Vallejo Fernández Rafael Alejandro

Pass-the-hash

Consiste en auntenticarse como un usuario sin la necesidad de tener la contraseña en texto claro y lo hace utilizando el hash de la contraseña.
Los hashes de las contraseñas que se utilizan se capturan con una técnica de acceso a credenciales. Una vez que son capturados se utilizan para autenticarse como ese usuario.

Es entonces que esta técnica es aplicada en Windows porque un atacante aprovecha los hashes LM o NTLM (que utiliza SSO - Single Sign-On) de la contraseña de un usuario para auntenticarse en un directorio o recurso.

SSO permite que los usuarios pongan una vez su contraseña (sin pedirla nuevamente después) para poder utilizar los servicios que tienen permitidos.

El hash de la contraseña se almacena en LSASS (Local Security Authority Subsystem) y Lsass.exe es quien se encarga de la autenticación.

La forma en que un atacante consigue los hashes de las contraseñas es mediante herramientas específicas como Mimikatz y extrayendo los hahses de la memoria del equipo comprometido.

Es importante mencionar que para sacarlas de la base de datos de Windows SAM o de la memoria se requiere de permisos de administrador.

El ataque de pass-the-hash reduce el tiempo en comparación con el crackeo o tratar de adivinar la contraseña de la víctima.

Algunas herramientas para realizar el ataque son:

- Pshtoolkit
- Msvcrl
- Metasploit PSEXEC module
- Mimikatz
- Tenable smbshell
- pwdump7
- Metasploit hashdump module

Referencias:

Ewaida, B. (2010). Pass-the-hash attacks: Toolsand Mitigation. Recuperado de: https://www.sans.org/reading-room/whitepapers/testing/pass-the-hash-attacks-tools-mitigation-33283