

Práctica 21. Cómo Saltarse a ZoneAlarm y a otros... (Por HxC Mods-Adm)

Atravesar los un **Firewall** bien configurado no es fácil, ni siquiera para los mas experimentados, por otra parte sería del todo imposible documentar técnicas para esquivar a varios **Firewalls**, aún así, y cómo en éste capítulo hablamos de **ZoneAlarm**, he buscado, rebuscado y navegado hasta encontrar algo que pueda ganar la batalla.

La filosofía de un **Cortafuegos** es “*examinar minuciosamente*” las conexiones entrantes a la Red Local y determinar si se permite o no el acceso dependiendo de los puertos, servicios, protocolos, etc. por los que las conexiones entrantes desean comunicarse.

Para las conexiones salientes los **Firewalls** suelen ser más permisivos, de forma que “*reconocen*” los equipos de la Red Local considerados de confianza, de manera que cuando un equipo solicita un nuevo servicio o puerto al tratarse de un equipo de “*confianza*” el cortafuegos deja pasar el tráfico sin bloquearlo. ¿Vas cogiendo la idea no? Ahora sólo nos queda “*hacernos pasar*” por un equipo de confianza para el **Firewall**....

Conseguir lo explicado en el párrafo anterior es complejo y dependerá mucho del tipo de **Firewall**, la configuración aplicada y los puertos, servicios y aplicaciones “*mapeadas*” al mismo.

Imaginemos una Red detrás de un Cortafuegos y un Router en la cual los usuarios comparten su información entre sí pero sólo usan Internet para navegar, leer correo (pero desde los servidores del proveedor) y bueno, claro siempre habrá alguno que se conecte al Chat, etc, etc.

En este escenario poco podemos hacer desde fuera, NO TENEMOS servicios por los que “*pasar*” del **router** a las máquinas locales, lo único que podemos hacer es usar el correo para intentar “*algo de ingeniería social*” y conseguir las claves del router, claro, también podemos intentar explotar alguna vulnerabilidad de los dispositivos de red (**Firewall**, **Router**, **Switch**,...) que usa y probar, si tenemos suerte entonces podremos “*abrir*” el tan deseado puerto para entrar en uno de los equipos de la LAN y “*saltar*” por los demás buscando la información que deseamos.

El caso anterior bien podría ser el de un equipo doméstico conectado a Internet mediante un Router ADSL configurado en multipuesto y con filtros a todos los servicios. Difícil, difícil..., como no entremos primero al **router** para “*reconfigurarlo*...”

Otro caso bien distinto sería el de una Red con un Servidor Web instalado en la propia LAN que hace las veces de servidor interno y/o externo, en este caso existirá una conexión entre el Servidor Web y el Router para poder mostrar las páginas web o lo que sea, por supuesto el **Firewall** debería de dejar pasar las conexiones al puerto 80 de entrada y dependiendo de los servicios implementados, las conexiones salientes por el SSL 443 (puerto de transmisión segura)

Este escenario sería bien distinto, si conseguimos “*infiltrarnos*” a través del puerto 80 y “*colocar algo*” que se ponga a escuchar por el 443, el **Firewall** NI SE ENTERARÁ, puesto que todas las conexiones salientes se originan desde el propio servidor web (calificado como de confianza), siendo esas peticiones canalizadas por el puerto 443 (abierto por el **Firewall** a propósito como puerto de conexión seguro) de forma que el tráfico originado atravesará nuestro **Firewall** y llegará a nuestra máquina por el puerto 443 sin problemas.

Seguro que te estás preguntando ¿y si el 443 está cerrado? Pues claro no podrás, habrá que buscar “*otros*” abiertos. ¿y si no tiene nada abierto? Pues estamos en el primer caso, pero piensa... ¿*Para qué demonios querría una empresa montar un Servidor Web al que no puede acceder nadie? ¿Para qué quieres un server FTP en el que no se permiten la descarga de Archivos?*

Bueno puede que esas preguntas tengan una respuesta: uso exclusivo para la **Intranet**, entonces o somos parte de la LAN o nada, si no tiene servicios al exterior, pues nada los del exterior no podrán entrar nunca.

Seguro que también estarás pensando ¿Y cómo se si tiene servicios, puertos abiertos, aplicaciones, etc.?

Encontrarás las respuestas en los próximos capítulos cuando se hable del escaneado, exploración, enumeración, etc.

Las aplicaciones que aquí encontrarás pueden analizar, comprobar y desactivar alguno de los Firewalls más conocidos del mercado, prueba con **FIREWAR**, desactivará **ZoneAlarm** si lo tienes corriendo...



Como verás permite la desactivación de varios **Firewall**, no modifica los binarios de ninguno de ellos, la que hace es interponerse en el área de memoria en el que están corriendo y los bloquea.

El mayor inconveniente es que el usuario se dará cuenta y además el antivirus lo detectará, vamos que no vais a conseguir mucho a no ser que se tenga acceso local a la máquina, desactivemos el antivirus y ejecutemos el programa, demasiados factores para que se tenga éxito, pero seguro que en breve se conseguirá evitar todas éstas situaciones. Que sirva como ejemplo de las posibilidades que ofrecen estas nuevas tecnologías y de la importancia que supone estar prevenidos y con nuestras defensas actualizadas.