Por qué Linux es más seguro que Windows

Hace unos días Google anunció que sus empleados dejarían de utilizar Windows, alegando que Windows tenía algunos huecos de seguridad importantes. Como ya vimos, si bien esto es cierto, puede tratarse de una estrategia comercial.

Sin embargo, esta decisión me dejó pensando: ¿qué hace más seguro a Linux? Cualquier usuario de Linux se da cuenta que es mucho más seguro... se siente más seguro que Windows. Pero, ¿cómo explicar esa "sensación"?

Este post es el fruto de varias horas de reflexión y búsqueda en internet. Si todavía usás Windows y querés saber por qué Linux es más seguro o si sos un usuario de Linux que disfruta de sus mieles y querés saber qué hace de Linux un mejor sistema en materia de seguridad, te recomiendo que leas este post detenidamente. Es largo pero vale la pena.

Introducción: ¿qué es la seguridad?

Mucha gente cree que es correcto decir que un producto es seguro, así por ejemplo, Windows es más seguro que Linux, Firefox más seguro que IE, etc. Esto es parcialmente cierto. En realidad, la seguridad no es un producto, algo que viene ya armadito y para llevar. Se trata, más bien, de un proceso en la que el usuario juega un rol central. En otras palabras, la seguridad es un estado que debe ser mantenido activamente a través de una interacción adecuada y responsable entre el usuario y el software y/o sistema operativo instalado.

Ningún software o sistema operativo es capaz de aportar ningún tipo de seguridad si el administrador pone claves tontas como "123", o si no toma los recaudos del caso. Dicho esto, sí es cierto que hay programas y SO más seguros que otros en tanto tienen menos "agujeros" o vulnerabilidades, se actualizan más rápido y, en términos generales, le hacen la vida más difícil a los atacantes.

Es en este sentido que podemos decir, por ejemplo, que Linux es más seguro que Windows. Ahora bien, ¿qué es lo que hace que Linux sea más difícil de vulnerar? Bueno, una respuesta que he leído y escuchado hasta el artazgo tiene que ver con el "security through obscurity" o "seguridad por oscuridad". Básicamente, lo que argumentan muchos supuestos "expertos en seguridad" cuando se les pregunta por qué Linux es más seguro es que como la mayor parte del mercado de SO está en manos de Microsoft Windows, y los hackers malos quieren hacer el mayor daño posible, entonces apuntan a Windows. La mayor parte de los hackers quieren robar la mayor cantidad de información posible o realizar alguna acción que los destaque por sobre los demás y les dé "prestigio" dentro de su círculo. En la medida en que Windows es el SO más usado, realizan todos los esfuerzos para crear hacks y virus que afecten ese SO, dejando de lado los demás.

Me parece muy importante destacar que hoy prácticamente nadie cuestiona que efectivamente Linux sea más seguro que Windows. En lo que se equivocan los supuestos "expertos" es en la fundamentación, he aquí la razón por la que me senté a escribir este artículo.

Los "expertos", como decía, sólo se basan en un mero dato estadístico para explicar por qué Linux es más seguro: existen menos virus y malwares para Linux en comparación con la enorme cantidad que hay para Windows. Ergo, Linux es más seguro... por ahora. Claro, al basar toda su argumentación en este mero dato, en la medida en que más usuarios se pasen a Linux, los hackers malos van a concentrarse cada vez más en crear utilidades y herramientas malignas para explotar todas y cada una de las vulnerabilidades de Linux. Se trata simplemente de un sistema de incentivos, que haría más atractivo para los hackers desarrollar virus y malware para Linux en la medida en que se vaya haciendo cada vez más popular. La supuesta seguridad de Linux, si acordamos con el análisis de los "expertos", sería una gran mentira. Linux no sería seguro sino utilizado por poca gente. Nada más... Yo creo, en cambio, que la mayor seguridad que aporta Linux se basa en algunos aspectos fundamentales de su diseño y estructura.

Otro dato estadístico alcanza para empezar a darnos cuenta de que los "expertos" no saben nada. El servidor web Apache (un servidor web es un programa que se encuentra alojado en una computadora remota que aloja y envía las páginas a tu explorador web cuando vos, visitante, pedís acceso a esas páginas), que es software libre y corre generalmente bajo Linux, tiene la cuota de mercado más grande (mucho mayor que la del servidor IIS de Microsoft) y a pesar de ello sufre muchos menos ataques y tiene menos vulnerabilidades que la contraparte de Microsoft. En otras palabras, en el mundo de los servidores donde la historia es al revés (Linux + Apache poseen la mayor cuota del mercado), Linux ha demostrado ser más seguro que Windows. Las empresas de software más grandes del mundo, los proyectos científicos más ambiciosos, incluso los gobiernos más importantes, todos eligen Linux para almacenar y proteger la información de sus servidores y cada vez más son aquellos que lo están empezando a elegir como sistema de escritorio. ¿Vos que vas a elegir?

Las 10 características que hacen a Linux muy seguro

En contraste con el endeble papelucho de cartón en el que, con suerte, te puede llegar el CD de Linux (estoy pensando en un Ubuntu, por ejemplo), el CD de Windows típicamente viene en una cajita de plástico que está cerrada herméticamente y que tiene una etiqueta bien visible que te pide con ansias que prestes conformidad con los términos de la licencia que acompaña al CD y que probablemente encuentres en la prolija caja de cartón en la que todo venía empaquetado. Este sello de seguridad está diseñado para prevenir que los gusanos vulneren la cajita de plástico de tu CD e infecten tu copia de Windows antes de que sea efectivamente instalada, lo cual constituye un recaudo importante y un activo de seguridad invaluable.

Claramente Windows le saca ventaja a Linux en lo que respecta a la seguridad física de sus copias (jaja), pero ¿qué sucede una vez que ya lo instalamos? ¿Cuáles son las 10 características que hacen a Linux más seguro que Windows?

1. Es un sistema multiusuario avanzado.

En la medida en que Linux se basa en Unix, originalmente pensado para su utilización en redes, se explican algunas de sus importantes ventajas en relación a la seguridad respecto de Windows. El usuario con más privilegios en Linux es el administrador; puede hacer cualquier cosa en el SO. Todos los otros usuarios no obtienen tantos permisos como el root o administrador. Por esta razón, en caso de ser infectado por un virus mientras un usuario común está sesionado, sólo se infectarán aquellas porciones del SO a las que ese usuario tenga acceso. En consecuencia, el daño máximo que ese virus podría causar es alterar o robar archivos y configuraciones del usuario sin afectar seriamente el funcionamiento del SO como un todo. El administrador, además, estaría habilitado para eliminar el virus fácilmente.

Una vez que concluye la instalación de cualquier distro Linux, se nos solicita que creemos un root y un usuario común. Esta falta total de seguridad que involucra la creación de más de un usuario por computadora es la causante de su poca popularidad. ¡Ja! No, hablando en serio, esta es una de las razones por las que Linux es más seguro.

En comparación, por ejemplo en Windows XP, las aplicaciones de usuario, como Internet Explorer, tienen acceso a todo el sistema operativo. Es decir, supongamos que IE se vuelve loco y quiere borrar archivos críticos del sistema... bueno, podría hacerlo sin problemas y sin que el usuario se entere de nada. En Linux, en cambio, el usuario tendría que configurar explícitamente la aplicación para que corriese como root para introducir el mismo nivel de vulnerabilidad. Lo mismo sucede con los propios usuarios. Supongamos que una persona se sienta en mi compu con WinXP. Va a C:\Windows y borra todo. No pasa naranja. Lo puede hacer sin problemas. Claro, los problemas vendrán la próxima vez que intente iniciar el sistema. En Windows el usuario y cualquier programa que él instale tienen acceso para hacer prácticamente cualquier cosa en el SO. En Linux esto no sucede. Linux utiliza una administración de privilegios inteligente por el cual siempre que el usuario quiera hacer algo que sobrepase sus privilegios se pedirá la contraseña del root.

Sí, es molesto... pero es lo que lo hace seguro. Hay que escribir la bendita contraseña cada vez que se quiera hacer algo que potencialmente pueda afectar la seguridad del sistema. Esto es más seguro porque los usuarios "comunes" no tienen acceso para instalar programas, ejecutar llamadas del sistema, editar archivos del sistema, cambiar configuraciones críticas del sistema, etc.

Desde el principio, Linux fue diseñado como un sistema multiusuario. Incluso ahora, las debilidades más importantes de Windows están vinculadas a sus orígenes como sistema independiente para 1 sólo usuario. Lo malo del modo de hacer las cosas en Windows es que no hay capas de seguridad. Es decir, una aplicación de alto nivel, como un explorador de internet o un procesador de textos, están unidos y pueden acceder a las capas más bajas del sistema operativo, con lo cual la más pequeña vulnerabilidad puede dejar expuesto a todo el sistema operativo.

Desde Windows Vista, se introdujo en Windows el Control de Cuentas de Usuario (UAC por sus siglas en inglés) que hace que cada vez que quiera ejecutarse un programa o realizarse alguna tarea potencialmente peligrosa se requiera la contraseña del administrador. Sin embargo, sin contar el hecho de que al menos aquí en Argentina casi todos siguen usando WinXP por su comodidad y facilidad, la mayor parte de los usuarios de Win7 o Win Vista se loguean siempre como administradores o le otorgan derechos de administrador a sus usuarios. Al hacerlo, cada vez que quieran realizar alguna de estas tareas "peligrosas" el sistema simplemente mostrará un cuadro de diálogo que el usuario debe aceptar o rechazar. Cualquier persona que se siente en tu escritorio y/o se apodere de tu máquina automáticamente tiene privilegios de administrador para hacer lo que se le cante. Para una comparación completa entre UAC y su, sudo, gksudo, etc. les recomiendo leer este artículo de Wikipedia.

2. Mejor configuración por defecto.

Por su parte, la configuración por defecto en todas las distros Linux es mucho más segura que la configuración por defecto de Windows. Este punto está íntimamente vinculado con el anterior: en todas las distros Linux el usuario tiene privilegios limitados, mientras que en Windows casi siempre el usuario tiene privilegios de administrador. Cambiar estas configuraciones es muy fácil en Linux y un poco complicado en Windows.

Claro que cualquiera de éstos puede ser configurado de tal modo de convertirlo en un sistema inseguro (al correr todo como root en Linux, por ejemplo) y Windows Vista o Windows 7 (que, por cierto, copiaron algunas de estas características de Linux y Unix) podrían configurarse de mejor modo para hacerlos más seguros y ejecutarse bajo una cuenta más restringida que la del administrador. Sin embargo, en la realidad esto no sucede. La mayor parte de los usuarios de Windows tiene privilegios de administrador... es lo más cómodo.

3. Linux es mucho más "asegurable"

En la medida en que la seguridad, como vimos al comienzo, no es un estado sino un proceso, aún más importante que venir "desde fábrica" con una mejor configuración por defecto es poder brindarle al usuario la libertad suficiente como para adaptar los niveles de seguridad a sus necesidades. A esto es a lo que yo llamo "asegurabilidad". En este sentido, Linux no sólo es reconocido por su enorme flexibilidad sino por permitir ajustes de seguridad que serían imposibles de conseguir en Windows. Esta es la razón, precisamente, por la que las grandes empresas eligen Linux para administrar sus servidores web.

Podrá sonar muy "zen", pero esta situación me recuerda a una anécdota que alguien me contó alguna vez. No sé si todavía sigue sucediendo pero me dijeron que en China la gente le pagaba al médico cuando estaba bien y dejaba de hacerlo cuando estaba mal. Es decir, al revés de lo que hacemos nosotros en la "sociedad occidental". Aquí sucede algo parecido. En Windows existe un enorme mercado en torno a la seguridad pero que se basa esencialmente en controlar o disminuir los efectos y no las causas que hacen de Windows un sistema inseguro. En Linux, en cambio, un usuario intermedio o avanzado puede configurar el sistema de tal modo que sea prácticamente impenetrable sin que ello implique la instalación de un antivirus, antispyware, etc. En otras palabras, en Linux el foco está puesto en las causas, o sea en las configuraciones que hacen a un sistema más

seguro; mientras que en Windows el acento (y el negocio) está puesto en las consecuencias de una posible infección.

4. No hay archivos ejecutables ni registro

En Windows, los programas maliciosos generalmente son archivos ejecutables que, luego de engañar al usuario o saltear su control, se ejecutan e infectan la máquina. Una vez que esto sucedió es muy difícil removerlos ya que, en caso de que podamos encontrarlo y eliminarlo, éste se puede replicar e incluso puede guardar configuraciones en el registro de Windows que le permitan "revivir". En Linux, en cambio, no existen, estrictamente hablando, archivos ejecutables. En realidad, la ejecutabilidad es una propiedad de cualquier archivo (sin importar su extensión), que el administrador o el usuario que lo creó puede otorgarle. Por defecto, ningún archivo es ejecutable a menos que alguno de estos usuarios así lo establezcan. Además, Linux utiliza archivos de configuración en vez de un registro centralizado. Es conocida aquella frase que dice que en Linux todo es un archivo. Esta descentralización, que permite evitar la creación de una enrome base de datos hipercompleja y enredada, facilita enormemente la eliminación y detección de los programas maliciosos así como dificulta su reproducción teniendo en cuenta que un usuario normal no puede editar archivos del sistema.

5. Mejores herramientas para combatir los ataques zero-day

No siempre alcanza con tener todo el software actualizado. Los ataques zero-day (un ataque que explota vulnerabilidades que los propios desarrolladores del software todavía desconocen) son cada vez más comunes. Un estudio ha demostrado que lleva solamente seis días a los crackers desarrollar software malicioso que explote estas vulnerabilidades, mientras que le lleva meses a los desarrolladores detectar estos agujeros y lanzar los parches necesarios. Por esta razón, una política de seguridad sensible tiene siempre en cuenta la posibilidad de ataques zero-day. Windows XP no cuenta con tal provisión. Vista, en modo protegido, aunque es útil, provee solamente protección limitada a los ataques a IE. En contraste, la protección provista por AppArmor o SELinux es ampliamente superior, proveyendo una protección muy "fina" contra cualquier tipo de intento de ejecución de código en forma remota. Por esta razón, es cada vez más común que las distros Linux vengan con AppArmor (SuSE, Ubuntu, etc.) o SELinux (Fedora, Debian, etc.) por defecto. En otros casos, se pueden bajar fácilmente desde los repositorios.

6. Linux es un sistema modular.

El diseño modular de Linux permite eliminar un componente cualquiera del sistema en caso de ser necesario. En Linux, se podría decir que todo es un programa. Hay un programita que gestiona las ventanas, otro que gestiona los logins, otro que se encarga del sonido, otro del video, otro de mostrar un panel de escritorio, otro que funciona como dock, etc. Finalmente, como las piezas de un lego, todas ellas forman el sistema de escritorio que conocemos y utilizamos diariamente. Windows, en cambio, es un enorme bloque de cemento. Es un bodoque que es muy difícil de desarmar. Así, por ejemplo, en caso de que tengas la sospecha de que Windows Explorer tiene alguna falla de seguridad, no vas a poder eliminarlo y reemplazarlo por otro.

7. Linux es software libre.

Sí, definitivamente esta es una de las razones más importantes por las que Linux es un SO mucho más seguro que Windows porque en primer lugar los usuarios pueden saber exactamente qué hacen los programas que componen el SO y, en caso de detectar una vulnerabilidad o irregularidad, pueden corregirla al instante sin tener que esperar un parche, actualización o "service pack". Cualquiera puede editar el código fuente de Linux y/o los programas que lo componen, eliminar la brecha de seguridad y compartirla con el resto de los usuarios. Además de ser un sistema más solidario, que incentiva la participación y la curiosidad de los usuarios, es mucho más práctico a la hora de resolver agujeros de seguridad. Más ojos permiten la detección y solución más rápida de los problemas. En otras palabras, hay menos agujeros de seguridad y los parches se lanzan más rápidamente que en Windows.

Además, los usuarios de Linux estamos mucho menos expuestos a los programas spyware y/o cualquier otro programa que obtenga información del usuario en forma oculta o engañosa. En Windows, no tenemos que esperar a infectarnos con algún programa malicioso para sufrir este tipo de robo de información; existen pruebas de que el propio Microsoft e incluso otros programas muy reconocidos realizado por otras empresas, han adquirido información sin el consentimiento de los usuarios. Concretamente, Microsoft es acusado de utilizar software con nombres confusos, como el Windows Genuine Advantage, para inspeccionar los contenidos de los discos rígidos de los usuarios. El acuerdo de licencia incluido en Windows requiere que los usuarios acepten esta condición antes de usar Windows y afirma el derecho de Microsoft para hacer este tipo de inspecciones sin notificar a los usuarios. En definitiva, en la medida en que la mayor parte del software para Windows es privativo y cerrado, todos los usuarios de Windows y los desarrolladores de programas para ese SO dependen de Microsoft para solucionar las brechas de seguridad más graves. Lamentablemente, Microsoft tiene sus propios intereses en materia de seguridad, que no necesariamente son los mismos que los de los usuarios.

Existe el mito de que, al estar disponible públicamente su código fuente, Linux y todos los programas de software libre que corren bajo Linux son más vulnerables porque los hackers pueden ver cómo funcionan, encontrar los huecos de seguridad más fácilmente y sacar provecho de ellos. Esta creencia está muy vinculada al otro mito que nos encargamos de deshacer al comienzo del artículo: la oscuridad trae seguridad. Esto es falso. Cualquier experto en seguridad realmente serio sabe que la "oscuridad", en este caso dada por tratarse de software de código cerrado, dificulta la detección de las brechas de seguridad por parte de los propios desarrolladores, así como dificultan el informe y detección de estas brechas por parte de los usuarios.

8. Repositorios = chau cracks, seriales, etc.

El hecho de que Linux y la mayor parte de las aplicaciones que se escriben para correr en él sean software libre ya, de por sí, es una enorme ventaja. No obstante, si esto no estuviera combinado con el hecho de que todo ese software se encuentra

disponible para su descarga e instalación desde una fuente centralizada y segura, probablemente su ventaja comparativa respecto de Windows no sería tan considerable.

Todos los usuarios de Linux sabemos que al instalar Linux automáticamente nos olvidamos de buscar seriales y cracks que, por otra parte, nos obligan a navegar por sitios inseguros o deliberadamente diseñados para hacer caer a los usuarios y jugar con sus necesidades. Tampoco precisamos de la instalación de ningún crack, los cuales muchas veces tienen algún virus o malware por ahí escondido. En cambio, sí tenemos, dependiendo de la distro que usemos, una serie de repositorios desde los cuales bajamos e instalamos el programa que necesitemos con un simple clic. Sí, ¡así de fácil y seguro!

Ya desde los primeros pasos de la instalación de Windows, éste demuestra su amplia superioridad en términos de seguridad. A medida que el proceso de instalación comienza, se insiste que el usuario ingrese un número de serie antes de continuar. Sin esta información vital, el usuario no puede continuar con la instalación. La mayor parte de los usuarios de Windows por suerte todavía no saben que una búsqueda rápida en Google puede brindarle acceso a miles de seriales, así que esta pieza de información es la defensa más poderosa contra los indeseados back-doors. Sí... es un chiste. :) ¿Qué seguridad brinda un sistema que puede ser crackeado y vulnerado de modo que se pueda evitar el ingreso del serial, único medio a través del cual Microsoft se asegura que los usuarios paguen por sus copias? Es un SO tan malo que ni siquiera pueden (¿ni quieren?) hacerlo invulnerable de modo tal que todos paguen por sus copias.

9. 1, 2, 3... Actualizando

Si sos como la mayoría de las personas que conozco, usás WinXP. El primer XP venía con el IE 6 (de agosto de 2001), el XP con el service pack 1 venía con el IE 6 SP1 (de septiembre de 2002) y el XP SP2 venía con el IE 6 SP2 (de agosto de 2004). En otras palabras, en el mejor de los casos, estás utilizando un explorador que fue desarrollado hace casi 6 años. No hace falta explicar la enormidad que esto significa en términos del desarrollo de software. En esos años no sólo se detectaron y explotaron miles de vulnerabilidades al WinXP sino también al explorador que utiliza por defecto.

En Linux la cuestión es bien diferente. Es mucho más seguro que Windows porque está siendo permanentemente actualizado. Gracias a que Linux es un sistema modular, desarrollado como software libre y que cuenta con un sistema de repositorios de gestión de actualizaciones e instalación de nuevos programas, estar al día es una pavada. Desde el explorador de internet hasta el más recóndito programita que gestiona los privilegios de usuarios o la gestión de las ventanas, etc., pasando por el kernel y los drivers necesarios para el funcionamiento del sistema, todo se actualiza mucho más rápido y fácil que en Windows.

Precisamente, en Windows, las actualizaciones se realizan una vez por mes. Claro, eso si no las desactivaste, ya sea porque te resultaban molestas, porque consumían parte de tu ancho de banda o simplemente por temor a que Microsoft detectara de algún modo tu copia ilegal. Pero eso no es lo peor. La actualización de cada una de las aplicaciones es independiente, esto significa que Windows no se encarga de actualizarlas, cada una de ellas tiene que encargarse de ello. Como bien sabemos, muchas no tienen la opción de buscar las actualizaciones. Es el usuario el que se tiene que preocupar por enterarse del lanzamiento de una nueva versión, la descarga y la posterior actualización (siempre con el temor de no saber si tiene que borrar la versión anterior o no).

10. Diversidad, bendita tu eres entre todas.

Los usuarios de Windows están acostumbrados a que Microsoft les diga qué programa utilizar para cada cosa. De este modo, la utilización del sistema se supone que es más sencilla, se crean estándares comunes, se facilita la compatibilidad, etc. En fin, todo esto ha demostrado ser falso. Por el contrario, ha contribuido meramente a la uniformidad y el direccionamiento desde arriba, como si se tratara de una dictadura. Esa homogeneidad ha facilitado enormemente la tarea de los atacantes para detectar vulnerabilidades y escribir programas maliciosos que las exploten.

En comparación, en Linux existen una cantidad infinita de distribuciones con diferentes configuraciones, rutas de sistema, sistemas de gestión paquetes (unos usan .deb, otros .rpm, etc.), programas de gestión de todas las actividades del sistema, etc. Esta heterogeneidad dificulta enormemente el desarrollo de virus que tengan un amplio impacto, como sí es posible en Windows.

Los detractores de Linux dicen que más distribuciones equivalen a una mayor propensión de error y, por consiguiente, mayores vulnerabilidades de seguridad. Esto, en principio, podría ser cierto. Sin embargo, como acabamos de ver, esto se ve más que compensado por el hecho de que esas vulnerabilidades son más difíciles de explotar y terminan afectando a menos gente. En definitiva, los incentivos de los hackers para escribir software malicioso que afecte a estos sistemas disminuyen notablemente.

Yapa. Los programas para Linux son menos vulnerables que sus contrapartes para Windows.

Esto es algo que, de algún modo, ya lo mencioné al desarrollar algunos de los otros puntos pero me pareció importante destacarlo como un punto aparte. El software para Linux es más seguro y menos vulnerable que su contraparte para Windows por varios de los aspectos que también caracterizan a Linux: es software libre, se actualiza mucho más rápido, se obtiene a través de los repositorios, existe una enorme diversidad de programas, etc. Es decir, tanto en su diseño y desarrollo como en su distribución y ejecución, los programas para Linux brindan mayores ventajas de seguridad.

fuente http://usemoslinux.blogspot.com/2010/06/por-que-linux-es-mas-seguro-que-windows.html