Seguridad en la Red

Ramón Barreiro López

1. Comunicación

Antes de saber en qué consiste la seguridad en una red, o en un único ordenador, vamos a explicar porqué son vulnerables.

Vamos a comenzar explicando cómo se comunica un ordenador que forma parte de una red, y para ello nos vamos a centrar en la comunicación a través de Internet, la red más grande. Dentro de Internet, como en cualquier otra red, lo que se realiza es el intercambio de información entre los equipos (en este caso, de lo más diversa). Por ejemplo, si se realiza una búsqueda en Internet, se envía una consulta y se recibirá una respuesta. Pero, ¿qué es lo que sucede? ¿Por qué nos llega la información y cómo lo hace?

En la vida cotidiana se utilizan habitualmente tipos de comunicación similares. Por ejemplo, se puede intercambiar información a través de un teléfono, teniendo en cuenta que antes de establecer la comunicación hay que marcar un número, con lo que el sistema encamina nuestro equipo hacia otro, que es el deseado. Al establecer la comunicación se puede efectuar el intercambio de información. Otro método de intercambio de información sería el que se utiliza mediante el correo postal (las cartas de toda la vida); con este método hay que escribir las cartas antes de enviarlas al destino, y luego echarlas a un buzón, que es el medio utilizado como enlace. Y así podríamos comentar muchos más sistemas de comunicación.

Lo que podemos sacar en claro de estos ejemplos son dos cosas, una más evidente que la otra. La primera es que para enviar información es necesario que nuestro destinatario esté "registrado" en la red de comunicación que utilicemos. En Internet la dirección que hace único a nuestro ordenador dentro de la red es la *dirección IP*. La otra, menos clara pero más lógica, es que si realizamos una llamada por teléfono el destinatario no recibirá una carta, sino que sonará su teléfono. De igual modo si escribimos una carta, en el destino no se recibirá un mensaje sms. Con este razonamiento podemos darnos cuenta de que la información debe ser *clasificada* para poder enviarla a su sitio correcto, en el formato y mediante los procesos correctos, para que pueda ser interpretada de forma correcta. Para realizar esto los ordenadores utilizan los *puertos*. Pero en este caso no nos referimos a

un puerto hardware; es decir, dentro de los ordenadores no existe una ranura especial para recibir datos de Internet como existe para las tarjetas gráficas, por ejemplo. El puerto del que hablamos es de tipo software, y es precisamente el que hará de enlace entre la información que llega del exterior y el software de nuestra máquina, que es capaz de convertir la información en algo comprensible por el ser humano. Los puertos tienen varios estados, y sólo pueden estar en uno de ellos. Los estados importantes para continuar con nuestra explicación son: *abierto* (el puerto puede recibir datos) y *cerrado* (el puerto rechazará todo lo que le llegue).

2. Intrusión

Una vez que conocemos la forma en la que se comunican los ordenadores dentro de una red, continuaremos con un esquema de cómo un intruso informático puede realizar un ataque a un ordenador víctima. Hoy en día existen infinidad de ataques diferentes para poder conseguir la finalidad que el intruso se proponga. Podemos citar algunos de estos métodos:

- *Trashing*: Su nombre indica algo así como "basureando", y consiste precisamente en meterse en la basura de la víctima para encontrar información. Hoy en día se practica bastante, y un ejemplo claro de esto es cuando en las noticias aparece una demanda a una empresa en la que discriminaban a las personas escribiendo los comentarios en los curricula que ellos mismos les entregaban. Estos informes se encontraron en la basura de la compañía.
- *Ingeniería social*: quizá éste sea el método más potente, y se basa en su totalidad en el error humano, centrándose en la confianza habitual que tienen las personas. Una frase que explica muy bien este método es: *"En el mundo de los ordenadores, si no tienes la contraseña no puedes entrar. Pero si alguien llama por teléfono se le cree sin más"* Kevin Mitnick (considerado el mayor hacker de ingeniería social de los Estados Unidos).
- La técnica de *Phising* (mails maliciosos para que la víctima introduzca un nombre de usuario y su contraseña) utiliza este método para realizar el ataque.
- Y para finalizar existe la detección de una víctima y la subsecuente explotación de sus vulnerabilidades a través de la red. Este método será el que explicaremos a continuación.

En cualquier caso, éstos son sólo algunos de los métodos más habituales, pero podemos decir que prácticamente existe un método diferente para cada forma de obtener información y para usarla en ataques de cualquier tipo.

Hemos de tener en cuenta que el hombre no es perfecto, por lo que comete errores y los acarrea en todo lo que hace; por ejemplo, a la hora de programar, aunque los programas realicen bien las tareas para lo que fueron diseñados, también contendrán errores, y por ello se recurre continuamente a los famosos *parches* en los programas. Este tipo de errores humanos son los que un intruso informático utilizará para poder explotar un sistema. Los errores a los que estamos haciendo referencia son a los de la programación del software que hay detrás de los puertos.

2.1. Detección de la víctima

Una vez que sabemos dónde se van a realizar los ataques de un intruso informático vamos a explicar cómo puede llegar hasta allí. En primer lugar, el atacante detectará a su víctima, lo que puede hacer por simple azar o buscando directamente una víctima concreta (recordemos que la víctima en la red estará perfectamente localizada a través de su dirección IP). Una vez que se tiene la dirección víctima, el siguiente paso será hacer un escaneo de los puertos del equipo.

2.2. Escaneo de puertos

Un escaneo de puertos, como casi todo en la informática, se puede realizar de diferentes formas. Para conseguir nuestro objetivo, nos limitaremos a explicar únicamente en qué consiste. Una definición simple es llegar a saber qué puertos están abiertos y cuáles cerrados. Esto servirá para saber qué servicios están activados y, naturalmente, detrás de un puerto abierto seguramente habrá un software vulnerable. Aunque tengamos instalado correctamente un *firewall*, en un principio todos los puertos del equipo estarán cerrados. Pero cuando se instale un programa que obligue a estar conectado a Internet (por ejemplo *eMule*) será necesario abrir ciertos puertos para que pueda fluir la información.

2.3. Explotación de debilidades

Una vez que se ha localizado un puerto abierto y un programa detrás de él, se puede comenzar a explotar sus debilidades. El número y el tipo de erro-

res que haya en un programa viene dado por los que el programador esté capacitado a cometer.

Como error más importante o común tenemos el gran error del programador que, por despiste o por malicia, hará que el propio programa proporcione algo de información restringida, ciertos privilegios de administración, etc. Otra posibilidad es que el atacante pueda inyectar código nuevo para que el programa ejecute lo que él desee. Es importante tener en cuenta que tras inyectar un código, lo que se ejecute desde entonces se ejecutará con los permisos que tenga el programa, es decir, cuando un usuario instala *eMule* el atacante hará lo que tenga permitido ese usuario. Pero hay que tener en cuenta que existen ciertos programas que tienen permisos de administrador (como puede ser *Internet Explorer*).

Hemos hablado de inyectar código, pero no de cómo se hace. Lo habitual es crear un programita denominado *exploit* que se lanzará hacia la víctima, al número de puerto deseado. La función del *exploit* consiste en atacar la vulnerabilidad que le permita inyectar su código, lo que sería la primera acción. Y la siguiente sería introducir el código para realizar las funciones que se deseen. Este *exploit* lo conseguiremos buscando en la red o, si se es un experto, se podrá programar personalmente.

Con esto finalizaría el ataque: se buscó la víctima, se buscaron sus vulnerabilidades y, si se encontraron, se terminó por atacarlas.

3. Puntos de vista del atacante

Este apartado es muy importante en cuánto a la cantidad económica que se deberá invertir en la seguridad de una red. Este balance se realizará, teniendo en cuenta dónde se encuentra la información y qué grado de dificultad existe para que ésta sea borrada, leída o modificada.

Antes de comenzar a enumerar diferentes puntos de vista, vamos a distinguir entre dos tipos de ataque. El primero al que haremos referencia será el *ataque físico*, ya que un ordenador, o incluso una red entera, puede encontrarse amenazado por ataques de la propia naturaleza. Por ejemplo, el sistema podría verse afectado por un terremoto o una simple tormenta que provoque apagones, interferencias eléctricas, etc. Por esta razón habrá que tener en cuenta la situación geográfica. También se consideran ataques físicos las condiciones que existan dentro de la propia red, donde será necesario tener una temperatura adecuada para que no se calienten en exceso o se quemen los dispositivos. Además, se recomienda incorporar fuentes de alimentación continuas, para evitar los cortes debidos a posibles apagones en la red.

El segundo ataque será a *nivel lógico*, en el que habrá que buscar desde qué puntos de vista puede ser vulnerable la red y, en caso de que sea atacada, saber a qué información se podrá acceder (ya sea para borrarla, leerla o modificarla) o qué tipo de control sobre la red podrá tener el atacante.

Siendo redundante en lo ya comentado anteriormente, en informática se puede hacer todo de distintas formas para alcanzar un mismo fin. En el apartado anterior enumeramos distintos tipos de ataques, y éstos podrán ser lanzados desde distintos puntos o zonas.

3.1. Zonas de ataque

El primer ataque del que se debe defenderse una red será aquel que provenga del exterior de la red, habitualmente desde Internet. Este tipo de ataque aunque sea el más fácil de reconocer, no tiene por qué ser el que más se produzca. Normalmente será realizado por: *hackers* (gurús de la informática que son capaces de crear sus propios métodos y programas), *supertscript kiddie* (persona con bastantes conocimientos de informática, que a la hora de atacar es consciente de lo que está haciendo y porqué, pero es alguien que necesita ser guiado y necesita disponer de ciertas herramientas) y *script kiddie* (estos son conocidos como consumidores de hacker, porque en realidad no saben con exactitud cuánto daño puede provocar su ataque, y normalmente la información para efectuar los ataques la obtendrán de revistas, la propia Internet, etc.).

La otra zona desde la que puede ser atacada una red será desde el interior, es decir, desde dentro de la propia red. Éste suele ser realizado principalmente por trabajadores descontentos. Quizá este ataque sea incluso más peligroso que el explicado anteriormente, debido a que el atacante estará enfadado y probablemente su finalidad es hacer el mal, lo que normalmente consiste en la destrucción de datos. Además no perderá tiempo intentando entrar en la red, ya que se encuentra dentro de la red. Esta posibilidad le beneficiará, ya que no necesitará ser un experto informático. Además, al pertenecer a la red seguramente sepa cómo esta estructurada, consiguiendo por ingeniería social puestos más altos de la red, pudiendo hacer su ataque más rápido y efectivo. Este tipo de ataque cada vez se da con mayor frecuencia, y lógicamente es mucho más difícil de evitar.

Hemos reflejado los puntos de vista más importantes respecto a las posibilidades de ataque. Sin embargo, a día de hoy la información viaja en múltiples formatos, y podemos pensar que no servirá de mucho crear una red supersegura, que nunca será totalmente invulnerable, si a la red pueden acceder muchas personas de las que no se tenga una confianza total, o también si se lleva una agenda de clientes, datos de gran valor o incluso una base de datos en un pendrive usb, que se puede perder fácilmente. En realidad, no hay que volverse paranoico, pero sí ordenado para saber en todo momento dónde está la información y cómo asegurarla.

4. Protección de la Red

Una vez analizados los tipos de ataque a los que puede verse sometida una red, y por quien o quienes pueden ser efectuados, será necesario intentar asegurarla. A continuación iremos explicando algunas de las técnicas usadas actualmente, dependiendo de qué es lo que se quiere asegurar.

Vamos a comenzar, como en los casos anteriores, por los ataques que puedan provenir de Internet o de otra zona externa a la red. En este punto definiremos tres métodos de defensa, que son además cien por cien compatibles entre sí:

- *Actualizaciones y parches*: Es muy importante estar al día de las nuevas vulnerabilidades que irán surgiendo, pero es obligatorio saber cuáles estarán relacionadas con el software que utilice la red para comunicarse con Internet, para poder parchear las vulnerabilidades y evitar al máximo ser atacados. Ejemplo: Si leemos una noticia en la que se describe una vulnerabilidad en Internet Explorer v.5.0, que es la que tiene su red, quiere decir que este programa es vulnerable. Por ello habrá que parchear o actualizar el programa.
- *Firewall*: Antes de explicar su función es necesario conocer su situación, si el firewall se encuentra entre la red o entre el ordenador propietario del firewall y el exterior, ya sea Internet o una red diferente. Actualmente es muy común que el firewall venga implementado en el propio router que da acceso a Internet o, incluso en el sistema operativo que se está utilizando. Con una buena configuración estos *firewall* cumplen a la perfección su función a nivel casero. Pero a la hora de proteger una red que lo precise, explicado en el apartado anterior, habrá que invertir en un *firewall* inteligente, es decir, que sea capaz de saber además de lo que circula, cuál es su propósito; por ejemplo, si se detecta un escaneo de puertos no debe proporcionar información a ese origen.
- *Zona Desmilitarizada (DMZ)*: Aunque tiene un nombre muy potente es muy sencillo de entender, y su función es muy interesante. Vamos a tomar como ejemplo una red importante, que da servicios a través de Internet, como puede ser correo, página web, etc. Suponiendo que el pirata informático consiguiese saltarse el firewall, y no existiese una DMZ, obtendría acceso a toda la red interna. Este método entonces consiste en dividir la red interna en dos subredes (en un caso real puede subdividirse en más zonas, pero para que el ejemplo quede más claro utilizaremos dos subredes). En la primera se encontraría la red de usuarios en la cual no se encuentra ningún servicio que proporcione la empresa en su relación con el exterior (la llamaremos LAN). Y en la segunda se encontrarían todos los servicios que se proporciona a y desde Internet: correo, página web, etc. (la llamaremos DMZ). Con este sistema, las conexiones permitidas serían: desde Internet a la zona DMZ y viceversa, y desde la LAN a la zona DMZ y viceversa. No quedaría permitida la conexión desde la DMZ a la LAN. De esta forma, la zona DMZ es la que tiene los servicios externos (por lo que puede ser atacada desde el exterior); de manera que si es atacada deje al pirata informático en un callejón sin salida, porque la conexión DMZ no puede pasar a la LAN. Aún así se podrán perder algunos datos (únicamente los residentes en la DMZ), por lo que será necesario tener en cuenta este punto de vista del atacante.

Después de explicar algunas formas de defensa a ataques provenientes del exterior, continuaremos con algunos métodos de defensa a ataques desde el interior de la red.

Este tipo de ataque es, comúnmente, el que menos preocupa a los administradores de sistemas. Esto es un grave error porque estarán dando ciertos grados de libertad, en cuanto al manejo de la red se refiere, a usuarios que por sus funciones no necesitarán tenerlas. Para evitar este tipo de ataques, que serán inevitables, será necesario realizar una correcta estructura jerarquizada de la red, de forma que el usuario que sólo vaya a confeccionar nóminas no necesita conectarse a Internet, y así sucesivamente. Es un trabajo muy tedioso porque requiere conocer a todos los usuarios de la red, así como sus funciones y además saber para qué van a utilizar su terminal.

Será bueno también tener una buena política de contraseñas, tanto los administradores como los usuarios. Además habrá que efectuar la encriptación de la información y las comunicaciones, para que sólo sea accedida por los usuarios indicados. Y también es más que recomendable realizar frecuentes copias de seguridad, algo que se considera siempre necesario. Las copias de seguridad serán las que, en caso de perdida de datos, permitirán que se pueda reestablecer el sistema actual.

4.1. Criptografía

Para finalizar este punto, explicaremos en qué consisten y qué son los algoritmos de cifrado (o de criptografía). Como una primera definición, según la R.A.E., criptografía es el arte de escribir con clave secreta o de un modo enigmático. Otra definición, según la enciclopedia Wikipedia (http://es.wikipedia.org), indica que la criptografía es el arte o ciencia de cifrar y descifrar información utilizando técnicas matemáticas que hagan posible el intercambio de mensajes de manera que sólo puedan ser leídos por las personas a quienes van dirigidos.

La acción de cifrar información consiste en modificarla o transformarla para que no pueda ser tratada. Por el contrario, la acción de descifrar devuelve la información a su estado original. Esta transformación de la información tanto al cifrar como al descifrar se realiza gracias al algoritmo de cifrado.

Ahora que el lector tiene una idea de qué es la criptografía, describiremos en qué consiste cada uno de los algoritmos de cifrado:

- *Claves simétricas:* Sin lugar a dudas, éste será el algoritmo más fácil de entender. Existe una clave o llave privada que será capaz de cifrar el texto que está en "claro", y de descifrar el texto ya "ilegible". Todo se realiza con la misma llave privada. Por ejemplo si se desea enviar una contraseña numérica de cuatro dígitos de un usuario a otro, y no se quiere que nadie la lea, los usuarios se pueden poner de acuerdo a la hora de elegir una clave. Supongamos que en este caso será mover 4 posiciones hacia delante cada cifra, es decir, al 1 le asignamos el 5, al 2 el 6 y así sucesivamente, cuando se llegue a 9 se continuara con el 0, entones al 6 le asignamos el 0, al 7 el 1, etc. Esta maniobra se realizará a la hora de cifrar. Sin embargo, para descifrar habrá que mover 4 posiciones hacia atrás.

  7342 — cifrado —> 1786 — descifrado —> 7342

  Esta técnica se puede aplicar de igual manera al abecedario para cifrar de manera sencilla los textos.

- *Claves asimétricas:* En estos algoritmos se basan los sistemas de criptografía modernos. En este caso cada usuario tendrá dos claves, que se denominan llave pública y llave privada. Estas llaves serán inversas entre sí, es decir, que una se encargará de cifrar la información, que será la llave publica y la otra se encargara de descifrar la información, que será la llave privada. Que sean inversas entre sí quiere decir que no se podrá cifrar y descifrar un mismo mensaje con la misma llave, ya sea la publica o la privada. La llave pública será la que el usuario-propietario entregará al resto de los usuarios para que le puedan enviar la información cifrada, y el usuario-propietario usará la llave privada para descifrar los mensajes.

Es lógico pensar que con el sistema asimétrico el usuario-propietario entregará la llave pública a un grupo de personas conocidas, o círculo de confianza. Si por cualquier motivo la llave saliese de este círculo, la persona que tuviese la llave podrá enviar mensajes cifrados al usuario-propietario haciéndose pasar por alguien del círculo, lo que pondrá en peligro el traspaso seguro de la información.

Para solucionar este problema se adjuntará la firma digital con la información enviada. Para hacerlo menos lioso, lo explicaremos a partir de un ejemplo. Suponemos que el consumidor desea realizar un pedido y que el intercambio de información se realizará entre el consumidor y el productor. En primer lugar debe haber un contacto entre ellos en el que cada uno entregará al otro su llave pública, de manera que se puedan enviar información cifrada. Cuando el consumidor realice el pedido antes de cifrar el mensaje con la llave pública del productor, lo firmará con su llave privada, y a continuación lo cifrará. Cuando el productor reciba el mensaje cifrado, lo descifrará con su llave privada y, a continuación, con la llave pública del consumidor verificará la autenticidad de la firma digital. Gracias a esto sabrá quien realiza el pedido.

Para finalizar, diremos que actualmente se pueden ver referidos los procesos de cifrar y descifrar como encriptar y desencriptar, aunque aún no es aceptado por la R.A.E., por lo que todavía no tienen una definición oficial.

5. Gestionando el correo electrónico

Cada vez es más común el uso del correo electrónico como medio de comunicación, pero la bandeja de correo se vuelve cada vez más peligrosa por el afán de los atacantes de perjudicar al mayor número de usuarios posible.

Es muy común realizar la siguiente clasificación a los distintos e-mails. Por un lado estará *Correo deseado* y por otro *Correo no deseado*. El primero se refiere a e-mails en los que el remitente es conocido por el destinatario, y el segundo grupo mencionado que por desgracia puede equivaler al 80% de los e-mails enviados en Internet, son en los que el destinatario desconoce al remitente.

Para realizar una buena gestión del correo electrónico sería necesario utilizar más de una cuenta de correo, en concreto con dos o tres serían suficientes. Dado que se van a utilizar varias cuentas, aunque sean pocas, se puede volver un poco pesada la tarea de estar abriendo distintas cuentas continuamente, por lo que el uso de un programita como podría ser el Microsoft Outlook, el Netscape Messenger o el Mozilla Thunderbird, facilitaría en gran medida el trabajo.

La primera cuenta se creará con un carácter personal o de ocio, es decir, esta cuenta se podrá proporcionar a personas conocidas por el propietario. Esta cuenta no debería de ser utilizada para rellenar formularios ni dentro ni fuera de Internet. La configuración de esta cuenta será filtrar todo el correo que no pertenezca al conjunto de usuarios conocidos por el propietario, de manera que todo ese correo se enviará directamente a la *papelera* o *correo electrónico no deseado*. De todas formas es bueno revisar la *papelera* o *correo electrónico no deseado* de vez en cuando, por si hubiera algún mensaje de interés.

Una segunda cuenta estará dedicada a todo lo que tenga que ver con información, es decir, el destinatario sabrá quién es el remitente, pero normalmente no tendrá un trato humano con él. Los diferentes usos que se podrían dar a esta cuenta serían: entregarla en la caja de ahorros, si se compra por Internet ésta debería de ser la cuenta a utilizar, para registrarse en páginas web que sean conocidas y fiables, etc.

Y como última cuenta, aunque en algunos casos no será necesario utilizarla, su uso fundamental será la de relleno, esto se refiere a que siempre que se desconfíe de quién exige una cuenta, se entregarán los datos de ésta. Por supuesto, también se utilizará esta cuenta para rellenar los múltiples formularios en los que se pide, o más bien se exige, una cuenta de correo electrónico. No debería ser necesario acceder a menudo a esta cuenta. En cuanto al mantenimiento sería el más simple, en el momento que se llene la bandeja de basura, se puede crear una cuenta nueva y olvidar la llena.

A la hora de abrir los e-mails será necesario tener en cuenta algunas medidas de seguridad; por ejemplo, sería bueno conocer el *asunto*, o mejor dicho tener una idea de que el correo recibido es correcto con el remitente, es decir, si se recibe un correo de nuestro amigo del pueblo, que no tiene ni idea de inglés y el *asunto* está en inglés, lo normal sería no abrirlo sino directamente eliminar ese correo. Otros correos que también se deberían eliminar, son los conocidos como cadenas, es decir, se recibe y se reenvía, en algunos casos el asunto comenzará *FW:* o *RE:*. Esto querrá decir que ha sido reenviado, casi siempre de una persona no conocida. Actualmente las imágenes que recibimos también pueden tener código malintencionado, que podría infectar nuestro ordenador, por lo que sería bueno configurar nuestra bandeja de modo que bloquee las imágenes.