Capítulo 1
Introducción

1. Preámbulo

Las redes y los sistemas informáticos se vuelven cada vez más complejos y más grandes. Para ciertas empresas son un mal necesario, y lo que podría ser una inversión se transforma en una ruina. De esta imagen, se deriva muchas veces el poco interés en aumentar el presupuesto destinado a la seguridad informática. Los administradores tienen hoy en día mucha carga de trabajo y preocupaciones. Están sometidos a una gran presión para alcanzar resultados rápidos en materia de despliegue o mantenimiento. No disponen, por lo tanto, de tiempo para prestar atención a los detalles de la instalación de un producto o una aplicación. Están desgraciadamente obligados a ir lo más rápido posible y parar en cuanto funcione, sin haber tomado el tiempo para analizar la seguridad antes o después de la instalación. Además, la seguridad interna es muchas veces descuidada en detrimento de una protección frente a una eventual amenaza externa.

Sin embargo, si la seguridad fuese perfecta en el interior, ¿qué podría hacer realmente un hacker externo?

Diferentes estudios demuestran que la seguridad informática de una empresa es en la mayoría de los casos fácilmente atacable desde el interior, además muestran también un aumento considerable de este tipo de incidentes, ya sea por usuarios ávidos o frustrados por la falta de poder o por personas que tienen malas intenciones, como vengarse, espiar, robar o destruir informaciones críticas o privadas. La realidad es tal y como la presentamos. Técnicas de hacking son regularmente empleadas con este fin. ¿Lo ha constado en su empresa?

En una empresa, los usuarios que carecen de funciones de administración informática tienen la mayoría de las veces permisos limitados sobre su puesto de trabajo. Esto tiene como finalidad proteger la máquina contra instalaciones de programas que pueden poner en peligro la red o que no se adaptan a la política de seguridad, si es que tal política existe. Tiene además como objetivo evitar que un empleado sea manipulado sin su consentimiento por un pirata interno o externo. Por lo tanto, es habitual únicamente otorgar a un usuario los permisos vinculados al software previsto para sus funciones.

Sin embargo, existen herramientas para evitar esta atribución de rol y, a su vez, poder hacer lo que se desea en el puesto de trabajo o en un servidor. También es posible ir aún más lejos; por ejemplo, obtener el rol de System en una máquina o llegar a ser administrador de un dominio entero. Algunos métodos son puramente técnicos mientras que otros necesitan además la interacción humana para conseguir las autorizaciones buscadas.

Para simplificar la acción de los piratas, no es extraño encontrarse con que un responsable informático concede más permisos de los necesarios, sin tener en cuenta los riesgos a los cuales se expone. Suele ocurrir que, en una empresa, todos los usuarios sean administradores de sus puestos de trabajo, lo que provoca una brecha ideal para realizar acciones de pirateo eficaces.

Además, los mecanismos de seguridad puestos en marcha por Microsoft son a veces mal entendidos. Los que se consideran pesados o intrusivos son muchas veces desactivados o no configurados para simplificar el trabajo. Sin estas protecciones, a pesar de que se activan por defecto, como por ejemplo el UAC (*User Account Control*) o la obligación de tener una macro firmada en un documento de Office, resulta trivial piratear una máquina, como sucedía con Windows XP.

A medida que avance en este libro, va a descubrir cómo obtener el control al ser un usuario con pocos o ningún permiso sobre un puesto de trabajo o un servidor. Esta obra aporta asimismo contramedidas técnicas, así como una respuesta en términos de administración sobre la problemática del hacking interno.

Las empresas dispondrán así de los medios necesarios para prevenir estos ataques antes de que ocurran e impedirlos.

2. Desciframiento de un ataque conseguido

Cuando se va de vacaciones, empieza en general por elegir el destino y esta decisión está condicionada por el presupuesto. Después de haber elegido el destino, se interesa por el itinerario, hasta conseguir la mejor relación calidad/precio. Una vez realizada su elección, lleva a cabo la reserva. Por fin llega el día de irse de vacaciones. Y allí, sin darse cuenta, ha realizado un proyecto empezando por la fase de estudio de las posibilidades. En cuanto tiene una ocasión, aprovecha para ampliar los detalles. Esta es la mejor manera de proceder para este tipo de proyecto: estudiar las oportunidades, analizar en detalle la posible o las posibles soluciones, para ir ahondando más en el detalle.

Al igual que en la metáfora anterior, el ataque de un sistema se desarrolla generalmente en varias fases. Las primeras consisten en la búsqueda de informaciones y la toma de huellas. Como habrá entendido, es lo mínimo que se debe hacer para llevar a buen puerto el proyecto. Todos los jefes de Estado lo han comprendido así. Trabajan siempre en colaboración con las agencias de inteligencia mucho antes de que un conflicto empiece. Las primeras fases son seguidas de la fase de ataque, la cual se elabora y testea en detalle. Copiar y pegar un script de este libro no basta para conseguir su proposito en las mejores condiciones; piense en dedicar el tiempo necesario para probar sus futuras acciones al igual que los militares prueban los nuevos misiles. Después, una vez el ataque está en desarrollo o terminado, resulta interesante conservar un control sobre los sistemas atacados para reducir el riesgo de volver a lanzar un nuevo ataque. Esto se realiza gracias a la instalación de una puerta trasera. Al terminar debemos borrar todo rastro para dejar los servidores «tan limpios como los ha encontrado al entrar». El enemigo no debe saber que hemos atacado, pero, si se diese cuenta, no debería saber quién lo ha hecho.

Este libro le ayudará en todas las tareas de este proceso. Guarde en mente que un ataque no es bueno si lo lanza al azar. Prepárese con minucia y pruebe sus técnicas como un mago prepara todos sus trucos. Al final, el éxito de todo proyecto se basa en una buena preparación.

3. Descifrado de contramedidas eficaces

Una contramedida eficaz es una contramedida que sabe contrarrestar en la medida de lo posible varios ataques potenciales sin que estos hayan sido forzosamente descubiertos como amenazas. La defensa debe aplicarse a 360º. No se trata de cerrar una puerta con dos vueltas de llave y dejar una ventana abierta de par en par. Es tan importante añadir un toque de gestión definiendo los procesos de control como controlar que todas las puertas y ventanas estén bien cerradas en su apartamento antes de que se vaya de vacaciones. Esta parte no es técnica, sino absolutamente procedimental. Es preciso entender perfectamente los riesgos técnicos y, para eso, resulta indispensable comprender el engranaje del *internal hacking* con objeto establecer una defensa a la altura de la amenaza.

3.1 Análisis de riesgos reales

Para defenderse correctamente, debe saber lo que se arriesga. Protegerse frente a lo desconocido es muy difícil en la medida en que no se desea bloquear todo. El análisis de riesgos debe tener en cuenta, por lo tanto, las amenazas reales y no solamente los riesgos catalogados en un listado, que en la mayoría de los casos da consignas generales para abarcar el máximo número de ellos. Pero al tratar de protegernos de un riesgo impreciso, nos arriesgamos a establecer medidas técnicas y procedimentales costosas, largas y complejas, todo eso para, quizás, no dar cobertura al riesgo real.

3.2 Consideraciones técnicas

Una defensa debe tener en cuenta aspectos técnicos aunque estos den una respuesta menos general o menos variable a una amenaza. Para preparar contramedidas adecuadas técnicamente, se debe utilizar el análisis de riesgos (reales) y así responder con los medios adecuados. Piense en comparar las soluciones integradas, muchas veces gratuitas, con las soluciones de pago que no aportan siempre una verdadera plusvalía. Debe cubrir los riesgos a 360°. He visto muchas veces que, para impedir que un usuario instale un programa en su puesto de trabajo, se bloquean las descargas de Internet, gracias a un proxy web. Pero, cuando se impide que un usuario descargue un programa, ¿realmente se impide que instale una aplicación? Algunas piensan que, si un usuario no es administrador de su puesto de trabajo, no puede instalar nada: pero esto es una falacia. Puede instalar ciertos programas o utilizar aplicaciones portables. Puede realizar sus propios programas. ¿El riesgo es la instalación o la ejecución de una aplicación peligrosa? Teniendo en cuenta todos estos aspectos puede considerar que cubre el riesgo a 360°.

3.3 Consideraciones sobre la gestión

La gestión de sistemas es importante. Si piensa solo en términos técnicos, va a dejar de lado ciertos fundamentos de la seguridad. Un ejemplo sencillo: si desea tener acceso a un proxy que vigila las conexiones a Internet de sus usuarios, debe prevenirles. Esto puede realizarse dentro de una política de seguridad, que incluye el reglamento de utilización de la infraestructura informática. Si la sala de servidores llegara a quemarse, ¿sabría cómo organizar los recursos humanos e informáticos para reinstalar un sistema lo más rápidamente posible y que esté disponible para que los profesionales puedan seguir trabajando? Cuando alguien deja la empresa, ¿qué ocurre con sus archivos, sus correos electrónicos, su cuenta de dominio, etc.? Cuando se detecta en la red un ataque por virus, ¿cómo reaccionan los usuarios?, ¿cuál es el proceso que informa del ataque? ¿qué sistemas permitirán investigar y resolver el problema?

Como habrá entendido, aunque los aspectos técnicos son muy importantes, no deben ser la guía para la puesta en marcha de contramedidas y en general para la instalación de una solución informática. La gestión de sistemas le ayudará a tener en cuenta los riesgos, pero deberá considerar también la formación de sus profesionales y los costes, lo que da un resultado mucho más cercano a las necesidades generales de la empresa que una solución realista y aplicable en términos de seguridad.

4. ¿Qué acciones, para qué roles?

Debe, antes de empezar a buscar información, saber en qué consisten los roles existentes y qué permiten hacer en el entorno dentro del cual trabaja.

Existen globalmente tres roles principales definidos: el de administrador local, que puede realizar cualquier cosa en su ordenador, el de administrador de dominio, que puede realizar casi cualquier tarea sobre el conjunto de ordenadores de la empresa y, por último, el más extendido, el de usuario, que se ha configurado para simplemente utilizar el sistema que le han asignado, es decir, para solamente realizar su trabajo. Existen variantes de estos roles que se crean con la ayuda de grupos de seguridad y de reglas de seguridad específicas muchas veces ligadas a un rol profesional, como contable, comercial, técnico en informática, etc.

A decir verdad, esquivando la utilización clásica del sistema y del rol que el responsable informático le ha atribuido, puede ir mucho más allá de lo que cree.