TIC

TALENTO TECH

REGIÓN 3

CAUCA – NARIÑO

LECCIÓN 3-UNIDAD 3

Universidad Tecnológica de Pereira | faceIT

Ataques a la autenticación

Son ataques que se lanzan contra las credenciales de una persona para hacerse pasar por ese usuario. Una vez se roban las credenciales, el atacante puede hacerse pasar por el usuario y robar información, instalar malware o causar daños a un sistema de datos. Una técnica muy común es empleando la fuerza bruta. Por ejemplo, en el caso de los 4 dígitos de una clave de una cuenta bancaria, un ataque de fuerza bruta consistiría en in intentando todas las combinaciones hasta dar con la correcta. Generalmente estos ataques se pueden detener bloqueando la cuenta luego de cierta cantidad de intentos fallidos de ingresar, o colocando temporizadores para que un usuario no pueda intentar acceder luego de unos minutos si ha fallado en ingresar más de cierto número de oportunidades.

Ataques de diccionario Son ataques similares a los de fuerza bruta, con la diferencia de que se cuenta con un diccionario de palabras y números de uso frecuente y asociados a un usuario. Estos ataques se pueden prevenir agregando símbolos y combinaciones de varias palabras en una contraseña para que sea más robusta.

Relleno de credenciales

Es común que un usuario utilice el mismo nombre y contraseña en muchos sitios web. Algunos seguros, que tienen el cifrado necesario y garantizan el buen manejo de la información y otros sitios que no tienen un nivel apropiado de seguridad. El ataque de relleno de credenciales consiste en que el atacante buscará nombres de usuario y contraseñas en bases de datos obtenidas al vulnerar sistemas poco seguros. Con esas credenciales el atacante automatizará intentos de inicio de sesión en muchas plataformas hasta obtener algún ingreso exitoso. Para evitar estos ataques es importante que no se empleen las mismas contraseñas en diferentes sitios, validar las prácticas de seguridad de los portales a los que se ingresa información y cambiar a menudo las contraseñas.

Registro de claves

Este ataque consiste en un programa que registra y guarda todas las teclas que se pulsan en el teclado. Comúnmente se encuentran en ciber cafés y computadores de uso compartido, en donde un atacante ha instalado el software de registro. El atacante que tiene acceso a esos datos intentará rellenar credenciales según la información legible en los registros del teclado. Para evitarlo no se deben digitar claves en computadores compartidos y se deben evitar las instalaciones de software cuyo origen sea desconocido.

Ingeniería social

La ingeniería social conlleva intentar que una persona revele información o realice una acción para hacer posible un ataque.

La mayoría de los ataques de autenticación implican la vulneración de equipos o el proceso de probar muchas combinaciones de credenciales. Los ataques de ingeniería social son diferentes, ya que aprovechan las vulnerabilidades de las personas. El atacante intenta ganarse la confianza del usuario legítimo y persuadirle para que divulgue información o realice una acción que posibilite causar daños o robar información.

Se pueden usar varias técnicas de ingeniería social para el robo de autenticación, entre las que se incluyen las siguientes:

- **La suplantación de identidad (phishing)** se produce cuando un atacante envía un correo electrónico aparentemente legítimo con el objetivo de lograr que un usuario revele sus credenciales de autenticación. Por ejemplo, puede parecer que un correo electrónico lo ha enviado el banco del usuario. Se abre un vínculo a lo que parece la página de inicio de sesión del banco, pero en realidad es un sitio falso. Cuando el usuario inicia sesión en el sitio falso, sus credenciales quedan a disposición del atacante. Existen diversas variantes de suplantación de identidad, incluido el phishing de objetivo definido, que suele estar dirigido a organizaciones, empresas o personas concretas.

- **El pretexto** es un método por el cual un atacante se gana la confianza de la víctima y le convence para que divulgue información segura. Después, puede

- usar estos datos para robar su identidad. Por ejemplo, un hacker podría llamarle por teléfono fingiendo ser del banco y pedirle su contraseña para comprobar su identidad. Podrían pedirle que responda a una encuesta o un cuestionario con preguntas aparentemente aleatorias e inocentes que le harán revelar datos personales, o bien podrían enviarle un mensaje con un juego divertido, como crear el nombre de su grupo de pop imaginario con su lugar de nacimiento y el nombre de su primera mascota.

- **El baiting** es una forma de ataque en el que el delincuente ofrece una recompensa o un premio falsos para animar a la víctima a divulgar información segura.