Distribuciones Linux de Seguridad Informática

¿Sabía usted que existen distribuciones de Linux especializadas en Seguridad Informática? Pues sí, las hay, y lo mejor de ellas es que por ser Linux un sistema operativo de código abierto, estas distribuciones son además de muy útiles… gratuitas!!

Hoy vamos a revisar tres distribuciones de Linux especializadas en seguridad:

- Backtrack
- Knoppix-STD y
- Helix

Todas ellas son basadas en LIVE CD, es decir *booteables* desde CD sin necesidad de ser instaladas en el disco duro del equipo, lo cual presenta la ventaja de poder convertir nuestro computador en un sofisticado ambiente para monitoreo, computación forense, hacking, etc., en cuestión de minutos!

Escogí estas tres de un abanico más amplio de opciones entre las que están otras muy buenas distros como Operator, PHLAK, Auditor-Whax y LAS Linux. La razón para la selección no sigue un benchmarking en particular, las escogí porque he trabajado con ellas durante los últimos años, sobre todo con Backtrack, y estoy familiarizada con las bondades que ofrecen en materia de seguridad informática.

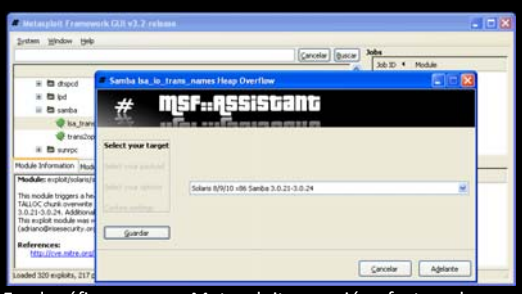
Backtrack

Backtrack es una distribución Linux basada actualmente en Slackware, aunque sus orígenes se remontan a la fusión entre las distribuciones Whax y Auditor Security Collection. Al momento de escribir este artículo la versión 4 de Backtrack se encontraba en Beta, por esta razón nos remitiremos a la última versión estable que es Backtrack 3.

La particularidad de Backtrack que lo hace sumamente popular entre los Administradores de Redes y los Consultores de Seguridades es que incluye alrededor de 300 herramientas especializadas de seguridad, cuyo enfoque se centra en la realización de Pruebas de Penetración o Hacking Ético. Por supuesto el uso ético de Backtrack, o de cualquier otro software de seguridades, depende de quién esté detrás del teclado y en muchas ocasiones esa persona podría ser un Cracker, o Hacker de Sombrero Negro. Pero el tema de la ética requiere un artículo aparte.

De todas las herramientas disponibles en Backtrack quizás la más popular es Metasploit, la cual es un esfuerzo de un grupo selecto de la comunidad de programadores de software libre, que intenta cubrir de manera abierta y gratuita todas las facilidades que brindan las herramientas profesionales y comerciales para Pruebas de Penetración.

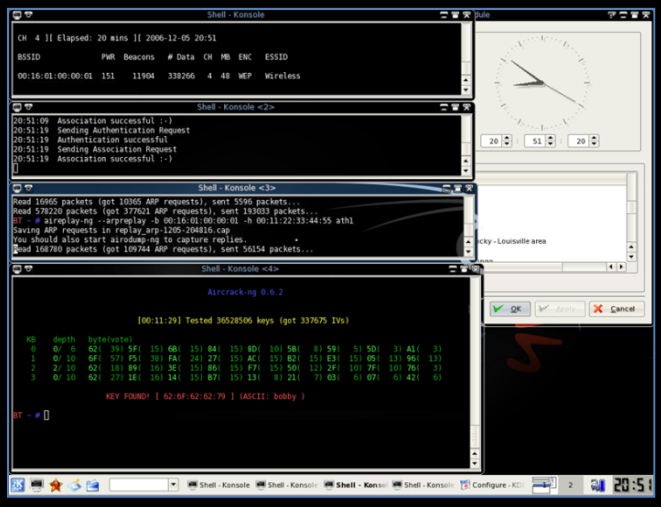
Proyecto Metasploit
http://www.metasploit.com
http://es.wikipedia.org/wiki/Metasploit



En el gráfico vemos a Metasploit en acción efectuando una prueba de vulnerabilidad del servicio SAMBA contra un sistema Unix-Solaris 8/9/10

El proyecto Metasploit está en constante desarrollo y se está acercando a pasos agigantados al nivel de herramientas comerciales costosas para Penetration Testing como son las populares Inmunity Canvas y Core Impact.

Otro fuerte de Backtrack es la variedad de herramientas para monitoreo y pruebas de redes inalámbricas que incluye tanto en su interfaz CLI como GUI. En la figura mostrada abajo podemos ver cómo se rompe una clave WEP de una red wireless haciendo uso de airodump, aireplay y aircrack[i].



Es importante resaltar que a pesar de la gran variedad de herramientas disponibles en Backtrack, éste tiene un bajo consumo de memoria y de procesador, lo que lo hace una distribución ligera e ideal para ejecutarse desde un LIVE CD. Sin embargo podemos instalarlo en nuestro disco duro ejecutando unos cuantos pasos manualmente para la versión 3, se espera que la versión 4 final incluya un instalador gráfico.

Si desea probar Backtrack le sugiero que primero lo instale en una máquina virtual. Para ello debe descargarlo primero desde esta dirección web http://www.remote-exploit.org/backtrack_download.html y luego siga los pasos indicados en este documento: http://www.elixircorp.biz/papers/installing-backtrack3-in-vmware.pdf (documento en idioma inglés).

Knoppix-STD

STD es una distribución basada en Knoppix Linux, que provee cientos de herramientas especializadas de seguridad. Las siglas STD vienen de Security Tools Distribution. Esta distribución tiene la particularidad de ser muy ligera, por lo que la mayoría de las utilidades se ejecutan desde la línea de comandos. Por esta razón no está orientada hacia los usuarios neófitos en Linux sino a los administradores con conocimientos intermedios-avanzados.

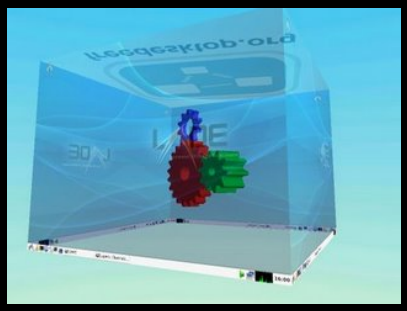
Si usted es un usuario que prefiere las interfaces gráficas entonces es recomendable que use el Knoppix original, creado por el consultor alemán Klaus Knopper[ii]. Aunque esta última distribución es muy amigable y contiene una buena cantidad de software relacionado con seguridad, no tiene tantas herramientas como la versión STD. Por supuesto, siempre existe la posibilidad de instalarla en nuestro disco duro desde el LIVE CD y entonces agregarle las herramientas adicionales que deseemos.

La última versión de Knoppix disponible al momento de realizar este artículo era la 6.0.1 en dos opciones, estándar y micro-knoppix con ADRIANE. La diferencia está en el tamaño y en la ligereza de las versiones, la versión micro-knoppix es una versión compacta que cabe en un solo CD y cuyo kernel ha sido completamente reescrito para guardar completa compatibilidad con su base inicial Debian Linux, optimizando los recursos al máximo y haciendo uso de una interfaz gráfica ligera llamada LXDE. Adicionalmente esta opción incluye el menú con respuesta auditiva ADRIANE (Audio Desktop Reference

Implementation And Networking Environment), el cual permite dar comandos hablados al sistema operativo en alemán e inglés.

Para aquellos fanáticos de los gráficos de alta resolución y de los escritorios en 3D existe además la alternativa de instalar Knoppix en nuestro disco duro y luego agregar otro ambiente gráfico que soporta estas y otras opciones llamado Compiz-Fusion.

En definitiva Knoppix es una excelente opción para el usuario no experto en Linux que desea incursionar en el uso de herramientas de seguridad de información. En el gráfico mostrado abajo podemos observar el escritorio 3D de Knoppix con Compiz-Fusion.



Helix

Helix3 es una distribución Linux basada en Knoppix que se especializa en Computación Forense, Respuesta a Incidentes y Descubrimiento Electrónico, desarrollada por e-Fense. Existen además versiones comerciales como Helix Pro y Helix Enterprise que agregan funcionalidades adicionales por un valor de subscripción anual.

Lo que hace único en su clase a Helix es que es una de las pocas distros libres y por ende **gratis especializadas en computación forense**. Casi todas las herramientas comerciales de buen nivel en esta línea de software cuestan muchos miles de dólares y representan una inversión significativa para el consultor forense que no se ve retribuida aún en nuestro país, en parte porque nuestra economía no tiene el nivel de ingresos que los países en donde se venden estos productos y otro tanto debido a que los empresarios nacionales no están aún acostumbrados a invertir en seguridad de información, con honrosas excepciones principalmente en el sector bancario, telefónicas, carriers e ISP's. Pero la tecno-evangelización de nuestros empresarios para que comprendan la importancia de invertir en seguridad informática para preservar el activo intangible más importante de cualquier organización: la información, es una vez más… tema para otro artículo (-;

Helix por supuesto está basada en LIVE CD, lo cual es importantísimo al momento de analizar un escenario donde ha ocurrido un incidente informático y se desea preservar la evidencia sin modificar los datos originales, para mantener la cadena de custodia tan importante durante un proceso legal, en el caso de que el afectado por un delito informático decida llevar a juicio a los responsables.

En la gráfica podemos ver a Helix en acción, como se puede observar su interfaz gráfica es muy agradable para el usuario:

Adicionalmente Helix incluye la posibilidad de analizar una imagen de un sistema operativo Windows, no sólo de Linux/Unix, lo cual es muy valioso para quien se dedica a la profesión de Investigador Forense Informático.

Lamentablemente en nuestro país no hay una clarificación en la "Ley de Comercio Electrónico, Mensajes Electrónicos y Firmas de Datos", ni tampoco en el reglamento aplicable a esta ley, que indique cuáles son las herramientas open-source y/o comerciales aceptables en un juicio para realizar un proceso de análisis forense, por lo que la validez del análisis dependerá del buen juicio, experiencia y apego a los estándares reconocidos internacionalmente por parte del consultor forense y seamos realistas, dependerá en última instancia de la decisión del juez de turno el cual puede o no estar bien capacitado o asesorado en materia de buenas prácticas de informática forense.

Vale rescatar que el régimen actual ha dado un primer paso positivo en materia de computación forense al proponer la creación de la Unidad de Delitos Informáticos del Ministerio Público, por lo que estaremos pendientes del desarrollo de la propuesta y de la puesta en marcha de esta nueva entidad.

Conclusiones

Tanto Helix como Backtrack y Knoppix son excelentes distribuciones LIVE CD de Linux para seguridad informática y lejos de decir que una es mejor que otra, la experiencia me ha demostrado que ellas se complementan a la hora de realizar Pruebas de Penetración y Análisis Forenses profesionales.

Por ello vale la pena tenerlas a la mano en nuestro kit de herramientas… para cuando el caso se presente.

Por Karina Astudillo B. – Gerente de IT
CCAI – CCNA – SCSA – Cisco FE SMB

---

[i] Para información sobre cursos de capacitación en Linux y cursos de Seguridades en general por favor escríbanos a cursos@elixircorp.biz o llámenos al 593-45000141 | 593-4-2302856 Ext 111.

[ii] El website principal está en idioma alemán, para visitar la página en inglés vaya **a** http://www.knopper.net/knoppix/index-en.html (no hay una página oficial en español, pero sí hay muchos sitios en Internet sobre Knoppix en español que pueden encontrarse fácilmente desde una máquina de búsqueda como Google, Yahoo, Metacrawler, etc.)