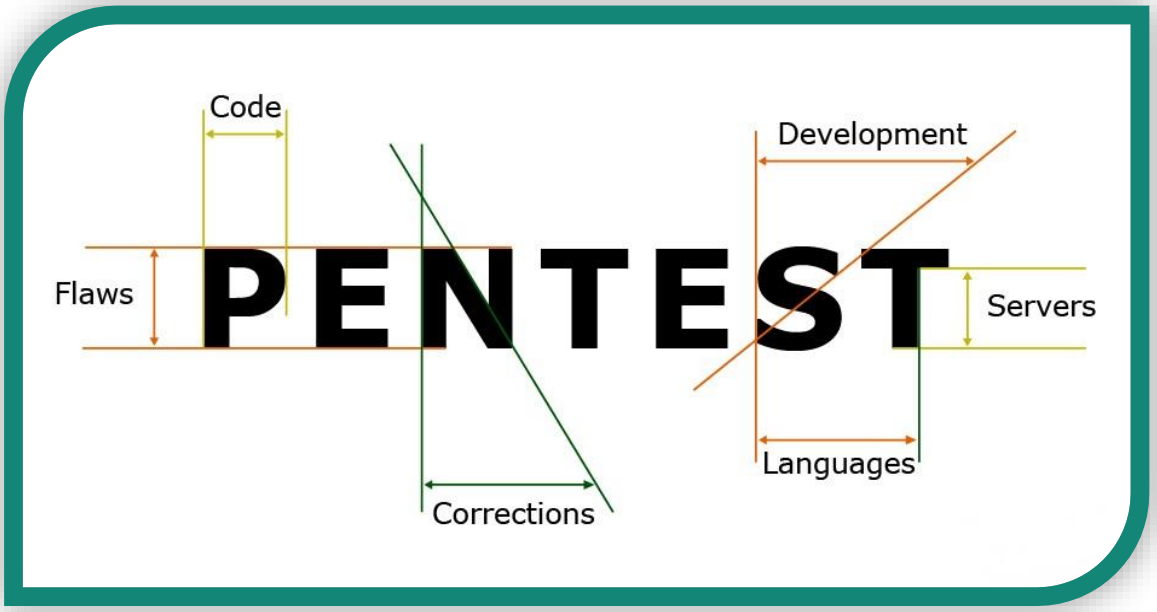
Pass the Hash (PtH)

Pruebas de Penetración



Pacheco Franco Jesús Enrique

jesus.pacheco@bec.seguridad.unam.mx

17/Abril/2019

Objetivo

Describir en que consiste un ataque del tipo Pass the Hash.

Descripción

Este tipo de ataques está enfocado a atacar sistemas que funcionen con un Windows Server que implemente Active Directory como mecanismo de autenticación centralizada.

El ataque se basa en haber logrado comprometer algún equipo dentro del dominio, una vez logrado esto lo que se intenta hacer es pivotear tratando de obtener mas credenciales y así escalar privilegios. Para lograr hacernos de mas credenciales lo que se hace es extraer los hashes NTLM de los usuarios almacenados localmente. Una vez obtenidos no tenemos que tratar de obtener la contraseña con Rainbow Tables o algo por el estilo ya que debido a la manera en la que trabaja Active Directory podemos utilizar directamente el Hash para autenticarnos por red.

El proceso de autenticación que permite esto se llama LSASS y cómo funciona es que una entidad llamada file server envía un desafío al cliente el cual consiste en cifrar un numero aleatorio de 16 bytes con el hash obtenido a partir de la contraseña, el cliente envía dicho numero cifrado al File Server y ahora el File Server envía al Domain Controller el usuario, el número en claro y el número cifrado por el cliente para que este lo verifique por que el DC almacena todos los usuarios y los hashes de las contraseñas, entonces descifra el numero cifrado con el hash que tiene del cliente y si coincide lo que se descifra con el número que recibió en claro del File Server entonces se le concede el acceso al cliente.

Como podemos observar en el proceso anterior en ningún momento necesitamos la contraseña en claro para autenticarnos, basta con tener el hash y por eso resultan tan peligrosos este tipo de ataques, sin embargo, parece ser que en sistemas operativos modernos esto ya ha sido corregido.

Referencias

- Elladodelmal.com. (2014). *Mitigación de ataques Pass-the-Hash y Pass-the-Ticket*. [online] Available at: http://www.elladodelmal.com/2014/07/mitagacion-de-ataques-pass-hash-y-pass.html [Accessed 17 Apr. 2019].
- YouTube. (2016). *What is a 'Pass-the-Hash' attack?*. [online] Available at: https://www.youtube.com/watch?v=cBXdoIuLzmA [Accessed 17 Apr. 2019].