"Suficiente con la estupidez de la seguridad en GNU/Linux®"

Cada pocas semanas, aparece una historia de seguridad que dice lo inseguro que es GNU/Linux®. Sólo hay un problema con la mayoría de ellas: son noticias falsas. ***El verdadero problema son los administradores de sistemas incompetentes.***

Traducción del artículo publicado por Steven J. Vaughan-Nichols donde trata el tema del "amarillismo informático", que también existe. Traductor Jimmy Olano.

Como todos los sistemas operativos, GNU/Linux® no es perfectamente seguro. Nada lo es. Como el gurú de la seguridad, Bruce Schneier bien lo dijo, "La seguridad es un proceso, no un producto". Es sólo que, en general, GNU/Linux® es más seguro que sus competidores. No podríamos decir eso por los recientes titulares que insisten en lo inseguro que es GNU/Linux®. Pero, si se mira más de cerca, se encontrará que la mayoría - no todas, pero la mayoría - de estas historias son falsas.

Por ejemplo, la vulnerabilidad *Boothole* sonaba francamente aterrador. ¡Puede obtener acceso de usuario raíz o *root* en cualquier sistema! **¡Oh no!** Mirad de nuevo. El grupo que lo descubrió dice que un atacante necesita acceso de administrador para que su treta haga el trabajo sucio.

Amigos, si alguien más que ustedes tiene acceso como usuario raíz a vuestro sistema, ya tenéis un verdadero problema. ¿Recuerdan lo que os dije acerca que GNU/Linux® no era perfecto? **Aquí hay un ejemplo.** El problema inicial era real, aunque solo muy peligroso para un sistema ya *crackeado* (comprometido o violentado). Pero varias distribuciones de GNU/Linux® hicieron una chapuza en el primer intento de arreglo, todo para que al final sus sistemas en buen estado no pudieran iniciar. ***Eso es malo.***

> "Fue peor el remedio que la enfermedad"

> Refrán popular agregado a propósito por el traductor.

A veces, arreglar algo rápidamente puede empeorar las cosas y eso fue lo que sucedió aquí.

En otro caso reciente, dos agencias gubernamentales de los Estados Unidos de América, el Buró Federal de Investigaciones (FBI) y la Agencia de Seguridad Nacional (NSA) emitieron una alerta de seguridad sobre el *malware* ruso llamado Drovorub o Drovorun. Este programa utiliza módulos del núcleo de Linux sin firmas digitales para atacar sistemas. Es cierto que, como lo dijo el Director de Tecnología (CTO) de la empresa de seguridad McAfee, Steve Grobman: "Los Estados Unidos son un entorno rico en objetivos para potenciales ciberataques", pero *¿la programación de GNU/Linux® está a cargo de alguien con una pista o idea acerca del peligro en ello?*

No lo creo.

En primer lugar, este *malware* sólo puede funcionar en distribuciones de GNU/Linux® que ejecuten el núcleo Linux® 3.6.x o anterior. *¿Adivinen qué?* El núcleo de Linux 3.6 fue publicado hace ocho años.

Suponiendo que si ustedes todavía están utilizando el obsoleto Red Hat Enterprise Linux (RHEL) versión 6, pues tendrán que preocuparse. Por supuesto, la solución para la firma de módulos del kernel de Linux® ha estado disponible para RHEL 6 desde el año 2012. Además, la mayoría de la gente está usando distribuciones de GNU/Linux® que son algo más nuevas que eso.

De hecho, hagamos una pequeña lista de las principales distribuciones de GNU/Linux® actualmente usadas:

- CentOS / RHEL 7 comenzó con el kernel 3.10.
- Debian 8 comenzó con el kernel 3.16.
- Ubuntu 13.04 comenzó con el kernel 3.8.
- SUSE Linux 12.3 se inició con el kernel 3.7.10.

Todas estas distribuciones, con años de antigüedad, desde que comenzaron ya eran inmunes a este ataque. Todas las versiones recientes de Linux son invulnerables a este *malware*.

Pero, ¡esperen! ¡Hay más! Y esta es la parte que realmente me molesta. Digamos que todavía

están ustedes ejecutando el ya sin soporte técnico Ubuntu 12.04, el cual es, en teoría, vulnerable. **¿Y qué?** Como señala el equipo de seguridad de Red Hat, "los atacantes [deben] obtener privilegios de usuario raíz o *root* usando otra vulnerabilidad antes de una instalación exitosa".

Una vez más para que GNU/Linux® se vea comprometido -para que su sistema reciba una dosis de Drovorub- ya dicho sistema tenía que estar completamente comprometido. **Si un atacante ya tiene acceso como usuario raíz, usted ya está totalmente arruinado.**

Sí, aquí hay un problema de seguridad, pero no es técnico. En el negocio de soporte técnico, nos gusta llamar a este tipo de incidentes de esta manera: "El Problema Está Entre el Teclado y la Silla (EPEEETYLS)" (en inglés "*Problem Exists Between Keyboard And Chair*" o PEBKAC). Así que sí, si tienen un completo idiota como administrador de sistema, tienen un verdadero problema, *pero no pueden culpar a GNU/Linux® por ello.*

Veamos otro ejemplo: Doki, un nuevo troyano (puerta trasera). Esta vez, aunque muchos lo describen como un problema de GNU/Linux®, no lo es. Sólo puede atacar con éxito a los sistemas GNU/Linux® cuando quienquiera que haya configurado los contenedores Docker haya expuesto la API de la Interfaz de Administración al Internet.

Eso es tonto, pero aún es más tonto para que caigan con este troyano: el cortafuegos de vuestro servidor debe estar configurado para tener abierto el puerto 2375. **Aquí hay una lección de seguridad de redes, primera clase, la 101: bloquear todos los puertos excepto los que debes tener abiertos.** Y, ya que están en eso, configuren vuestro muro de fuego para que rechace todas las conexiones entrantes que no respondan a las solicitudes salientes. Si vuestro administrador aún no lo ha hecho, es un incompetente.

Finalmente, consideremos el problema reciente del comando **sudo**. Esta vulnerabilidad de seguridad de **sudo** era verdadero, desde entonces ha sido solucionada, pero requiere, nuevamente, un caso de EPEEETYLS (PEBKAC) para que funcione. En este caso, tendría que estar mal configurado el comando **sudo** de tal manera que cualquier usuario pudiera ejecutar dicho programa. **Una vez más, si usted ya tiene un sistema inseguro, esto solo puede ir a peor.**

Aquí hay un tema común. Los problemas a menudo no están en GNU/Linux®. Los problemas están en administradores totalmente incompetentes. Y cuando digo "totalmente incompetente", eso es exactamente lo que quiero decir. No estamos hablando de pequeños errores sutiles que cualquiera pueda cometer. Estamos hablando de errores fundamentales.

Ya sea que esté ejecutando Windows Server®, GNU/Linux®, NetBSD®, lo que sea en sus sistemas de misión crítica, si falla completamente en establecer las normas comunes de seguridad, no importa cuán "seguro" sea su sistema operativo. Es como dejar las llaves de su automóvil en el encendido y con las puertas sin seguro, su sistema será *crackeado*, su auto será robado.

Entonces, basta de culpar a GNU/Linux®. Culpemos al verdadero problema: la simple incompetencia del administrador del sistema.

Traducción del artículo publicado por Steven J. Vaughan-Nichols donde trata el tema del "amarillismo informático", que también existe. Traductor Jimmy Olano.
