Importancia del Software Libre en la Seguridad Informática

Importance of Free Software in Computer Security.

Diego Osorio, Andrés Acosta, Leidy Aldana.
Estudiantes de pregrado en Ingeniería de Sistemas

Resumen

El software libre hace parte de una construcción social que beneficia a la comunidad; en el campo de la Seguridad Informática juega un papel importante con entornos y herramientas potentes que han revolucionado este campo.

Palabras clave: Confiabilidad, Integridad, Disponibilidad, Libertad, Seguridad.

Introducción

Compartir conocimiento ha aportado en la evolución de las sociedades, de forma similar, compartir código ha aportado a la construcción de software de mayor calidad; más allá del código abierto este artículo hace referencia al Software Libre, el cual permite la libertad del usuario y la libertad del software, permite modificar de acuerdo a necesidades propias, permite ayudar a una persona o a una comunidad; el software es libre al tener cuatro libertades, enunciadas en *Software Libre para una Sociedad Libre* (Stallman, 2004, página 236):

0. La libertad cero es la libertad de ejecutar el programa con cualquier propósito.
1. La libertad uno es la libertad de ayudarte a ti mismo cambiando el programa para que se ajuste a tus necesidades.
2. La libertad dos es la libertad de ayudar al prójimo distribuyendo copias del programa.
3. La libertad tres es la de ayudar a distribuir a tu comunidad publicando una versión mejorada de modo que los otros puedan beneficiarse de tu trabajo.

Gracias a estas cuatro libertades el Software Libre ha contribuido y puede contribuir en el aprendizaje, en la construcción y el soporte de grandes empresas o en la enseñanza; de hecho puede ser una alternativa que resulta más interesante, alejada del tedio y más próxima al área científica. Cabe resaltar que libre es diferente de gratis (libre como pensamiento libre más no como barra libre), que el software libre no quita el reconocimiento de la persona que contribuye a crear software o otro aporte hecho a la construcción de conocimiento libre.

El Software Libre tiene la ventaja de ser estudiado, ejecutado, modificado y distribuido.

Su importancia se ve reflejada en la mejora continua, en que brinda la oportunidad de aprender apartir de aportes realizados por otras personas, se ve reflejada en el hecho de que el conocimiento debería ser libre. Para algunas personas más allá de estas ventajas mencionadas anteriormente, la elección de utilizar Software Libre es una cuestión ética, de ciencia, de no permanecer tanto en la ignorancia, tomando como ejemplo el área de la seguridad informática (área que hace parte de la mayoría de las tecnologías de la información y la comunicación), hay programas no libres que cuentan con código oculto utilizado para conseguir información del usuario o ejecutar procesos sin permiso del usuario.

Se denomina por seguridad informática a las medidas y controles que garantizan la confiabilidad, integridad y disponibilidad de los activos del sistema de información; incluyendo hardware y software, firmware e información procesada, almacenada y comunicada.

El área de la seguridad informática influye en la mayoría de las áreas en la actualidad, como en el desarrollo web, en la inteligencia artificial, en el manejo de grandes volúmenes de información; desde una perspectiva más cotidiana influye en el simple hecho de enviar un correo electrónico (para que llegue sin modificaciones exclusivamente al destinatario), de hacer una transacción bancaria en linea, o realizar la conexión a una red wi-fi sin que la información de nuestros dispositivos sea vulnerable.

La seguridad informática son las medidas y controles que garantizan la confiabilidad, integridad y disponibilidad de los activos del sistema de información.

De esta forma, este artículo busca mostrar al lector la importancia del trabajo conjunto de estos dos campos a través de ventajas, de herramientas, de alternativas.

Herramientas

Las herramientas utilizadas en la seguridad informática que son de código abierto, permiten que la comunidad examine el código, lo entiendan e incluso lo modifiquen, lo que permite a los usuarios aprender acerca del software, ajustarlo a sus necesidades e incluso contribuir. Esto lo hace más versátil e incluso agrega la confiabilidad de usarlo sabiendo que muchas personas han examinado el código y nos da la certeza que hace lo que debe, que en este no se encuentra código malicioso que pueda afectar a quien lo use y que ya ha sido probado.

El fácil acceso a todo tipo de usuarios, dónde no se tiene que pagar por utilizar, y el gran aumento del uso de las tecnologías de la información y el mundo digital, permite que la comunidad que utiliza software libre en la seguridad informática sea cada vez más, en los últimos años ha ganado mucha popularidad, incluso la demanda laboral ha aumentado drásticamente en los últimos años al igual que el uso de software libre a nivel profesional en la seguridad informática y personas especializadas en él.

Al ser probado constantemente por diferentes personas, con diferentes enfoques hace que se encuentren mayor número de problemas y fallos en menor tiempo que un software que sólo es mantenido por una empresa. Al haber más personas que pueden contribuir a mejorarlo, se ve una evolución constante haciendo las herramientas de software libre actualizadas, versátiles y altamente competitivas.

Es bastante la información que se encuentra en Internet de las herramientas de software libre en el campo de la seguridad informática, en los principales blogs se discute y comparte especialmente sobre software de código abierto. Tanto organizaciones como personas individuales comparten constantemente documentación, guías, tutoriales, vídeos, experiencias, preguntas, trucos, etc. generando una gran cantidad de material en múltiples idiomas permitiendo que casi cualquier persona con iniciativa y con algunos conocimientos básicos de la informática pueda aprender a utilizar estas herramientas.

Kali Linux

Es una distribución de software libre la cual esta en constante evolución con nuevas características que se agregan constantemente, esta distribución esta diseñada específicamente para pruebas de penetración profesional y auditoria de seguridad.

Cambios principales de esta distribución

Usuario único, acceso root por diseño:

Es diseñado para trabajar en un único escenario root (usuario principal o administrador del sistema) ya que la mayoría de las herramientas utilizadas en pruebas de penetración requieren privilegios escalonados.

Servicios de red deshabilitados de forma predeterminada:

Kali Linux contiene Demonios (scripts en segundo plano) que desactivan los servicios de red de forma predeterminada. Estos Demonios nos permiten instalar varios servicios en Kali Linux, a la vez que nos aseguramos de que nuestra distribución permanezca segura de forma predeterminada, sin importar qué paquetes estén instalados. Los servicios adicionales, como Bluetooth, también están en la lista negra de forma predeterminada.

Núcleo Linux personalizado:

Kali Linux utiliza un kernel en sentido ascendente, con parches para inyección inalámbrica.

Un conjunto mínimo y confiable de repositorios:

Dado los objetivos y metas de Kali Linux para mantener la integridad del sistema como un todo. Con ese objetivo en mente, el conjunto de fuentes de software ascendente que Kali utiliza se mantiene en un mínimo absoluto. Muchos nuevos usuarios de Kali están tentados a agregar repositorios adicionales a sus *sources.list*, pero al hacerlo corre un riesgo muy serio de romper la instalación de Kali Linux.

¿Es Kali Linux adecuado para usted?

Los desarrolladores de Kali linux recomiendan que esta distribución debe ser usada por probadores de penetración profesional y especialistas en seguridad, ya que no es una distribución para soluciones generales

de GNU/LINUX como el desarrollo de aplicaciones, diseño web, juegos, etc.

El uso indebido de herramientas de seguridad y de pruebas de penetración dentro de una red, en particular sin una autorización específica, puede causar daños irreparables y tener consecuencias significativas, personales y/o legales. *"No entender lo que estabas haciendo"* no va a funcionar como una excusa.

Sin embargo, si usted es un probador de penetración profesional o está estudiando pruebas de penetración con el objetivo de convertirse en un profesional certificado, no hay mejor juego de herramientas - a cualquier precio - que Kali Linux.

Algunas Herramientas de seguridad y hacking.

Nmap *("Mapeador de redes")*

Es una herramienta de código abierto para la exploración de redes y sondeo de seguridad de puertos, se diseño para analizar rápidamente grandes redes, utiliza paquetes IP çrudos"para poder determinar que equipos se encuentran disponibles en la red, esta herramienta generalmente se usa para auditoria de seguridad, administradores de redes, y es útil para realizar tareas rutinarias, como puede ser el inventariado de la red, la planificación de actualización de servicios y la motorización del tiempo que los equipos o servicios se mantiene activos en la red. El código fuente lo puedes encontrar en: github.com/nmap/nmap

John the Ripper

Es un programa libre de código abierto de criptografia, el cual aplica fuerza bruta para descifrar contraseñas, esta herramienta nos permite romper algoritmos de cifrado o hash, como DES, SHA-1 y otros. El código fuente lo puedes encontrar en: github.com/magnumripper/JohnTheRipper

Nikto

Nikto es un software de código abierto (GPL), diseñado para evaluar la seguridad de los servidores web. Este software encuentra varios archivos predeterminados e inseguros, configuraciones y programas en cualquier tipo de servidor web. El código fuente lo puedes encontrar en: github.com/sullo/nikto

Wireshark

Wireshark es un software de código abierto (GPL) el cual lo usan administradores de redes para analizar el trafico de la red, capturar paquetes de diferentes tipos de protocolos que existen. El código fuente lo puedes encontrar en: github.com/wireshark/wireshark

Metasploit

Metasploit es un proyecto de código abierto para seguridad informática el cual proporciona información acerca de vulnerabilidades de seguridad y nos ayuda a realizar tests de penetración "Pentesting"junto con el desarrollo de firmas para sistemas de detección de intrusos. El código fuente lo puedes encontrar en: github.com/rapid7/metasploit-framework

Referencias

[1] Stallman, Richard. *Software Libre para una Sociedad Libre*, disponible en pdf. Madrid, España: Traficantes de sueños, 2004.

[2] 2017 Offensive Security. *Documentación oficial de Kali Linux*, https://docs.kali.org/.

[3] *Guía de referencia de Nmap*, https://nmap.org/man/es/.

[4] RAPID1. *John the Ripper password cracker*, http://www.openwall.com/john/.

[5] Wireshark Foundation . *Documentación oficial de Wireshark*, https://www.wireshark.org/docs/ .

Diego Osorio Estudiante de Ingeniería de Sistemas, actual director del GLUD. Interesado en el Software Libre, el desarrollo de Software y la Seguridad Informática.
daosoriog@gmail.com

Andrés Acosta Estudiante de Ingeniería de Sistemas.
andres.taamap@gmail.com

Leidy Aldana
Estudiante de Ingeniería de Sistemas, interesada por aprender continuamente; quien ve en el software libre una perspectiva más agradable e interesante de su carrera.
LeidyMarcelaAldana@gmail.com