

Protección de nuestros sistemas contra chicos malos

# LECCIONES DE KARATE KID

Vamos a mostrar cómo las lecciones del Señor Miyagi que aprendimos en la película "Karate Kid" de los años 80 pueden aplicarse para asegurar nuestros sistemas. **POR KURT SEIFRIED**

Últimamente vengo observando una tendencia preocupante, y cuando digo últimamente me refiero a los últimos cinco años. El estado de seguridad de Linux no parece mejorar. Esto no significa que no se hayan producido algunos importantes avances tecnológicos: SELinux es ahora común en muchas distros y muchos proveedores se encuentran en la actualidad distribuyendo servicios deshabilitados por defecto y cortafuegos habilitados también por defecto. Pero sobre todo, encuentro que el número de bugs y sus diferentes tipos no han cambiado en realidad demasiado o, incluso, la cosa está empeorando.

En el 2007, Red Hat publicó notificaciones de seguridad sumando un total de 371 identificaciones CVE, cada una de

los cuales representando al menos un problema de seguridad específico y singular y, a veces, más de uno. Mandriva va un poco por detrás, pero no demasiado lejos, con 350. Lo que es ya mucho más preocupante son las 444 de Debian y las 539 de Gentoo.

## Pero No Lo Escribimos

La primera cosa que debemos recordar es que la mayoría del software distribuido por los proveedores de Linux no está escrito por ellos. La mayor parte de las herramientas del espacio de usuario en un sistema Linux han sido reempaquetadas y quizás ajustadas por el proveedor, pero aparte de retroportar los parches de seguridad, la mayoría de los proveedores le hacen muy poco al software. Esto conduce a algunos problemas, tales como

permisos de ficheros débiles. Un ejemplo perfecto es

CVE-2002-0849. En el 2002 encontré que el software iSCSI principal para Linux, que fue producido por Cisco, incluía la contraseña CHAP (Challenge Handshake Authentication Protocol) en un fichero de lectura global: `/etc/iscsi.conf`. Con esta contraseña, un atacante podría acceder a los datos en un iSCSI como el servidor, evitando en gran parte los permisos de ficheros u otros mecanismos de seguridad.

Así que informé debidamente, Cisco lo resolvió y el mundo siguió girando.

Ahora estamos en el 2008, y si miramos una lista de vulnerabilidades de seguridad, encontraremos CVE-2007-5827: "iSCSI Enterprise Target (*iscsitarget*) 0.4.15 usa permisos débiles para `/etc/ietd.conf`, lo que permite a usuarios locales obtener contraseñas."

¿¿¿¿¿Cómo??!!?

Si echamos un vistazo a nuestro directorio `/etc` y comprobamos los archivos que contienen contraseñas, encontraremos muchos de ellos en poco tiempo (véase la Tabla 1).

Todo esto se encontró simplemente ejecutando como usuario normal

```
grep -i password /etc/*
grep -i password /etc/*/*
```

Véase la Figura 1.

Encontrar esta clase de problemas – y solucionarlos – debería ser trivial para la mayoría de los proveedores. Es improbable que se vea afectada la funcionalidad del sistema, porque la mayoría de los servicios de red se inician como root, leen sus archivos de configuración y luego renuncian a los privilegios.

Generalmente, todo cuanto necesitamos es eliminar los permisos de lectura

globales de esos ficheros y queda resuelto el problema. Debería ser suficiente añadir una simple línea `%post` al instalar el script en un RPM, por ejemplo, ejecutar `chown o-r [nombre fichero]`.

Sin embargo, los proveedores han decidido no hacerlo, y en gran parte ignoran el problema o abiertamente se niegan a solucionarlo. Así que, ¿qué nos enseña Karate Kid [1]?

Como Karate Kid, nuestros administradores de sistemas tienen que aprender karate (sistema de seguridad) o los chicos malos nos saltarán en un callejón y usarán nuestras cabezas y riñones como una piñata (haciéndose root en el sistema y poseyéndolo). Muchos administradores han hecho enemigos sin darse cuenta: activistas, compañías competidoras, criminales y otros podrían hacerse con el poder de nuestro servidor felizmente por cualquier número de razones, incluyendo almacenamiento de información robada o material ilegal, para descargar datos de clientes, etc.

A diferencia de Karate Kid, la mayoría de nosotros no tiene un Mr. Miyagi para ayudarnos a derrotar a los demoníacos estudiantes del Cobra Kai Dojo. Además, en esta batalla los chicos malos pelean sucio. Realmente sucio.

### Lecciones Aprendidas

1. Una tregua es inverosímil: En Karate Kid, los buenos solicitaron una tregua mientras Ralph Macchio estaba entrenando. Lo más probable es que proponiendo una página web o un correo electrónico los spammers regresen solicitando una tregua mientras aprendemos cómo compilar sistemas de seguridad y a

administrarlos sin incidentes no funcione. Sin embargo, podemos darnos a nosotros mismos un pequeño respiro y limitar la cantidad de tiempo que gastamos ocupándonos de peticiones de usuarios de manera que podemos centrarnos en mejorar nuestros sistemas, lo cual puede acabar siendo muy positivo.

2. Encontrar un mentor: Habitualmente, encontrar un mentor es una buena idea. He pasado bastante tiempo (re)inventando la rueda para saber que a veces gastar dinero en un libro es la opción más rápida y sencilla. Aunque tener a alguien que pueda enseñarnos y responder a nuestras preguntas es una verdadera bicoca.

Algunos grupos y organizaciones, tales como ISC2, ISACA y ISECO, fomentan la seguridad de la información. Muchos poseen programas para fomentar el aprendizaje y la educación, y lo más probable es que podríamos encontrar a alguien que estuviera dispuesto a ayudarnos.

3. Aprender a luchar cuando nos hieren: Cuando te enfrentes a un atacante vas a estar impedido por leyes y regulaciones, y el chico malo no va a jugar limpio. Inundará alegremente nuestros buzones con miles de correos y, mientras nos ocupamos de éstos, entrará en nuestro servidor web y cogerá todos los registros de los clientes. Debemos tener un

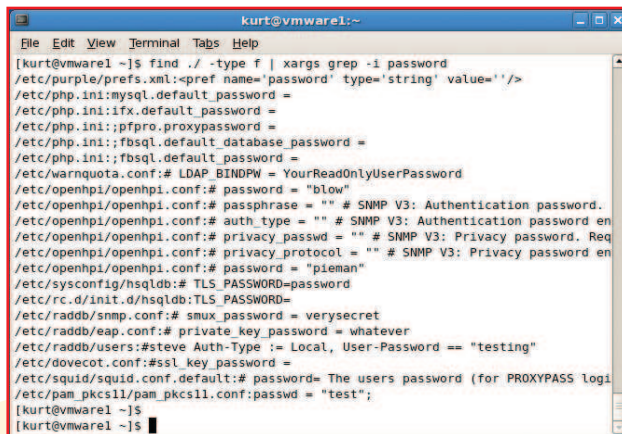


Figura 1: Encontrarás bastantes archivos que contienen contraseñas.

plan de contingencia de manera que estemos preparados si nuestro sistema se ve comprometido.

4. Si es necesario, patearemos a nuestro oponente en la cara: A diferencia de Karate Kid, nosotros no vamos a ganar puntos por el estilo cuando tratamos con atacantes. Tratar con atacantes de manera rápida y eficiente nos permite movernos al problema siguiente. A menudo he visto gente intentando encontrar la “mejor” solución a un problema de seguridad, en vez de buscar simplemente una “buena” solución. Ninguna solución será perfecta: los sistemas y redes cambian, se encontrarán nuevos ataques y se descubrirán nuevas defensas. Aprender a despachar a los atacantes rápidamente dará más tiempo para pasarlo compilando sistemas mejores, y aprender a compilar mejores sistemas rápidamente nos dará más tiempo para centrarnos en la prevención.

### Conclusión

Si queremos un sistema seguro hay que trabajar en pos de él, algunos proveedores nos lo proporcionan listo para ser usado.

Además, probablemente tengamos que trabajar para encontrar el tiempo y la energía necesarios para gastarlos en el entrenamiento y la creación de sistemas y redes mejores. A pesar de que esto no siempre es fácil de hacer, cualquier otra alternativa simplemente mantendrá el status quo y prolongará el sufrimiento. ■

Programa	Fichero	Variable Contraseña
Dovecot	/etc/dovecot.conf	ssl_key_password
FreeRADIUS	/etc/raddb/eap.conf	private_key_password
FreeRADIUS	/etc/raddb/mssql.conf	password
FreeRADIUS	/etc/raddb/postgresql.conf	password
FreeRADIUS	/etc/raddb/radiusd.conf	multiple passwords
FreeRADIUS	/etc/raddb/snmp.conf	smux_password
FreeRADIUS	/etc/raddb/sql.conf	password
FreeRADIUS	/etc/raddb/users	user-Password
HSQIDB	/etc/init.d/hsqldb	TIS_PASSWORD
libpurple	/etc/purple/prefs.xml	password string
OpenHPI	/etc/openhpi/openhpi.conf	MuTIPIE
pam_pkcs11	/etc/pam_pkcs11/pam_pkcs11.conf	ldap passwd
quota	/etc/warnquota.conf	IDAP_BINDPW
Squid	/etc/squid/squid.conf	MuTIPIE
Tomcat	/etc/tomcat/server.xml	connectionPassword

**RECURSOS**

[1] Karate Kid: [http://en.wikipedia.org/wiki/The\\_Karate\\_Kid](http://en.wikipedia.org/wiki/The_Karate_Kid)