Intrusión de hackers en tu sistema Mambo/Joomla

Cómo evitar hackeos en sitios Mambo/Joomla

Por favor no utilices este recurso para hacer daño a quienes trabajan y dedican tiempo y esfuerzo en proyectos o sitios web. Utiliza este material para aprender más sobre seguridad y protegerte.

La mejor forma de evitar hackeos e intrusiones es conociendo cómo actúan los hackers y qué acciones ejecutan para defasar, apropiarse o estropear sitios web ajenos. Voy a distinguir entre dos grupos: hackers - crackers, y pseudo-hackers, *lamers* y *script kiddies*

Los primeros son personas que buscan vulnerabilidades para informar y proteger posibles víctimas, o contribuir al arreglo de los bugs / vulnerabilidades de seguridad. Los segundos son los típicos pelotudos con la autoestima muy baja que en muchos casos no saben ni cómo se ejecuta un comando shell pero sin embargo se las ingenian para buscar en foros o sitios de hackers la manera de hacer daño a los demás y estropear el trabajo de otros simplemente para alimentar su triste ego (vean un ejemplo: **http://foro.elhacker.net/index.php/topic,75216.0.html**). En el caso particular que me toca a mi, el hacker que se introdujo en los sistemas de dos de mis clientes, dejaba mensajes de amor a su novia, para demostrarle a ella cuán valiente es, y de las osadías de que es capaz de hacer. Este tipo de personas, y el daño que me han provocado profesionalmente hace unos días atrás, me lleva a escribir este artículo sobre seguridad para Mambo/Joomla.

10 consejos para evitar la intrusión de hackers en Mambo/Joomla:

1. Descarga Mambo/Joomla sola y únicamente de los sitios oficiales: **www.joomla.org** y **http://mamboforge.net**
2. No instales componentes o módulos con poca fama, o sin soporte. El core del sistema puede ser impenetrable pero si instalas algún addon vulnerable, vuelves vulnerable todo.
3. Haz back up periodicamente tanto de la base de datos como de los archivos
4. Manten actualizado el sistema con la última versión. Al momento de descubrirse una vulnerabilidad es muy corto el tiempo en el cual se desarrolla un parche o arreglo para la misma. Si tienes el sistema actualizado y/o parcheado con los últimos patches disminuyes notablemente la probabilidad de que te hackeen el site.
5. Utiliza **.htaccess** para controlar los accesos, y para proteger con contraseña el directorio **/administrator/** (HTTP Authentication)
6. Utiliza servicios online de detección y alertas contra hackers
7. Investiga y conoce muy bien el funcionamiento de usuarios y permisos en sistemas Unix/Linux. No otorgues permisos innecesarios de escritura a cualquier archivo o directorio. Haz no escribible el archivo **configuration.php** luego de hacer cambios.
8. Utiliza componentes SEFs avanzados para enmascarar las verdaderas URLs de Mambo/Joomla
9. Evita utilizar nombres o contraseñas "fáciles" de adivinar o de vulnerar mediante "fuerza bruta". Nunca utilices las mismas contraseñas y usuarios para FTP y para las bases de datos (esto último es muy peligroso). Evita utilizar "admin" y "admin" para el ingreso al administrador del sistema.
10. Contrata hostings profesionales, donde conocen a fondo y dan mucha importancia al tema de la seguridad. La configuración de PHP es vital aquí: Registros globales desactivados, modo seguro, activación de comillas mágicas GPC, ejecución de shell deshabilitado para PHP, etc.
11. Deshabilita el reporte de errores de PHP, hasta cuando necesites identificar problemas únicamente.

Explotando vulnerabilidades

Las vulnerabilidades son agujeros de seguridad por donde el hacker puede introducirse de alguna manera en el sistema y luego utilizar estas vulnerabilidades mismas para propósitos con malas intenciones. Aquel medio o herramienta que le permite al hacker introducirse clandestinamente en un sitio web o servidor se le llama "EXPLOIT". Esto puede ir desde sencillas ejecuciones de códigos por URL hasta la programación de complejos scripts en PHP utilizados remotamente para vulnerar sitios Joomla/Mambo

Algunos términos relacionados:

XSS (Cross Site Scripting) - este tipo de vulnerabilidad es consecuencia de errores en el filtrado de las entradas de datos en aplicaciones web.
Remote File Inclusion - Técnica de hackeo avanzado mediante la cual se incluye scripts con código PHP/Perl (sin ejecutar) en servidores remotos (utilizados por los hackers), los cuales ejecutan acciones arbitrarias en el servidor de la víctima.
Backdoor - script programado en PHP/Perl que le permite al hacker (luego de que ha conseguido subirlo al servidor de la víctima), subir nuevos archivos, forzar permisos, recorrer directorios, editar o borrar archivos, ejecutar sentencias shell o sql, etc. Un back-door es una especie de mini "panel de control" de archivos en el servidor (algo muy peligroso).

Vulnerabilidades en el historial de Mambo

Algunos ejemplos de vulnerabilidades en las primeras versiones de Mambo.

Cerrar ventana