Hackers, el regreso a la involución

Osvaldo Callegari
Analista de Sistemas
ocalle@ar.inter.net

Desde que se crearon las "redes de redes" estuvieron vigentes las vulnerabilidades de los accesos remotos, por tal motivo, se hace indispensable aprender nuevas técnicas de defensa, que intentaremos describir de manera clara y sencilla en esta nueva sección.

El antivirus de ayer hoy es obsoleto, lo mismo que un cortafuegos (firewalls) o un código malicioso (spy ware). Es necesario buscar caminos alternativos sino cada día que pasa somos más dependientes de estos artilugios.

Introducción

"*La tecnología es la mejora constante de los productos al servicio del hombre*", es una frase que puede estar registrada o no pero es válida, ahora bien me toca hablar hoy del otro dilema que la misma presenta, todos los avances se suceden a la velocidad de la luz y no alcanzamos a vislumbrar o aprender lo actual o vigente que ya se presenta algo nuevo. Con ello ha surgido lo que podríamos llamar una sub-especie denominada hackers, que son a la postre como un tipo de guía de lo que no se debe hacer. Determinar el alcance de este fenómeno, nos genera una especie de miedo de lo que nos pueda suceder en nuestra computadora. Se observa que a la par de los acontecimientos tecnológicos están presentes en nuestras vidas como los señores dueños de lo desconocido.

Es importante evitar que este arquetipo se convierta en nuestro maestro de enseñanza y surgen inquietudes como las que se presentan en los cursos de capacitación en las exposiciones tecnológicas: *¿Quienes aprenden con estos cursos, las personas afectadas al sector o nuevos hackers contratados?*.

Acceder a una red ajena o trucos para robar información son premisas que siempre estuvieron alejadas de la ética y la honestidad.

Nos deja a la vista una realidad que ya la dijeron varios pensadores...."*se nos hizo una brecha en el conocimiento de lo que se viene*" y nos cuesta atar cabos de lo que dejamos atrás en lo técnico y en lo que llega en los próximos diez minutos. No tenemos el tiempo suficiente de analizar las cosas en su justa magnitud y permanecen aisladas de nuestra conciencia. Atado a los conocimientos de estos sujetos, se encuentran las falencias de seguridad que existen en las redes para las cuales es necesario aprender nuevas técnicas de defensa.

Un hacker que da clases, entrega solo fragmentos de conceptos, no explica todo sino dejaría de ser admirado. *¿Es una realidad qué necesitamos falsos ídolos?*.

Esta generación de "*intruders*" beneficiados por aquel modelo de las películas de "*misión imposible*" de aquel que se las sabe todas, presenta alteraciones psicológicas propias del mundo en que vivimos. Ahora bien, es que a lo mejor todos nos imaginamos ser como él o al menos forma parte de nuestro subconsciente actual.

No perdamos el sentido común, apostemos a las organizaciones que establecen los estándares de la información, colaboremos con nuestro esfuerzo para aumentar la cultura de lo que se puede hacer bien y exijamos a los productores de software reglas claras de seguridad.

Claves e información para estar más protegido.

Areas vulnerables en las configuraciones de los sistemas de Windows®

Las áreas expuestas en estos sistemas están siendo explotados por una nueva familia de bots y de gusanos. Estas debilidades pueden agruparse en las siguientes categorías:

Palabras claves vulnerables en cuentas de Windows® o accesos compartidos en redes.

En los últimos 10 años el esquema de autenticación en *Windows*® ha sido el problema más importante en el ranking de las vulnerabilidades.

LAN Manager® (LM®) ha reemplazado sus fallas de seguridad con varias versiones de autenticación NTLM.

Windows® posee su propio nivel de autenticación y seguridad con mejor aplicación que LM®.

Continúa en página 136

Viene de página 132

Cualquier palabra clave que pueda ser considerada como robusta puede ser descifrada en un corto período de tiempo. A través de lo que se conoce como *fuerza bruta*, un hacker puede resolverlo en una semana.

Las claves conocidas por defecto son las primeras que se investigan desde un diccionario de palabras estandarizado.

Herramientas como *THC Hydra*® pueden ser usadas para descifrar remotamente claves de usuarios.

LophtCrack® y *John the Ripper*® son los programas más conocidos en apertura de claves.

Muchas familias de gusanos o bot zombies como *Gaobot*, *Phabot* y *Agobot* atacan las redes que tienen unidades compartidas con claves sencillas.

Estos pequeños programas transportan una lista de claves y realizan la fuerza bruta inicial para tratar de vulnerar el sistema y poder acceder.

Configuraciones por defecto en servidores.

Cuando instalamos *Microsoft*® *Data Engine*® (MSDE) o *SQL Server*®, la clave por defecto del administrador es "*sa*" y tiene por defecto un espacio en blanco como palabra clave. Este espacio en blanco es vulnerable y permite operar a gusanos, como es el caso de *Voyager Alpha Force*, *Sql Spida* y *Cblade*.

IIS Servers® tiene por defecto una configuración que es vulnerable a los ataques. Instalaciones creadas por un usuario anónimo del tipo "*IUSR_computername*" permiten el acceso remoto de gusanos.

Los servicios FTP, NNTP o SMTP deben ser deshabilitados para evitar males mayores.

Sistemas operativos afectados

Windows NT®, Windows 2000®, Windows XP® y Windows 2003®.

Como protegerse contra esas vulnerabilidades

- Utilice políticas de claves muy complejas o difíciles, con doce caracteres o más si es posible.
- Use herramientas como *LophtCrack*® o *John The Ripper*® para auditar cuentas con password débiles.
- Prevenga a *Windows*® que el hash de *Lan Manager*® se almacene en el directorio activo o en la base Sam.
- Link para leer soporte *(en inglés)*: http://support.microsoft.com/default.aspx?scid=KB;EN-US;q299656&
- Link *(en español)* útil para bloquear el registro en la rama compartir las redes. Modifique el registro según este link de soporte http://support.microsoft.com/kb/q246261
- Modifique las configuraciones por defecto de los servidores *IIServers*® y *MS-SQL*®

Los nombres o marcas antes mencionados son marcas y nombres registrados por sus propios autores o empresas, los productos que se sugieren utilizar son bajo exclusiva responsabilidad de quien los utilice.

Fuentes de vulnerabilidades SANS Institute (www.sans.org).