Herramientas y tipos de ataques

Además de la penetración en un sistema, los ataques por denegación del servicio (DoS - *Denial of Service*) son muy frecuentes. Tienen como objetivo solicitar un servicio de red repetidamente hasta que este no puede responder a las solicitudes legítimas, e incluso se para. Para conseguir una mayor eficacia, puede ser que miles de máquinas ataquen simultáneamente. Se habla de denegación de servicio distribuida (DDoS - *Distributed Denial of Service*).

1. Ingeniería social

Esta técnica, llamada en inglés «social engineering», consiste en manipular a las personas para eludir los dispositivos de seguridad. Se parte de la idea de que el ser humano es el eslabón débil en el sistema de información y se aprovecha su ignorancia o credulidad.

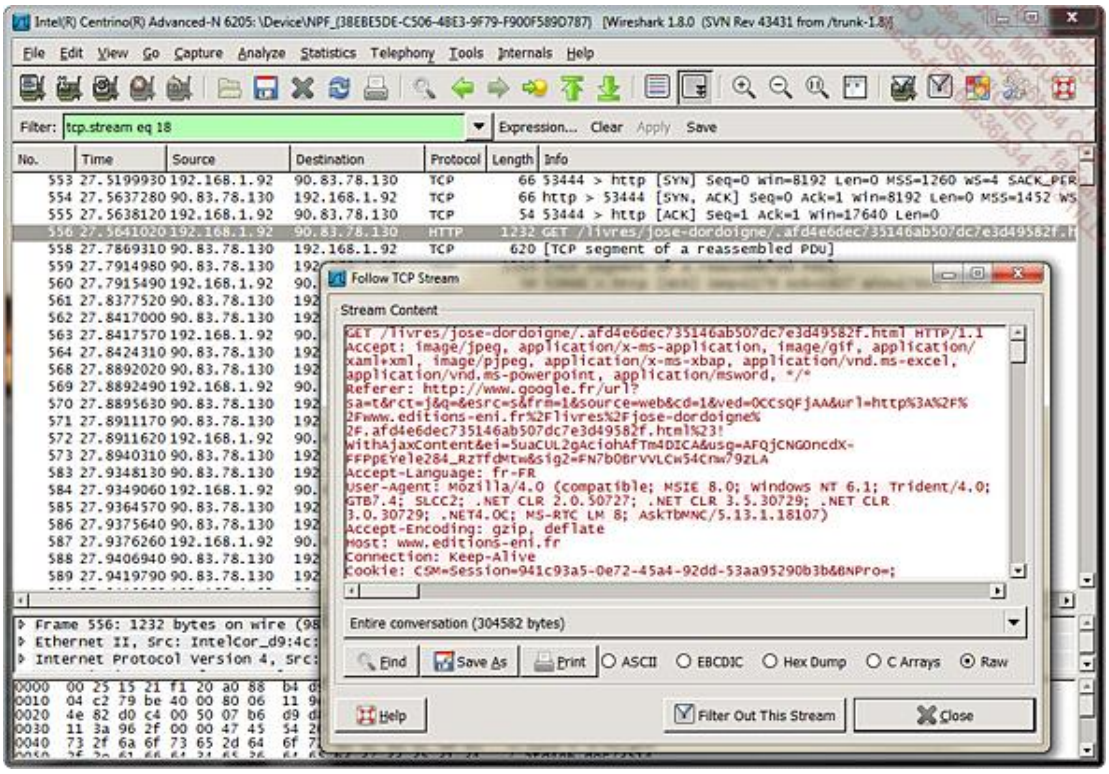
La estafa mediante el *phishing*, compuesta por las palabras inglesas *phreaking*, (piratería de líneas telefónicas) y *fishing* (pesca), es una variante muy eficaz. Este timo consiste en un envío por correo electrónico para incitar al usuario a divulgar sus datos confidenciales, como por ejemplo los bancarios. Primero se envía un correo electrónico que contiene un enlace a un sitio web falso que imita a uno real. A menudo, el objetivo es obtener el número de la tarjeta de crédito.

El sitio fraudwatchinternational.com resume las principales alertas de phishing existentes:

Alertas phishing en www.fraudwatchinternational.com

2. Escuchas de red

En el mundo del software libre, existen muchas aplicaciones. Entre ellas, WireShark ha reemplazado al célebre Ethereal. Es capaz de reconstruir una sesión TCP, es gratuito y tiene licencia GPL. La escucha de red, o *sniffing*, es sobre todo una actividad de expertos, ya que las herramientas no sustituyen a la capacidad de interpretación.



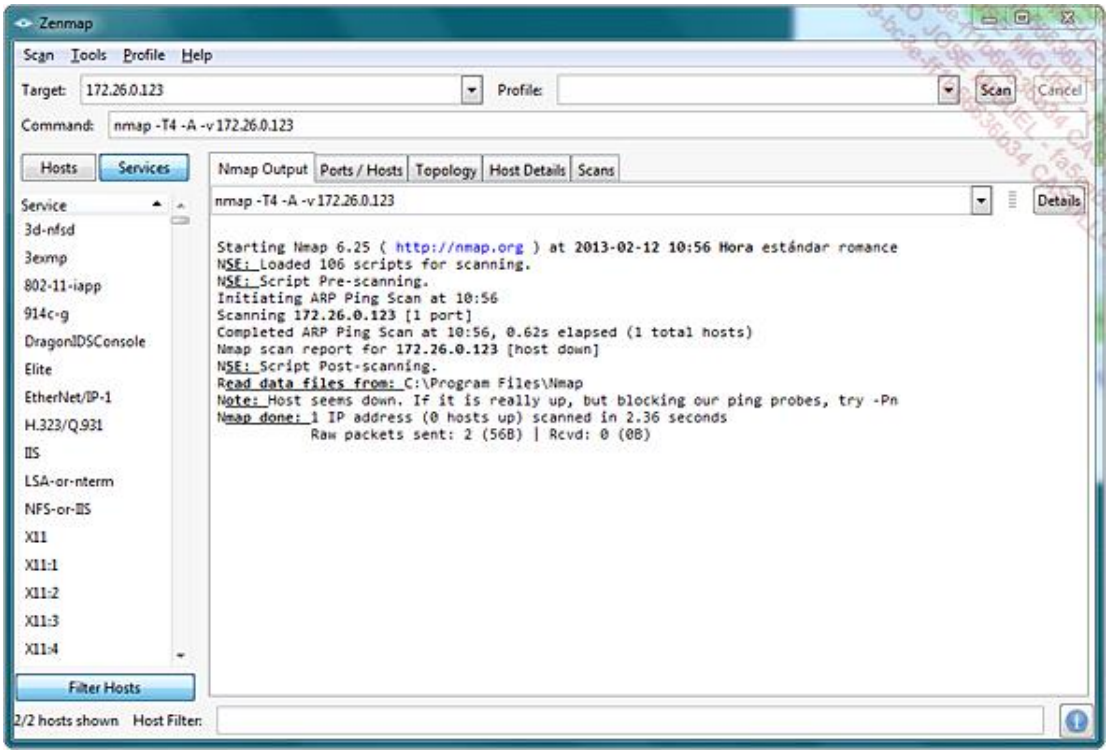
Ejemplo de seguimiento de una sesión TCP

3. Análisis de los puertos

En una red de tipo TCP/IP, un servicio escucha por un puerto, TCP o UDP, que le es propio. A cada uno corresponde un número entre 0 y 65.535. La primera serie, hasta 1024, incluye los puertos conocidos (*well known port*) de aplicaciones estándar, como:

- 80, para HTTP.
- 25, para SMTP.
- 53, para DNS.
- 21, para FTP.

El análisis de puertos consiste en recorrerlos sucesivamente. Se habla de «scan». Cuando se solicita un puerto en escucha, responde. A veces se devuelve mucha información, como se puede ver en la siguiente imagen. Este servidor Windows 2003, de prueba afortunadamente, acumula, entre otras cosas, los servicios de directorio LDAP, y las funciones de servidor HTTP y SMTP de *Internet Informations Server* (IIS). El escáner de puertos utilizado es gratuito y extremadamente fácil de utilizar.



Ejemplo de análisis con Nmap

Existen numerosos programas gratuitos disponibles en Internet, como Nmap (*Network mapper*) o SuperScan. Proponen diferentes técnicas de barrido, más o menos discretas, que permiten que la escucha sea menos activa.

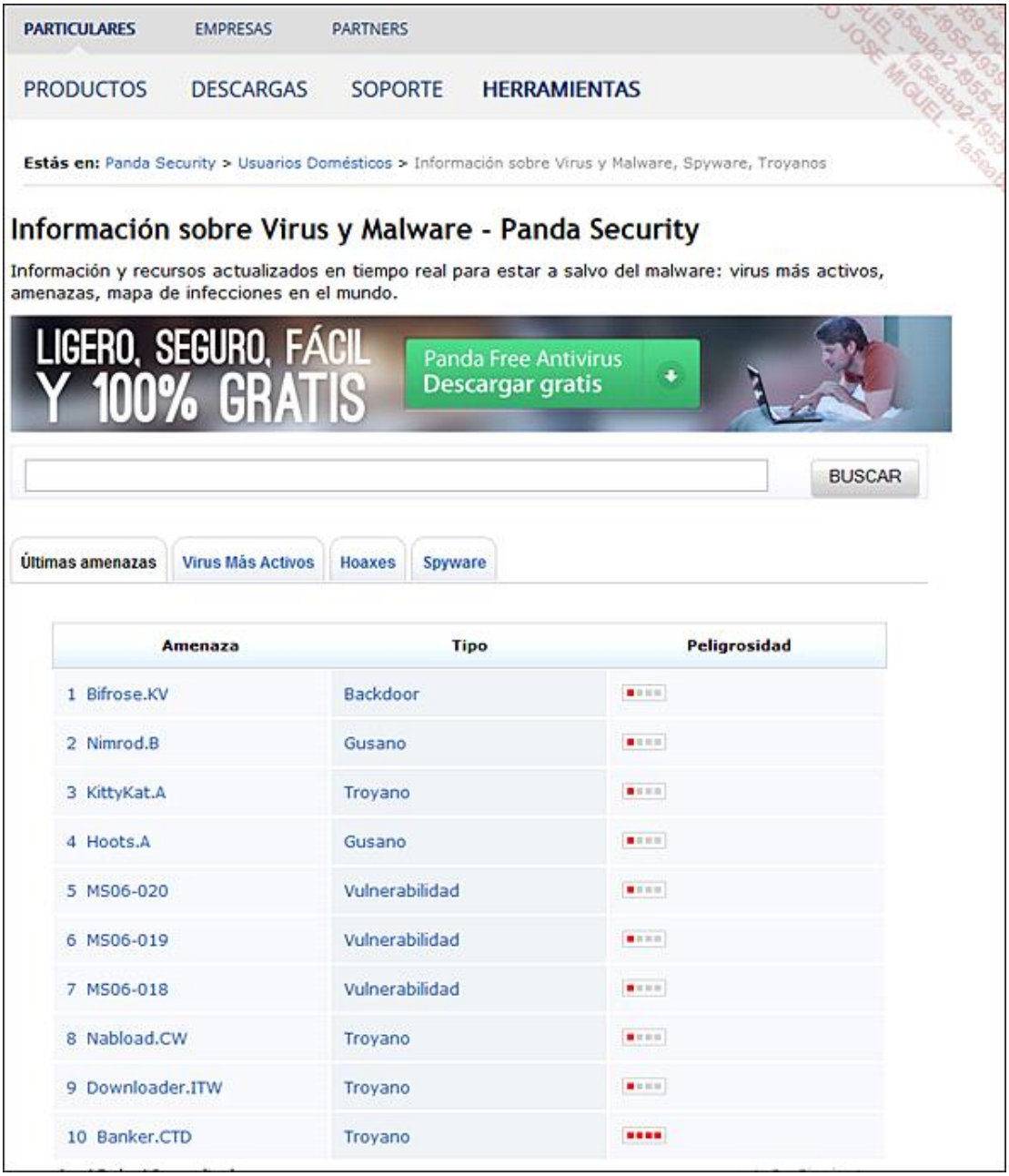
4. Códigos maliciosos

Estas aplicaciones se pueden componer de dos funciones diferentes:

- La posibilidad de reproducirse.
- La posibilidad de ataque, con una carga nociva.

A menudo se designan con el nombre genérico de virus, pero realmente se les puede diferenciar. Este nombre se define claramente en la RFC 1135, que puede encontrarse en la dirección http://www.ietf.org/rfc/rfc1135.txt.

Un virus es un bloque de código que se introduce en un huésped para propagarse, pero hay que ejecutarlo para que se active. Es diferente del gusano (*worm*), que se propaga por el correo electrónico o por fallos de la red. El gusano no contiene necesariamente una carga nociva. La bomba lógica, que se ejecuta condicionalmente, por ejemplo en una fecha determinada, es una tercera variación en este tema.



Alertas de virus y troyanos en http://www.pandasecurity.com/spain/homeusers/security-info/

Estos códigos maliciosos provocan numerosos ataques. Las principales intrusiones se dan a conocer por los medios de comunicación, lo que demuestra la importancia de sus efectos.

Los códigos maliciosos disponen de dos medios importantes de propagación. El primero es seguir utilizando la credulidad de los usuarios, mediante ingeniería social. De hecho, son muchos los que no se resisten al asunto tentador de un mail que contiene un documento adjunto recibido de un remitente desconocido.

La utilización de las vulnerabilidades de las aplicaciones es la segunda vía para su transmisión. Los sistemas operativos no son los únicos afectados. Los navegadores web Internet Explorer y Mozilla Firefox son los más vulnerables.

5. Programas furtivos

El caballo de Troya (*Trojan horse*), o troyano, podría entrar en la categoría de códigos maliciosos, pero no tiene las

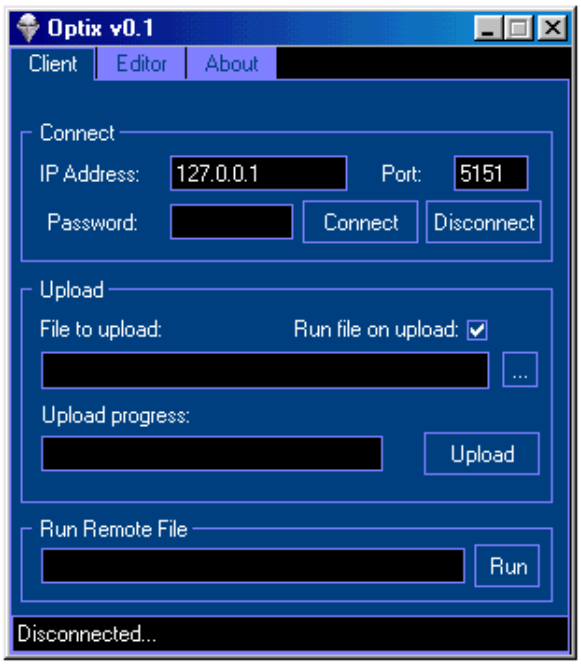
dos funciones de estos. Por el contrario, un gusano puede instalarlo en un ordenador.

Una vez instalado, este programa permanece oculto. Puede que su función sea simplemente abrir un puerto de red, o utilizarse como un servidor. Así, el pirata toma el control de la máquina.

Por ejemplo, podemos citar a Optix, que es un troyano. Permite a una persona maliciosa descargar y ejecutar archivos en el ordenador de su víctima.

Una vez que se ha instalado el programa, haciendo creer que se trata de un antivirus, u ofreciéndolo en un paquete más completo para que pase desapercibido, el programa se copia en la carpeta Windows y modifica el registro para ejecutarse automáticamente al arrancar el ordenador.

Una vez arrancado, abre un puerto y espera que un usuario remoto le pida realizar operaciones de transferencia de archivos o de ejecución remota por medio de la siguiente utilidad.



Ejemplo de una interfaz para manejar un troyano

El software espía, o *spyware*, es una subcategoría de caballo de Troya. Puede ser:

- Con un objetivo comercial, recogiendo datos para orientar campañas publicitarias.
- Informador, que recoge información y la envía discretamente.

En esta última categoría de software espía, los programas *keyloggers* se encargan de transmitir la información introducida por medio del teclado, como contraseñas o números confidenciales.

Los *bots*, diminutivo de robots, son software que permite controlar una máquina remota. Pasan a ser «zombies» y se pueden utilizar para lanzar un ataque programado, o servir de enlace para los ataques de *spam*. Un *bot* también permite desencadenar un informador durante un periodo determinado o ejecutar un caballo de Troya a petición.

En cualquier caso, este software trabaja de espaldas al usuario, pero también de los informáticos de la empresa.