Teléfono: 01 (33) 36 38 76 85

INGENIERIA SOCIAL

MANIPULACIÓN DE PERSONAS POR INTERNET.

La ingeniería social consiste en la manipulación de las personas para que voluntariamente realicen actos que normalmente no harían; aunque a nadie le gusta ser manipulado, en algunos casos no es excesivamente perjudicial (por ejemplo un vendedor puede aplicar ingeniería social para conocer las necesidades de un cliente y ofrecer así mejor sus productos), si las intenciones de quien la pone en práctica no son buenas se convierte quizás el método de ataque más sencillo, menos peligroso para el atacante y por desgracia en uno de los más efectivos. Ese atacante puede aprovechar el desconocimiento de unas mínimas medidas de seguridad por parte de personas relacionadas de una u otra forma con el sistema para poder engañarlas en beneficio propio. Por ejemplo, imaginemos que un usuario de una máquina Unix recibe el siguiente correo electrónico:

From: Super-User <root@sistema.com>
To: Usuario <user@sistema.com>
Asunto: Cambio de clave
Hola,
Para realizar una serie de pruebas orientadas a conseguir un óptimo funcionamiento de nuestro sistema, es necesario que cambie su clave mediante la orden 'passwd'. Hasta que reciba un nuevo aviso (aproximadamente en una semana), por favor, asigne a su contraseña el valor 'PEPITO' (en mayúsculas). Rogamos disculpe las molestias. Saludos, Administrador

Si el usuario no sabe nada sobre seguridad, es muy probable que siga al pie de la letra las indicaciones de este e-mail; pero nadie le asegura que el correo no haya sido enviado por un atacante - es muy fácil camuflar el origen real de un mensaje -, que consigue así un acceso al sistema: no tiene más que enviar un simple correo, sin complicarse buscando fallos en los sistemas operativos o la red, para poner en juego toda la seguridad. Sin saberlo, y encima pensando que lo hace por el bien común, el usuario está ayudando al pirata a romper todo el esquema de seguridad de nuestra máquina.

Pero no siempre el atacante se aprovecha de la buena fe de los usuarios para lograr sus propósitos; tampoco es extraño que intente engañar al propio administrador del sistema4.1. Por ejemplo, imaginemos que la máquina tiene el puerto finger abierto, y el atacante detecta un nombre de usuario que nunca ha conectado al sistema; en este caso, una simple llamada telefónica puede bastarle para conseguir el acceso:

Administrador: Buenos días, aquí área de sistemas, ¿en qué podemos ayudarle?
Atacante: Hola, soy José Luis Pérez, llamaba porque no consigo recordar mi password en la máquina sistema.upv.es.
Administrador: Un momento, ¿me puede decir su nombre de usuario?
Atacante: Sí, claro, es jlperez.
Administrador: Muy bien, la nueva contraseña que acabo de asignarle es rudolf. Por favor, nada más conectar, no olvide cambiarla.
Atacante: Por supuesto. Muchas gracias, ha sido muy amable.
Administrador: De nada, un saludo.

Como podemos ver, estamos en la situación opuesta a la anterior: ahora es el root quien facilita la entrada del atacante en la máquina; lo único que este ha necesitado es un nombre de usuario válido.

Evidentemente, cualquier mensaje, llamada telefónica o similar que un usuario reciba debe ser puesto inmediatamente en conocimiento del administrador del sistema; hay que recordar a los usuarios que en ningún caso se necesita su contraseña para realizar tareas administrativas en la máquina. De la misma
forma, si es el administrador quien directamente recibe algo parecido a lo que acabamos de ver, quizás sea conveniente notificar el hecho a los responsables de la organización, y por supuesto poner la máxima atención en la seguridad de los sistemas involucrados, ya que en este caso se sabe a ciencia cierta que alguien intenta comprometer nuestra seguridad; en [Rad97] y [WD95] se muestran algunas de las reglas básicas que debemos seguir en nuestra organización para prevenir ataques de ingeniería social y también para, en el caso de que se produzcan, reducir al mínimo sus efectos.