

En busca de síntomas de un ataque

# EL GATO Y EL RATÓN

Si creemos que nuestros sistemas son tan complicados como para preocuparnos de un atacante, es hora de pensárselo dos veces. Los intrusos de hoy día acechan todo tipo de víctimas. **POR JOE CASAD**

¿Tenemos las puertas cerradas? ¿Está nuestra información a salvo? En los comienzos, los primeros atacantes de redes sólo jugaban con los sistemas. Se introducían simplemente para demostrar que podían hacerlo, como un reto intelectual o tal vez para demostrar valentía.

Sin embargo, los tiempos cambian, y si nos preocupa la seguridad, lo mejor es adaptarse a los cambios. Los sistemas actuales albergan información crítica con valor económico: números de tarjetas de crédito, historiales médicos, direcciones de email, etc. Los cibercriminales emplean sofisticadas técnicas que llevan a ordenadores normales y corrientes a que reenvíen spam y a que lancen ataques de denegación de servicio. ¿Y los vándalos adolescentes? Aún tenemos que ocuparnos de eso. Para estar por delante de ellos, tenemos que saber lo que ellos saben, por lo que necesitamos conocer qué aspecto tienen sus ataques. En el tema de portada de este mes, dedicado a la detección de intrusos, os mostramos qué debemos buscar.

Un intruso que comprometa la seguridad de una red siempre querrá crear una puerta escondida para volver a entrar. Estas entradas secretas, conocidas como puertas traseras, pueden disfrazarse de distintas maneras. Comenzamos el tema de portada con un vistazo a algunas de las técnicas de puerta trasera más comunes. Os mostramos también cómo buscar señales de un ataque usando la versátil herramienta de administración Isof. A continuación analizaremos iWatch, una prometedora herramienta que usa la interfaz Inotify del kernel de Linux para monitorizar nuestros directorios y enviar avisos de accesos no autorizados en tiempo real. En nuestro último artículo presentamos BackTrack, una distribución live de Linux con una formidable colección de herramientas para simular un ataque de red.

Si queremos aprender a pensar como un intruso, o incluso si sólo estamos buscando algunas técnicas sencillas para nuestra defensa, siga leyendo para obtener experto consejo en cuanto a detección de intrusos. Esperamos que disfrute del tema de portada de este mes de Linux Magazine. ■



## TEMA DE PORTADA

Puertas Traseras.....	12
Detección de intrusos con Isof.....	18
iWatch.....	23
Backtrack.....	25
ARP Attack.....	29