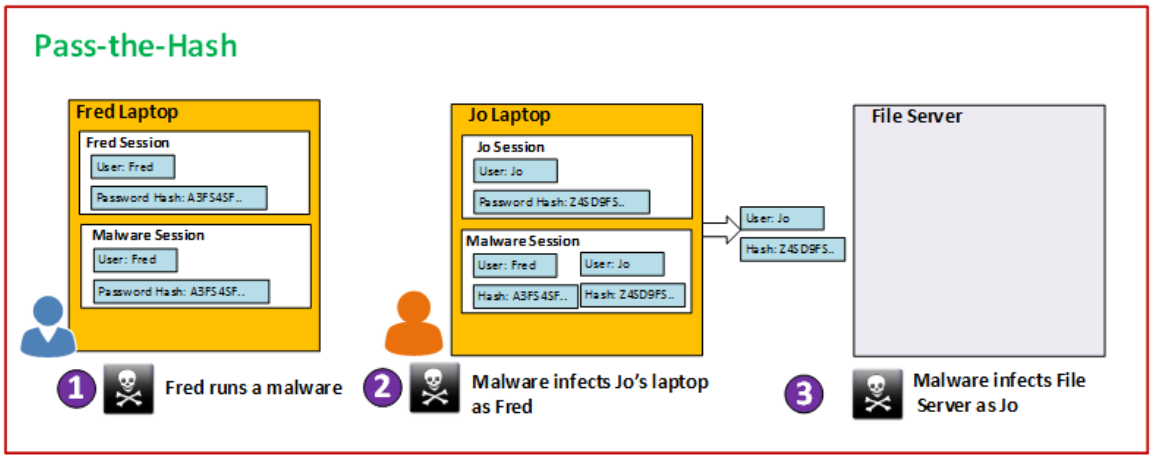
Diana G. Tadeo Guillén

PASS THE HASH ATTACK



Es un tipo de ataque muy comúnmente usado durante los últimos años en los equipos Windows pues usan la autenticación tipo NTLM (Para Active Directory) tomando en cuenta el hecho de que las contraseñas de los usuarios nunca se envían en texto claro.

En el momento en que un usuario decide acceder con su contraseña a alguna aplicación del dominio, esta contraseña se pasa del texto en claro a un hash del tipo LM o NT, enseguida, este hash es enviado al servidor remoto. El análisis de este mecanismo ha demostrado que la contraseña de texto no es necesaria para completar la autenticación de la red con éxito, solo se necesitan los hashes.

Si un atacante tiene los hashes de la contraseña de un usuario, no necesita forzar la contraseña de texto simple; simplemente pueden usar el hash de una cuenta de usuario arbitraria que han recopilado para autenticarse en un sistema remoto y hacerse pasar por ese usuario.

Sin embargo, los hashes de contraseña solo pueden ser robados si un atacante ingresa a la red.

Por ejemplo, si un atacante convence a un empleado para que revele sus credenciales a través de un ataque de phishing o infecta la computadora de un empleado de bajo nivel con malware. Una vez dentro de la red, todo lo que un atacante debe hacer es esperar hasta que el empleado tenga un problema con su computadora, llame a TI y alguien de TI se detenga con sus credenciales administrativas para solucionar el problema.

Cuando su administrador de TI ingresa credenciales de cuenta privilegiadas. Si el atacante puede capturar el hash, puede usarlo en cualquier lugar de la red, sin necesidad de conocer la contraseña original.

REFERENCIAS

https://thycotic.com/solutions/pass-the-hash-attacks/