales. Los hashes capturados se utilizan con PtH para autenticarse como ese usuario. Una vez autenticado, PtH puede utilizarse para realizar acciones en sistemas locales o remotos.

Referencias

https://www.beyondtrust.com/resources/glossary/pass-the-hash-pth-attack
https://attack.mitre.org/techniques/T1075/