Tuxinfo

/tuxinfo
@tuxinfo

una revista libre, para un mundo libre.

nro.53

- Top Aplicaciones Android (II)
- Nessus: Un gran escaner de vulnerabilidades
- Novedades sobre UEFI
- GNOME 3.6: Un cambio necesario
- HTC One X: El gran contrincante del S3 de Samsung
- TuquiGRUB
- La curiosidad mató al gato
- Opinión: La esperanza del desbloqueo
- Privacidad en Internet ¿realmente es posible?
- Linux Containers
- Empaquetamiento RPM (I)

Martín Escboyez | LibreGraphics/Crafts

#53
noviembre 2012

Dirección
Ariel M. Corgatelli

Marketing
Claudia A. Juri

Corrección
Luis Luque
Oscar Reckziegel

Diseño de tapa
Martín Eschoyez

Diseño
Jorge Cacho Hernández

www
http://www.tuxinfo.com.ar

facebook
http://www.facebook.com/tuxinfo

email
info@tuxinfo.com.ar

twitter
@tuxinfo

editorial

Como todos los meses, nos encontramos con un nuevo número de TuxInfo. El avance de Google es muy grande. Muchas veces me han preguntado cuál es el negocio que el gigante de las búsquedas utiliza para subsistir y brindar la gran cantidad de servicios gratuitos que ofrece. Y la respuesta es más que simple: tienen el mayor negocio de publicidades online, pero claro esto no termina de ser comprendido por todas las personas.

Y de hecho la contra pregunta es: si algún día pierden todos los usuarios y al no brindar un producto específico, perderían todo. Claro que esta afirmación tiene algo de razón, pero lo que no se está teniendo en cuenta, es que Google invierte desde hace tiempo en su propia línea de smartphones y ahora también en tabletas (como para romper con el tema de que Android es brindado a los fabricantes de forma gratuita). La línea es muy conocida por su nombre, la misma es "Nexus".

Obviamente detrás de la fabricación de estos dispositivos, lo que hace Google es empujar al mercado móvil a un constante avance y a una constante evolución, contando con productos de primera línea, completamente actualizables desde origen y con las más fuertes características del mercado. Con lo cual la pregunta se responde directamente sobre los productos físicos, además hay que tener en cuenta algo muy importante: la tienda de Android; la misma tiene millones de visitas, millones de descargas y otras tantas apps disponibles para los usuarios en todo el mundo.

De esta manera hay ganancias por el simple alojamiento de las aplicaciones móviles como también por las comisiones que se les cobra por venta a cada desarrollador.

Por lo tanto resumiendo, Google goza de la mejor salud para seguir en el mercado por muchas décadas, liderando el uso del software libre a gran escala.

Y como para ir cerrando, este mes que pasó, la empresa presentó su nueva tableta Nexus 10 pulgadas (de la mano de Samsung), su smartphone Nexus 4 (de la mano de LG) y además muchos más productos relacionados con el software libre. Por supuesto tenemos muchas buenas notas en esta nueva edición de la revista, ya casi terminando el 2012; a la espera de nuevas secciones para el 2013 y por supuesto de nuestro libro conmemorativo por los 5 años de vida de TuxInfo.

Como para redondear el editorial, les cuento que el número está plagado de notas interesantes tales como: la segunda parte del Top Apps Android; TuquitoGrub; Linux Containers; Empaquetamiento RPM Parte I; Nessus 5.0.2. Un gran escáner de vulnerabilidades; Curiosity; Actualización de UEFI; HTC One X, el gran contrincante del S3 de Samsung; Privacidad en Internet; "GNOME 3.6"; y mucho más...

Repetimos la misma convocatoria de meses anteriores en donde podamos tener más sugerencias de ustedes y así adaptar los contenidos de las notas a vuestras necesidades y preferencias, las mismas las podrán realizar a nuestros medios de contacto.

Ariel M. Corgatelli
@arielmcorg

índice

imagen: **ilco**
http://www.sxc.hu/photo/1206711

Top Aplicaciones Android (II)

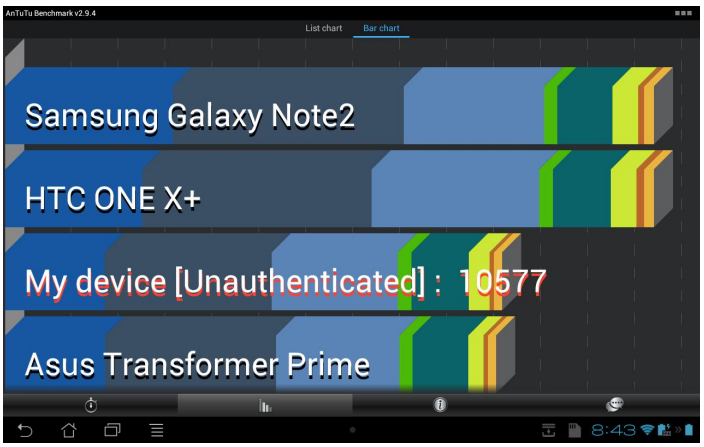
POR **JUAN MANUEL DANSA**

Nos volvemos a encontrar con la última tanda de aplicaciones que utilizo en mis dispositivos: Samsung Galaxy S3 y una Tableta ASUS Transformer PAD TF300T.

ACLARACIÓN: todas las aplicaciones se las puede encontrar en el Google Play con sólo buscarlas, pero también pondré los vínculos a las mismas, y en el caso que no estén se aclarará. Con respecto a las contras que puedo detallar, son solamente desde mi punto de vista y pueden variar según el usuario :-).

Comencemos:

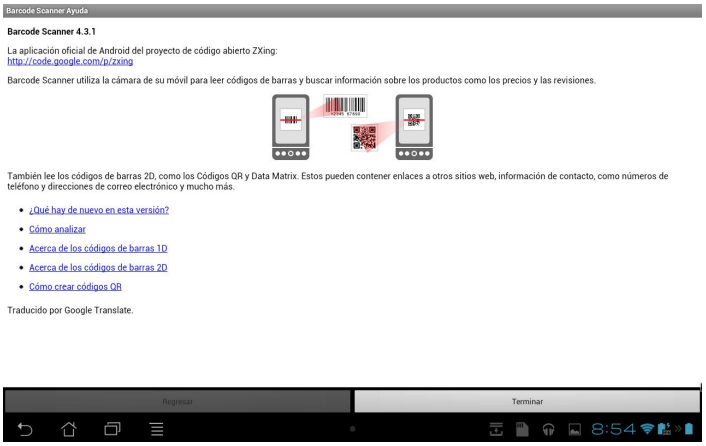
1) AnTuTu Benchmark: Es una excelente aplicación para saber la potencia de los equipos y en qué escala se encuentran. Es ideal para “overclockers”, ya que realiza un análisis de RAM, CPU Integer, CPU flat-point, 2D graphics, 3D graphics, Database IO, SD card W/R, CPU frecuency, Total Score, Battery life score.



https://play.google.com/store/apps/details?id=com.antutu.ABenchMark&feature=search_result#?t=W251bGwsMSwxLDEsImNvbS5hbnR1dHUuQUJlbmNoTWFyayJd

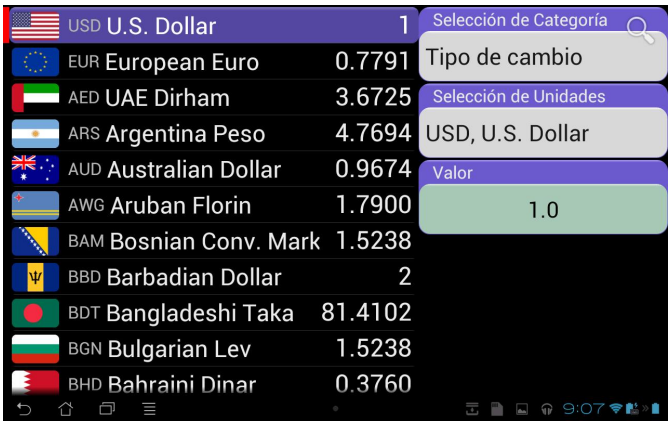
2) Barcode Scanner: El nombre lo dice todo, es un scanner de código se barra, Data Matrix y códigos QR, pequeño y muy útil.

Contra: Dependiendo del dispositivo le cuesta enfocar la cámara. Se recomienda apagar el autoenfoque.



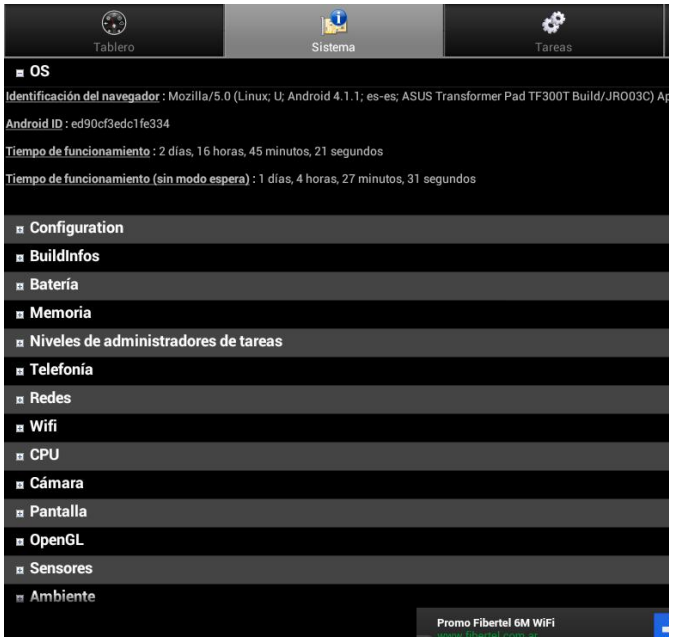
https://play.google.com/store/apps/details?id=com.google.zxing.client.android&feature=search_result#?t=W251bGwsMSwxLDEsImNvbS5nb29nbGUuenhpbmcuY2xpZW50LmFuZHJvaWQiXQ..

3) Conversor de unidades (ConvertPad): Un espectacular conversor de unidades de todo tipo desde distancia hasta divisas. Muy útil para los que necesitan hacer todo tipo de conversiones



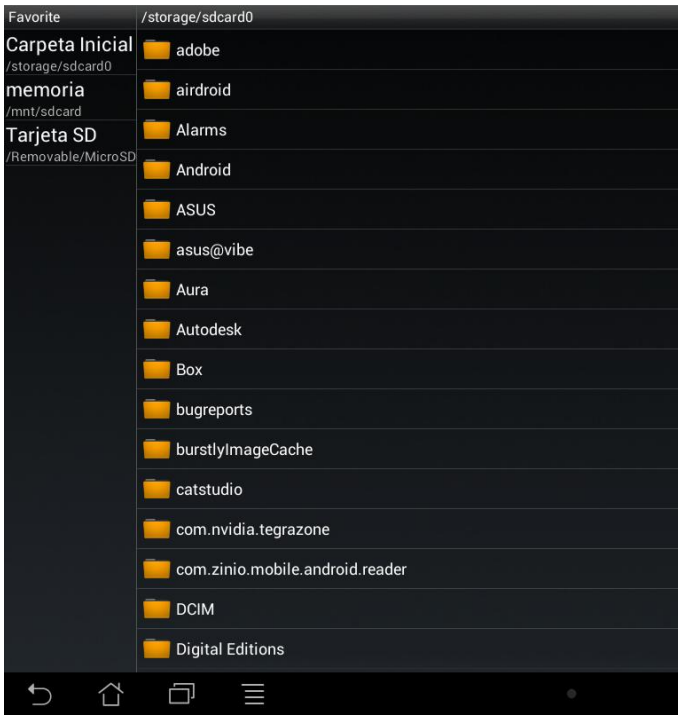
https://play.google.com/store/apps/details?id=com.mathpad.mobile.android.wt.unit&feature=search_result#?t=W251bGwsMSwxLDEsImNvbS5tYXRocGFkLm1vYmlsZS5hbmRyb2lkLnd0LnVuaXQiXQ.

4) Android System Info: Excelente aplicación que nos permite conocer mucha información técnica de nuestros dispositivos (Hardware, Sistema, Telefonía...).



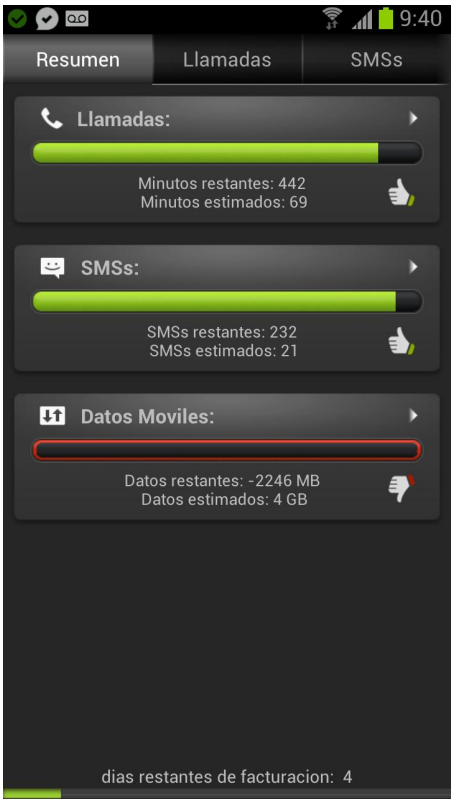
https://play.google.com/store/apps/details?id=com.electricsheep.asi&feature=search_result#?t=W251bGwsMSwxLDEsImNvbS5lbGVjdHJpY3NoZWVwLmFzaSJd

5) Zarchiver: Gestor de archivos que nos permite manejar una alta gama de compresores y en especial 7zip. Nos permite crear los siguientes tipos de archivo: 7z (7zip), zip, bzip2 (bz2), gzip (gz), XZ, alquitrán; descomprimir archivos tipos: 7z (7zip), zip, rar, bzip2, gzip, XZ, iso, tar, arj, cab, LZH, LZMA, xar, tgz, TBZ, Z, deb, rpm, zipx, mtz; ver los archivos contenidos en: 7z (7zip), zip, rar, bzip2, gzip, XZ, iso, tar, arj, cab, LZH, LZMA, xar, tgz, TBZ, Z, deb, rpm, zipx, mtz, y otras funciones muy interesantes.



https://play.google.com/store/apps/details?id=ru.zdevs.zarchiver&feature=search_result#?t=W251bGwsMSwxLDEsInJ1LnpkZXZzLnphcmNoaXZlciJd

6) DroidStats: Esta aplicación nos permite controlar llamadas, cantidad de sms y tráfico de datos. Puedes establecer límites para cada uno, hacer un seguimiento de tus costos y mucha más información y estadísticas acerca de tus llamadas, sms y tráfico de datos. Ideal para cuando nos quieren cobrar de más, vale la pena perder un rato de tiempo para configurarlo bien :-)



https://play.google.com/store/apps/details?id=nitro.phonestats&feature=search_result#?t=W251bGwsMSwxLDEsIm5pdHJvLnBob25lc3RhdHMiXQ..

7) Speedtest.net Mobile: La mejor aplicación para las pruebas de ancho de banda e información relacionada.

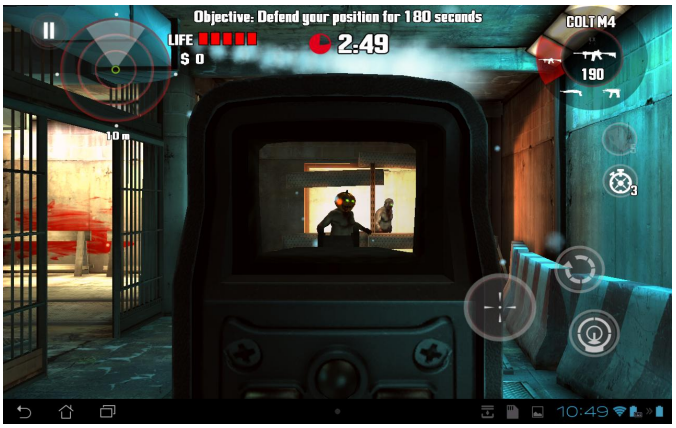
Contra: No optimizado visualmente para tabletas.

https://play.google.com/store/apps/details?id=org.zwanoo.android.speedtest&feature=search_result#?t=W251bGwsMSwxLDEsIm9yZy56d2Fub28uYW5kcm9pZC5zcGVlZHRlc3QiXQ..

8) Y por último he elegido un juego de tantos que hay. Le ha tocado a **DEAD TRIGGER** de MADFINGER Games.

Uno de los mejores FPS, con gráficos de lujo (muy optimizados en micros TEGRA 2 y 3) un “Zombie Killer” de primera línea. Un gran arsenal , niveles detallados con increíbles efectos de luces, un control simple que funciona a la perfección, actualizaciones gratuitas con más armas, personajes. Horas de juego garantizadas al máximo.

Los Fanáticos de “Resident Evil” no pueden dejar de bajarlo.



https://play.google.com/store/apps/details?id=com.madfingergames.deadtrigger&feature=search_result#?t=W251bGwsMSwxLDEsImNvbS5tYWRmaW5nZXJnYW1lcy5kZWFkdHJpZ2dlciJd

Con esto termino de mostrar algunas de las aplicaciones que utilizo en mis dispositivos Android, hay otras muy conocidas por todos como Flipboard, TuneIn Radio que bien valen la pena, pero son por demás conocidas y solo elegí las que me parecían un poco más interesantes :-). Espero haberles sido de utilidad nos vemos la próxima!!!

Juan Manuel Dansa (Amonal)
amonal88@gmail.com
*twitter: @Amonal_*
g+: Amonal Novell

http://www.tuxinfo.com.ar

TUXINFO

dotLinuX
Infraestructure · Security
Training · Design

ubuntu®

Educación a Distancia para toda América Latina por expertos profesionales

Curso Administrador LINUX

- ¿Qué es Linux?
- ¿Cómo funciona?
- Instalando Linux por primera vez
- Comandos Básicos para Linux
- ¿Qué son los procesos?
- Gestión de Usuarios y Permisos
- Gestores de Paquetes
- Dispositivos de Almacenamiento
- Sistemas de Almacenamiento en Red
- Montaje de un Servidor LAMP

Y de regalo te llevas los siguientes cursos

- Servidores de Correo
- Virtualización
- Ethical Hacking

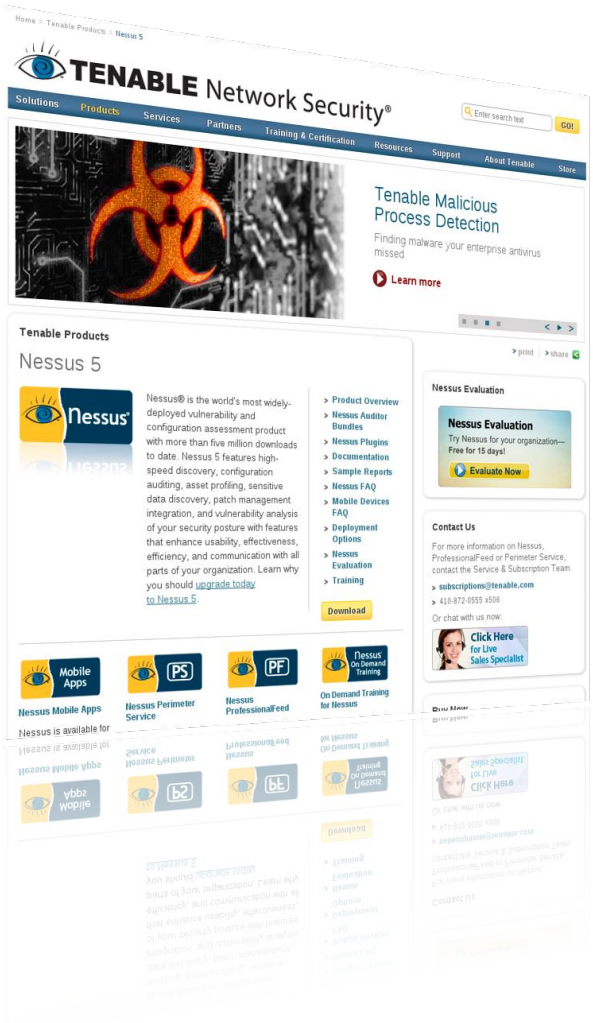
Con el respaldo de la Organización Argentina de Hackers Eticos

Consulta las formas de pago disponibles para tu país

Santander Río · Galicia · Banelco · Link · Visa · MasterCard · American Express · Argencard · Cabal · rapipago · Pago Fácil · Mercado Pago · DineroMail · Payoneer · PayPal · Western Union

cursos@tuxinfo.com.ar

http://www.tuxinfo.com.ar



Nessus

Un gran escaner de vulnerabilidades

POR **RAFAEL MURILLO**

Debo admitir que ha sido más difícil decidir el título de la nota, que la nota en sí... Supuse que muchos de nuestros lectores no conocen esta herramienta, y muchos otros sí, pero se me hacía personalmente “raro” tener que poner en el título de qué se trata esto.

Nessus es un escáner de vulnerabilidades (herramienta indispensable para pentesters), es libre y está disponible en su Sitio Oficial (http://www.nessus.org).

Nessus fue iniciado y es mantenido por Renaud Deraison. Este software es liberado bajo licencia GPL y mucha gente contribuye en su desarrollo, especialmente cuando se trata de pluggins. Nessus trabaja en diversos tipos de UNIX y Linux, ya sea como cliente o servidor, y en Win32 como un cliente.

Como ya mencioné anteriormente, para descargar esta aplicación, debemos visitar su sitio oficial (http://www.nessus.org).

Requerimientos

Como cualquier Software que queramos instalar, debemos conocer primero los requerimientos previos (sí, todo software requiere algunas cosas, aunque no se hayan detenido a leer la documentación de lo que instalan). Para usar esta herramienta, necesitas al menos nmap y Gtk (juego de herramientas de Gimp). Los enlaces para esas herramientas son proporcionados en el sitio web de Nessus. Sin embargo, puesto que se lo puede usar desde la línea de comandos, Gtk no es obligatorio.

Nessus viene con diferentes utilidades (nasl, un lenguaje de script, nessus-adduser, nessus-build). Cada una de estas utilidades tiene su propia página de manual (man), tanto para el cliente como el servidor. Y si te hace falta, hay más documentación en el sitio web de Nessus.

Retomando el tema que comentaba más arriba, los pluggins son el "corazón" de Nessus. Lo que proveen son precisamente las pruebas de seguridad, esto significa descubrir una vulnerabilidad determinada. NASL (Nessus Attack Sripting Language) es un lenguaje recomendado para escribir pruebas de seguridad.

Imagina lo importante que son los pluggins para Nessus que de hecho, existen aproximadamente 20 familias de ellos. Algunos ejemplos de estas familias son: puertas traseras, denegación de servicio, lograr accesos root remotamente, etc. Obviamente, cada pluggin de cada familia, al ejecutarse, reporta la información encontrada, esto es, nos dice qué está incorrecto y qué deberíamos hacer para corregir el problema que se haya encontrado.

Y hablando de pluggins, simplemente es imposible pasar de largo sin nombrar a CVE (Common Vulnerabilities and

Exposures - Riesgos y Vulnerabilidades Comunes). Es una enorme base de datos de información disponible en http://cve.mitre.org. En este sitio podrás encontrar TODO, acerca de los riesgos de seguridad conocidos.

Opciones en la implementación

Cuando implementamos esta aplicación, resulta de mucha utilidad tener conocimiento sobre directivas de firewalls, enrutamiento y filtros. Se recomienda implementar Nessus de modo que tenga una buena conectividad IP con las redes que analiza. No es recomendable que se implemente detrás de un dispositivo NAT, a menos que se vaya a analizar una Red Interna.

Es muy importante recalcar que cuando se realice un análisis de vulnerabilidades mediante una NAT o un proxy de aplicación de algún tipo, la comprobación se puede distorsionar y producir un falso positivo o negativo. Además, si el sistema en el que se ejecuta Nessus posee firewalls personales o de escritorio, estas herramientas pueden limitar considerablemente la eficacia de un análisis de vulnerabilidades remoto.

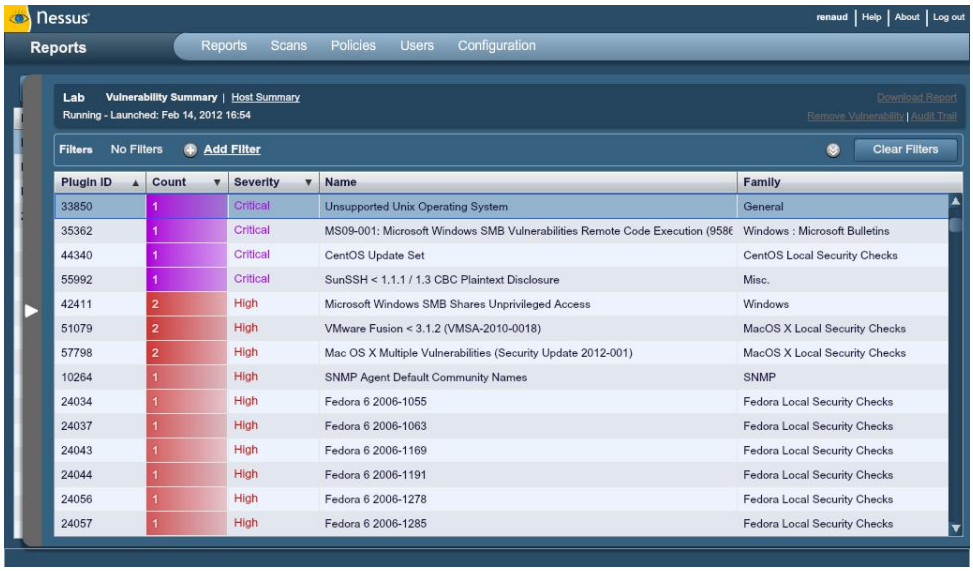
¿Costo?

En sí la aplicación es gratuita, pero, ¿qué hay de los pluggins? Todos los días los proveedores, los investigadores y demás fuentes publican numerosas vulnerabilidades nuevas. Tenable se esfuerza para que las comprobaciones de vulnerabilidades recientemente publicadas se prueben y se pongan a disposición de los usuarios a la mayor brevedad, normalmente dentro de las 24 horas de la divulgación. La comprobación de una vulnerabilidad específica tiene en el analizador Nessus la denominación “pluggin”. Una lista completa de todos ellos se encuentra disponible en http://www.nessus.org/plugins/index.php?view=all. En el caso de Nessus, Tenable distribuye los pluggins de vulnerabilidades más recientes en dos modos:

- ProfessionalFeed
- HomeFeed

Los pluggins se descargan directamente desde Tenable a través de un proceso automatizado de Nessus, en el cual verifica las firmas digitales de todas las descargas de pluggins para garantizar la integridad de los archivos. En el caso de las instalaciones de Nessus sin acceso a Internet, existe un proceso de actualización sin conexión que se puede usar para garantizar que el analizador permanezca actualizado.

¿Cuál es la diferencia entre Professional Feed y Home Feed?



- **Home Feed**.- Si vas a usar Nessus de forma doméstica, con fines no profesionales, puedes suscribirte a HomeFeed. Los usuarios recibirán de inmediato los nuevos pluggins correspondientes a las vulnerabilidades de seguridad más recientes. El uso de HomeFeed es gratuito. Sin embargo, existe una licencia independiente de HomeFeed cuyo cumplimiento debe aceptarse por parte de los usuarios. Para registrarse a fin de obtenerlo, visita http://www.nessus.org/register/ y registra tu copia de Nessus. Use el código de activación que reciba durante el proceso de registro al configurar Nessus para realizar actualizaciones. Los usuarios de HomeFeed no obtendrán acceso al Tenable Support Portal, a comprobaciones de compatibilidad ni a directivas de auditorías de contenido.

- **Professional Feed**.- Si usa Nessus con fines comerciales (por ejemplo, consultoría), en un entorno empresario o gubernamental, debe adquirir una ProfessionalFeed. Los usuarios de la misma recibirán de inmediato los nuevos pluggins correspondientes a las vulnerabilidades de seguridad más recientes. Los clientes de SecurityCenter se suscriben de manera automática y no deberán comprar una fuente adicional, a menos que tengan un analizador Nessus que no sea administrado por SecurityCenter.

Tenable proporciona asistencia comercial, mediante el Tenable Support Portal o por correo electrónico, a los clientes de ProfessionalFeed que usan Nessus, lo cual también incluye un conjunto de comprobaciones de compatibilidad basadas en hosts para Unix y Windows que son muy útiles para realizar auditorías de compatibilidad, tales como SOX, FISMA o FDCC.

Puedes adquirir una ProfessionalFeed a través de la tienda en línea de Tenable en https://store.tenable.com/ o por una orden de compra a través de Authorized ProfessionalFeed Partners (Socios Autorizados de ProfessionalFeed). Posteriormente recibirás un código de activación de Tenable. Este código se usará al configurar tu copia de Nessus para recibir actualizaciones

Como se pueden dar cuenta, Nessus es una herramienta que por sí sola es muy poderosa, pero si además la combinamos con otras herramientas de Seguridad Informática, aunque es difícil de creer, supera por mucho las expectativas de cualquier Pentester; y como ya lo dije antes, es imprescindible para los Administradores de Sistemas y Redes.

No puedo escribir más al respecto ya que la herramienta trae infinidad de pluggins, opciones, etc... pero les he dejado ya los links de su documentación para que, si les interesa, ustedes mismos revisen poco a poco la misma. En Internet se dice que ni con un libro completo se alcanzarían a ver todas las opciones, pluggins, etc, de esta herramienta; y es algo obvio, ya que está en constante actualización. Todos sabemos que en temas de informática siempre nos tenemos que estar actualizando, así que, a leer mucho y sobre todo, a practicar.

Rafael Murillo
twitter: @linxack & @itxpertsmx
Web: http://www.itxperts.mx
Blog: http://www.itxperts.mx/blog

Novedades sobre UEFI

POR **HERNÁN "HeCSa" SALTIEL**

En el artículo pasado describimos qué es UEFI, cómo funciona, cómo se está implementando, cómo coarta la libertad de sistemas operativos, y qué se está haciendo desde el lado de las comunidades y las empresas que basan sus modelos de negocio en el software libre para sortear los inconvenientes que esta tecnología conlleva. Veamos ahora qué hay de nuevo bajo el sol.

El anuncio

Hace pocos días la Linux Foundation hizo un anuncio interesante. Su “Technical Advisory Board” (algo así como su grupo de gobierno técnico) generó un plan para permitir que GNU/Linux y en cierta medida cualquier sistema operativo de código abierto, o diferente de Windoze 8, puedan ser cargados en máquinas que tengan tecnología UEFI, y Secure Boot habilitado. El anuncio vino de la mano de James Bottomley, uno de los más importantes y activos desarrolladores del kernel de nuestro querido sistema operativo.

En pocas palabras, lo que la Linux Foundation hará es obtener una llave de Microsoft y firmar un pequeño cargador de arranque, que cargará a la vez otro cargador sin verificación de firma de cargador, para finalmente cargar GNU/Linux u otro sistema operativo en las nuevas máquinas.

El cargador en cuestión utilizará la técnica “present-user” para asegurar que al ejecutar un sistema operativo instalado, un CD/DVD, o un LiveCD/LiveUSB, no se está tratando con un malware.

La Linux Foundation anunció que si bien el proceso de adquisición de una llave de Microsoft puede llevar un tiempo en ser adquirida, el “pre-bootloader” (así es como se llamará) en breve estará disponible en el sitio de esta entidad para ser descargado y utilizado por quien quiera.

Ahora bien, este plan suena muy bueno, pero tiene como contra que no agrega seguridad a lo que hoy en día utilizamos para ejecutar nuestros sistemas operativos libres. Por ende, parte del anuncio dice que si bien esta tecnología puede ser utilizada sin problemas, viene a cubrir un bache que hay en el tiempo necesario para que comunidades tales como las de Ubuntu, SuSe y Fedora lleguen a una verdadera solución gracias a los esfuerzos que están realizando en este sentido. En pocas palabras, es un paliativo, no una solución real.

Como era de esperarse, en la comunidad comenzó el ruido de fondo. Matthew Garrett, uno de los desarrolladores de “Shim”, la solución que Fedora considera, será la mejor, lanzó sus críticas hacia lo anunciado por la Linux Foundation. Nada a lo que no estemos acostumbrados. Creo que coincidirán conmigo en que es mucho mejor el debate que el silencio. Una solución bien discutida tendrá teóricamente mayor chance de éxito, o por lo menos, representatividad en la comunidad informática.

Por ejemplo, SuSe ya está implementando lo que llaman “Shim extension”, que básicamente es Shim, pero que deposita la verificación de las llaves en la base de datos MOK (“Machine Owner Keys”, o “Llaves del dueño de la máquina”), que puede ser actualizada por el usuario sin necesidad de acceder al UEFI. Suena bastante más interesante y evolucionada. Pero, sobre todo, demuestra investigación y esfuerzo para sortear problemas.

Claro está, Fedora embarró notablemente la teoría cuando se le preguntó por sus planes para los cada día más populares procesadores ARM. La respuesta por parte de su comunidad, que me recordó a otras que ya en el pasado fueron casi tomadas como una broma de mal gusto, fue que “el usuario debe preferir la compra de dispositivos que no tengan Secure Boot”. Por lo pronto, Fedora 18 asegura que soportará UEFI Secure Boot sobre plataformas Intel y AMD, una grata noticia.

Tecnológicamente hablando

Veamos algo de la tecnología asociada a esta solución.

Como primer punto, el “pre-bootloader” está diseñado para ser lo más pequeño posible. De esta forma, el trabajo duro continuará del lado del cargador de arranque real. Claro está, este cargador de arranque deberá estar instalado en la misma partición que el “pre-bootloader”, y contendrá un archivo binario llamado “loader.efi”, que podrá ser invocado desde cualquier otro cargador, y eso incluye al ya famosísimo Grub2, que muchos de nosotros estamos usando en este momento.

Es entonces que el “pre-bootloader” intentará ejecutar el archivo “loader.efi”, el cual de finalizar con éxito, permitirá el normal desempeño del resto del cargador de arranque que se esté utilizando.

Pero la ejecución de este archivo puede terminar bien, o con un error de seguridad. En este segundo caso, se solicitará al usuario una confirmación para continuar con el normal arranque del sistema operativo (por eso se llama a esta prueba “present user test”). De aceptarse, tal como en el caso anterior, el arranque continuará ejecutando “loader.efi” en modo inseguro, para luego seguir como antes mencioné.

Otra cosa que hará el “pre-bootloader” es verificar si la máquina se encuentra en “Setup Mode”, en cuyo caso pedirá al usuario permiso para cargar la firma digital de “loader.efi” en la base de datos de firmas autorizadas. Cuando se instale esta firma, el sistema operativo podrá ejecutarse sin que en el futuro se haga ningún tipo de “present user test”, aún cuando la plataforma se configure en modo “Secure Boot”.

Para los que tengan ganas de ver cómo funciona esto a nivel de código, pueden utilizar su cliente GIT favorito y dirigirlo a git://git.kernel.org/pub/scm/linux/kernel/git/jejb/efitools.git donde encontrarán los fuentes del programa “loader.c”, que tanto bien nos está haciendo.

Conclusión

Tanto en mi caso como en el de muchos otros usuarios y desarrolladores de soluciones de código abierto, la noticia sobre UEFI fue recibida como un trago agridulce. Viendo esfuerzos de este estilo, avivamos la nunca perdida esperanza, focalizándonos en hacer lo que siempre hemos hecho: liberar tecnologías para ser usadas por todo el mundo. Literalmente, todo el mundo.

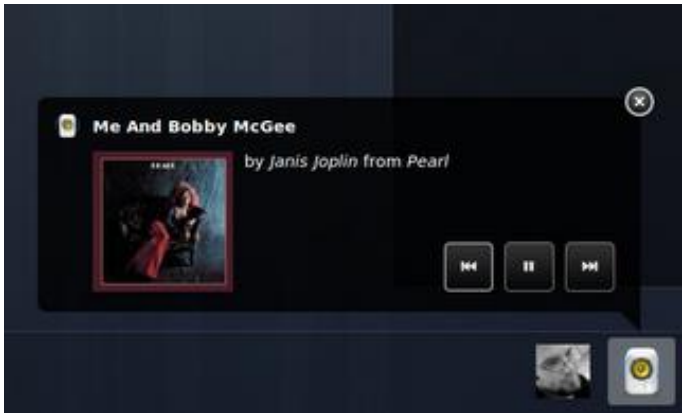
Efectivamente, era cuestión de tiempo

Hernán “HeCSa” Saltiel
AOSUG leader
CaFeLUG Member
hsaltiel@gmail.com
http://www.aosug.com.ar

GNOME 3.6
Un cambio necesario

POR **JUAN PABLO LOZANO**

Esta nueva versión de GNOME 3.6 trae muchas mejoras y evas características, entre las que podemos destacar: una bandeja de mensajes con un nuevo diseño, notificaciones más elegantes, el diseño de “Actividades” ha mejorado, nuevo diseño para “Archivos” (Nautilus) y una nueva pantalla de bloqueo. ¡Echemos un vistazo a lo que hay de nuevo!



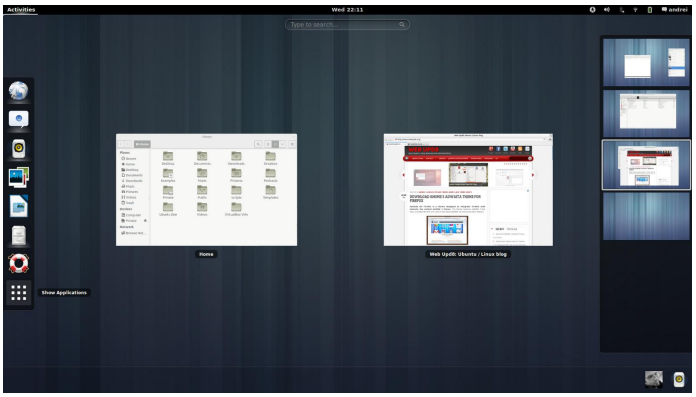
La bandeja de mensajes y notificaciones ha recibido algunos cambios importantes:

- Los mensajes de la bandeja y los elementos son más grandes, la esquina caliente ha sido sustituida por el borde inferior de la pantalla entera, también se puede acceder a las mismas a través de un atajo de teclado (Super + M).

- Las notificaciones son más inteligentes, más sensibles y más fáciles de descartar gracias a un botón de cierre.

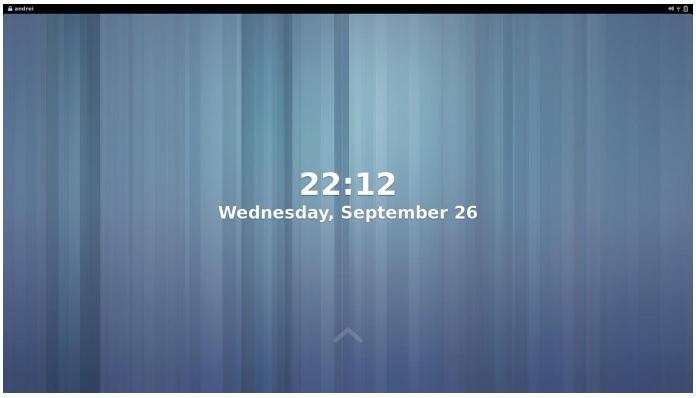
Otro cambio, tal vez no tan importante, pero que sin duda agradará a algunos usuarios, es que en el Menú de usuario de GNOME Shell el elemento de apagado está presente de forma predeterminada.

La sección de “Actividades” ha recibido algunos cambios importantes. En primer lugar, ahora al hacer clic en "Actividades" en la parte superior izquierda, se muestran las ventanas y para acceder a las aplicaciones se debe hacer clic en un “botón de rejilla” en la parte inferior del tablero, o escribiendo el nombre de la aplicación.



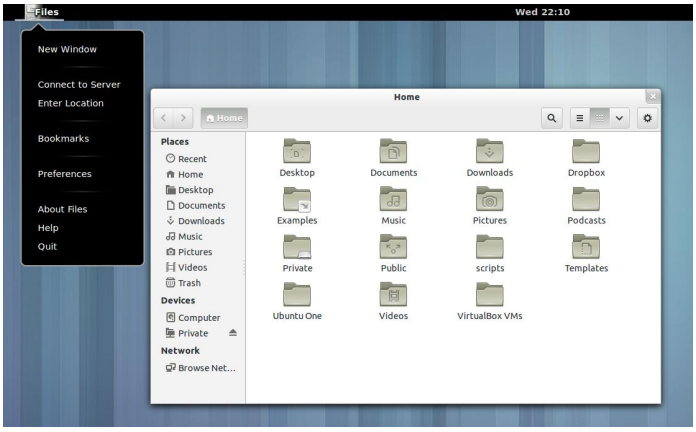
Otra gran novedad es una nueva pantalla de bloqueo (requiere el uso de GDM ya que si usted está utilizando Ubuntu 12.10 con LightDM en lugar de GDM, no podrá usar esta característica) que muestra la hora y la fecha

junto con las notificaciones. El usuario también tiene la capacidad de controlar la reproducción de medios de comunicación:



Aplicaciones de GNOME

Ahora un poco acerca de las aplicaciones de GNOME. **Archivos** (Nautilus) es la aplicación que ha recibido probablemente la mayor atención en GNOME 3.6. “Archivos” viene con una nueva interfaz de usuario que ahora es compatible con las otras aplicaciones de GNOME, pero hay algunas características eliminadas también, como el panel doble.



Los cambios en “Archivos” son:

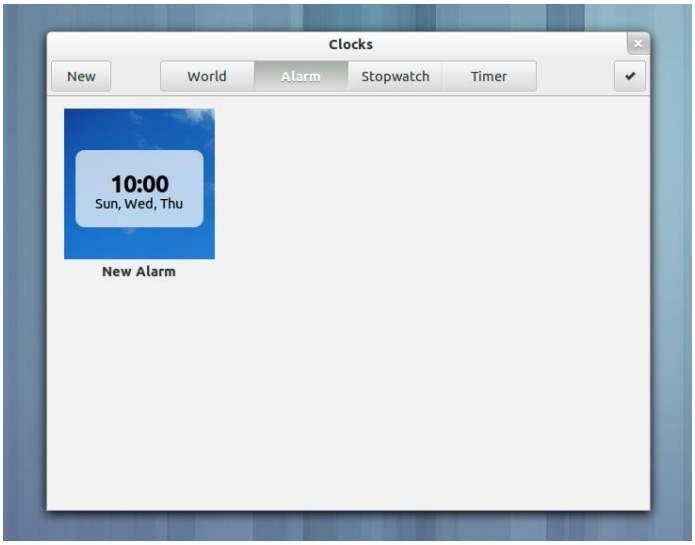
- una nueva forma de búsqueda de archivos ha sustituido tanto la vieja herramienta como la característica de "buscar mientras escribe".

- nueva barra de herramientas y de direcciones, menú de aplicación, un nuevo botón para el menú, íconos simbólicos para la barra lateral y una nueva sección "reciente" en esta barra lateral.

- cambios en la vista de lista: nueva pantalla de formato de fecha, mejor orden de las columnas y el nuevo tamaño de los iconos es de 32px.

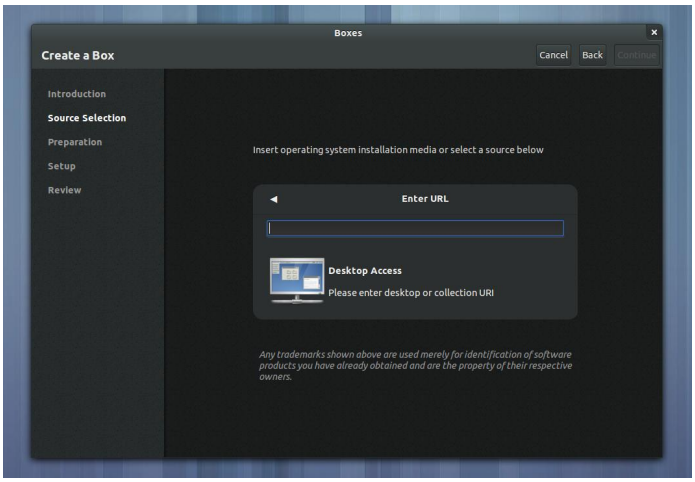
Relojes: es una nueva aplicación introducida como una "versión previa" ya que, de acuerdo con los desarrolladores de GNOME, no está lista para el primer lanzamiento por el momento.

Sin embargo ya es funcional y puede ser utilizada para mostrar la hora en todo el mundo, establecer una alarma, cronómetro y un temporizador:

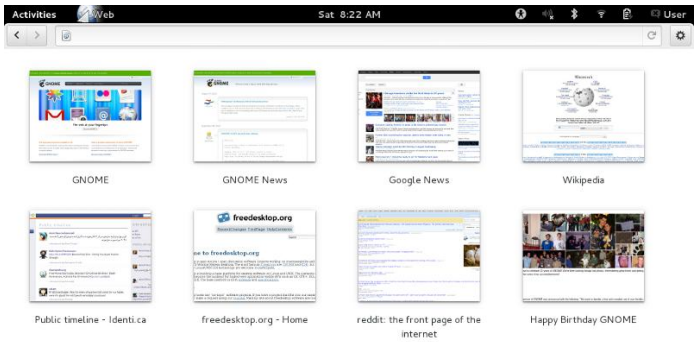


Cajas: introducida como una “versión previa” en GNOME 3.4, cajas (una aplicación para conectarse a máquinas remotas y administrar máquinas virtuales) es ahora oficialmente una aplicación de GNOME.

Los cambios en las últimas versiones incluyen un modo de selección trabajado, permiten personalizar un cuadro de memoria y tamaño de disco antes de que sea creado y mucho más:



Epiphany (Web): ha introducido "vista general" con la versión 3.6. Este es el comienzo de un nuevo diseño que debería mejorar la experiencia del usuario:



Por ahora "Vista General" no tiene la funcionalidad que se anunció hace un tiempo, y sólo presenta una cuadrícula con las páginas más visitadas. La nueva versión también viene con un modo de pantalla completa mejorada y otros cambios.

Por supuesto, hubo muchas otras mejoras, incluidos varios cambios para el analizador de uso de disco; discos; visor de fuentes; soporte para Microsoft Exchange; Windows Live y Facebook para cuentas en línea; cuadros de diálogo modales que ahora se expanden desde el centro en vez de dejar caer desde la parte superior; Empathy ahora utiliza Zeitgeist; la accesibilidad y la internacionalización de muchas mejoras.

También hay una nueva función que estoy seguro que a quienes les gusta personalizar su escritorio les encantará: con GNOME 3.6, las extensiones de GNOME Shell instaladas a través de extensions.gnome.org se actualizan automáticamente.

La próxima versión estable de GNOME, será la 3.8 y se espera para el 27 de marzo de 2013.

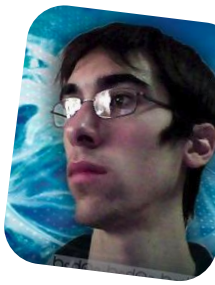
Si desean probar la versión 3.6 de GNOME, pueden hacerlo descargando Ubuntu, con la distribución “Ubuntu Gnome Remix” o desde la versión Alpha de Fedora 18.

Ubuntu Gnome Remix:

https://wiki.ubuntu.com/UbuntuGNOME/ReleaseNotes/12.10

Fedora 18 Alpha:

https://fedoraproject.org/get-prerelease



Lozano Juan Pablo
lozanotux@gmail.com
twitter: @lozanotux

HTC One X

El gran contrincante del S3 de Samsung

POR **ARIEL M. CORGATELLI**

Sin lugar a dudas el HTC One X es un duro competidor del Samsung Galaxy S3. En algunos puntos hasta es superior al mismo y en otros no tanto. Pasemos a detallar algunas de las funciones para lo cual parece haber sido creado. En primer lugar nos vamos a encontrar con un equipo muy compacto, de sólido diseño, gran potencia, excelente resolución en pantalla, como así también un acabado redondeado en toda su periferia.

Uno de las características que más me llamó la atención, y no es justamente ninguna relacionada a sus features, es el formato curvado desde el contorno hasta el mismo cristal de la pantalla. Este último punto hace que la misma pueda ser observada incluso desde un lateral a un ángulo de 25 grados.

Video revisión completa del Smartphone HTC: http://youtu.be/Rx1r8A_nrRg

Luego en lo que se refiere a características técnicas, no quiero entrar en muchos detalles ya que más abajo leerán con lujo de detalles cada una de ellas. Lo que sí no puedo dejar pasar por alto, es el gran potencial del micro quad-core, con el cual se pueden realizar tareas de forma casi automáticas, tomar fotos en cuestiones de milésimas de segundo, incluso sin darnos cuenta que la misma fue tomada.

En cuanto a la interfaz, está recontra pulida gracias a HTC Sense 4; la cual le brinda un acabado de funcionalidades excelentes para su correcto y simple funcionamiento. Sobre la cámara, un punto muy a favor luego de la pantalla, podemos decir que la misma se comporta como si fuera del tipo profesional, además desde su mismo menú podremos no sólo tomar fotos, sino también filmar, ya que no hace discriminación alguna pues hay un widget independiente para cada una de ellas.

Es decir abrimos la cámara y tenemos las dos opciones a la vista, tanto para tomar fotos como para filmar; y como si esto no fuera poco, podemos estar filmando en HD, y tomar fotos de forma simultánea sin salir de la filmación, además de poder acceder al zoom óptico y encender por ejemplo la lámpara (LED) que tiene junto a la cámara de 8mpx. Es decir podemos filmar sin luz natural y hacer zoom mientras registramos el video y además podemos sacar fotos al mismo instante.

Las opciones de ráfagas y panorámicas, sumadas a las configuraciones precargadas de la cámara hacen que la misma pueda trabajar de forma óptima para el más exigente fotógrafo.

Luego en lo que se refiere al software, encontraremos las opciones clásicas y las aplicaciones más comunes que se obtienen en cualquier equipo con Android 4.0.3 ICS; sumado a la interfaz HTC Sense, la cual le da un tono de

distinción al mismo. Por ejemplo una de las funciones Sense que más me gustaron fue la de recordar las últimas aplicaciones accedidas, en donde podremos movernos desde las mismas como si fuera una galería.

Haciendo un breve resumen de sus características antes de pasar por el detalle completo, podemos decir que: posee una pantalla HD 720p de 4.7 pulgadas con tecnología Gorilla Glass, procesador quad-core Tegra 3 a 1.5GHz, cámara de 8 megapixels con captura de video full HD, cámara frontal de 1.3 megapixels, Beats Audio, 1GB de RAM, 32GB de almacenamiento interno y corre Android 4.0 Ice Cream Sandwich con la interfaz de usuario Sense 4.0.

Y como si esto fuera poco, el equipo viene con una promoción excelente de la mano de Dropbox; con la cual se podrá acceder de forma gratuita a 25gb de espacio en tu cuenta por el término de 24 meses.

Detalles técnicos del equipo

- Display Tipo Super IPS LCD2 touchscreen capacitivo, 16M colores
- Tamaño 720 x 1280 pixels, 4.7 pulgadas
- Soporte multi-touch
- Pantalla Gorilla Glass
- Sensor acelerómetro para auto rotación
- Sensor de proximidad para auto apagado
- Sensor giroscópico
- Controles sensibles al tacto
- Interfaz de usuario HTC Sense v4.0
- Slot de tarjeta MicroSD - NO
- 32GB almacenamiento interno, 1GB RAM
- Procesador Nvidia Tegra 3 quad-core 1.5GHz, GPU ULP GeForce
- OS Android OS, v4.0 Ice Cream Sandwich
- Colores Gris, Blanco
- Cámara 8 MP, 3264x2448 pixels, autofocus, flash LED, geo-tagging, captura de video y fotos simultáneos, video 1080p@30fps stereo, cámara frontal 1.3MP 720p
- GPS con soporte A-GPS
- Brújula digital
- Tecnología Beats Audio
- EDGE - 3G HSDPA 21Mbps/ HSUPA 5.76Mbps
- Wi-Fi 802.11 a/b/g/n, DLNA; Wi-Fi Direct
- Bluetooth v4.0 A2DP
- NFC
- microUSB 2.0
- Cancelación activa de ruido con micrófono dedicado
- Integración Google Search, Maps, Gmail, YouTube, Google Talk, Picasa
- Integración con redes sociales
- Salida TV
- Manos libres incorporado
- Conector de audio 3.5 mm
- Batería Standard, Li-Po 1800 mAh
- Red GSM 850 / 900 / 1800 / 1900 - HSDPA 850 / 900 / 1900 / 2100
- Tamaño Dimensiones 134.4 x 69.9 x 8.9 mm
- Peso 130 g

Lo bueno del equipo

Sin lugar a dudas, la característica más importante es su pantalla, su potencia y su poder en cuanto al procesamiento de las imágenes capturadas. Otro punto muy importante para destacar, es la app "cars"; con la cual convertimos al smartphone en un completo GPS para nuestro auto, obviamente con acceso al móvil, música, etc.

Lo malo del equipo

El primer punto negativo que le pudimos encontrar se encuentra relacionado al registro del sonido cuando realizamos una filmación; el mismo no es de muy buena calidad y cuando la fuente de sonido es muy fuerte, el registro se termina saturando y entrecortando.

Luego otro punto en contra es la posibilidad de no poder insertar una tarjeta MicroSD, claro que con sus 32 GB de almacenamiento es más que suficiente, pero de cualquier manera no estaría nada mal tenerlo; y por último, el no contar con un botón físico desde su parte frontal para activar el dispositivo, algo que se soluciona cuando accedemos al botón superior de encendido.

Puntuación

8,5 sobre 10

Información adicional y valores en el mercado

Pueden encontrar mucha más información del modelo desde la web oficial de HTC España, en donde a su vez podrán encontrar vídeos detallando las diferentes funciones.

http://www.htc.com/es/smartphones/htc-one-x/

Conclusión personal del equipo.

La experiencia total con el equipo fue completamente excelente, el mismo se comportó muy bien en todo el tiempo que lo tuvimos a prueba; pudimos hacer uso del mismo como cámara principal para la cobertura de eventos; además poder registrar vídeos, escribir informes y mantenernos comunicados como si fuera una tableta + una cámara profesional. Si tendría que recomendar el equipo, no dudaría ni un minuto en hacerlo, ya que es un excelente smartphone.

Ariel M. Corgatelli
twitter: @arielmcorg

(*)

(*) Únete a "Radio Geek", nuestro podcast diario de actualidad tecnológica
http://radiogeek.ivoox.com

Universo Tuquito

TuquiGRUB

POR **PATRICIO PRIETO GARAY**

GNU/Linux Tuquito es una distribución nacida en la provincia de Tucumán, Argentina, y cuenta con una serie de programas tales como Garfio, Aptito o el Gestor de Programas que fueron generados por el equipo de trabajo de la distro buscando mejorar la experiencia del usuario y especialmente pensadas para quienes se inician en el uso del software libre. En esta ocasión les presentamos TuquiGRUB.

¿Qué es el Grub?

GNU GRUB (GNU GRand Unified Bootloader) es un gestor de arranque múltiple, desarrollado por el proyecto GNU que se usa comúnmente para iniciar uno, dos o más sistemas operativos instalados en un mismo equipo. Es utilizado principalmente en sistemas operativos GNU/Linux.

Recuperando el menú de arranque de GNU/Linux

TuquiGrub nace de la necesidad de restaurar el menú del grub, que se encuentra en el sector cero del disco rígido de la computadora, también conocido como MBR (Master Boot Record).

Siempre se ha dicho que se puede instalar Linux en la computadora junto a Windows, al instalar tu distribución favorita. Durante el proceso de instalación se genera un menú que es guardado en el MBR (la primera parte de tan sólo 512 bytes) el cual permite que al encender la computadora puedas elegir el sistema operativo a utilizar en esa sesión. Hasta acá todo como siempre, entonces....

¿Qué es TuquiGrub y para qué sirve?

Cuando en nuestra compu tenemos Windows y GNU/Linux y por alguna razón debemos reinstalar Windows, el instalador de Win elimina los datos existentes en el MBR y hace un acceso al sistema de la ventanita. La próxima vez que inicie su computadora notará que ha desaparecido el menú del Grub, afortunadamente no borra la partición de Linux por lo tanto lo único que se debe reparar es el menú del Grub. Para los menos expertos esto era un dolor de cabeza y para recuperar su linux reinstalaban el mismo, con resultados adversos al perder los sistemas instalados y los datos guardados en el mismo. Los expertos realizaban montajes de discos y asignación de unidades temporales para poder recuperar el grub perdido.

TuquiGRUB puede recuperar el menú del Grub eliminado, de esta forma es más sencillo para los usuarios expertos como los novatos.

Con sólo arrancar la compu desde un LiveCD de Linux e instalando el TuquiGrub, puede recuperar en pocos pasos el menú del Grub.

La instalación del programa se hace sobre un disco virtual, es decir que para la tranquilidad del usuario, los datos NO SE BORRAN.

En el próximo reinicio del sistema notará que se ha recuperado el menú del grub, puede ser que se pierdan los efectos gráficos, por tratarse de un programa genérico, sin embargo se puede recuperar ejecutando el

comando sudo update-grub2 para volver al estado anterior del grub, como los gráficos y diseños de la distro instalada.

TuquiGrub puede ser instalado en debian, ubuntu, red hat y derivados de estos.

A partir de la versión final de Tuquito 6, TuquiGRUB pertenece a los paquetes en los repositorios oficiales de GNU/Linux Tuquito.

Algunas aclaraciones

Es recomendable ejecutar Tuquigrub desde un live cd de tu distro basada en debian/red hat, la partición linux no debe estar montada y por eso se necesita un acceso desde un live-cd.

La contraseña del superusuario (root o administrador) puede ser una palabra vacía, si no verifique en la página de la distro.

Debe tener conocimientos de las particiones que genera linux, manejar el gparted o algún programa de particiones con resultados satisfactorios.

Para más detalles vea el Manual del usuario de TuquiGrub, al final de la nota encontrará los enlaces.

Desarrollo y Calidad

TuquiGRUB fue desarrollado por Patricio Prieto Garay junto a la colaboración de Mario Colque, ambos miembros del Tuquito Team! en el mes de julio de 2012. El desarrollo y la calidad del programa se realizó via web, contando con la colaboración de personas de distintos lugares de la Argentina, por ejemplo Débora Badilla de Neuquén (Tuquito Team!), Mario de Tucumán (Salteño de nacimiento) y quien escribe del Partido de La Costa, Pcia de Buenos Aires; y colaboradores miembros del Tuquito Social como Nestor Lugo de Berisso, Provincia de Buenos Aires y al resto de los integrantes del social que han aportado y reportado los errores del sistema.

Enlaces y fuentes:

MBR:
http://es.wikipedia.org/wiki/Registro_de_arranque_principal

Manual del usuario de TuquiGrub:
http://api.ning.com/files/pFaL6m*Zw5KvdJbWXQQdv0jp-STOYV4w46XKMKfb7lACi0zAusJLuBSKwa0v16mjpc8z4kAXqXkWpEedUZ9nBuGm6BjA*3Vg/manualTuquiGrub.pdf

Tuquito:
http://www.tuquito.org.ar

Tuquito Team!
http://www.tuquito.org.ar/team.html

Tuquito Social
http://social.tuquito.org.ar

Grub
http://es.wikipedia.org/wiki/GNU_GRUB

Patricio Prieto Garay
Tuquito Team
patriciosprieto@tuquito.org.ar

La curiosidad mató al gato

POR **HERNÁN "HeCSa" SALTIEL**

Algunos de los más “nerds”, como es mi caso, habrán seguido con mucho interés las tareas que estuvo desarrollando la unidad robotizada “Curiosity” en su expedición sobre suelo marciano.

Efectivamente, el pasado 6 de agosto de 2012 amanecimos con la grata sorpresa de saber que este dispositivo tecnológicamente muy avanzado había pisado terreno marciano y que, a pesar de requerir un pequeño ajuste en su software (para los detractores del teletrabajo, esto se hizo, lógicamente, en forma remota), ya comenzaba a emitir datos de este planeta.

La pregunta de rigor que los lectores se estarán haciendo es: ¿qué tiene ésto que ver con el código abierto? Pues bien: mucho, mis queridos pingüinos... mucho.

Crónicas marcianas

Una de las cosas que el vehículo marciano Curiosity debía hacer era enviar a nuestro planeta enormes cantidades de información. Tengamos en cuenta que no es sencillo o barato enviar un aparato como éste a un sitio tan lejano, por lo que todo el proceso de recolección, codificación, envío, recepción, decodificación y distribución debía funcionar a la perfección para que la inversión esté justificada.

Claro está, la comunidad científica es bastante grande. Muchas expectativas se pusieron en esta expedición, y por lo tanto, muchas personas esperaban ansiosas las imágenes que llegaban.

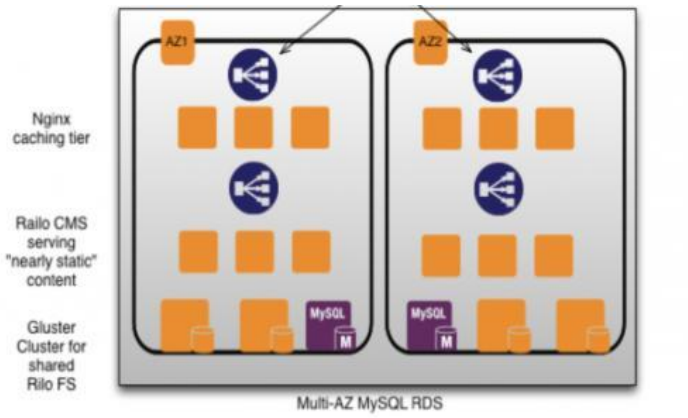
¿Cómo distribuimos imágenes cuando hay millones de personas en el mundo esperando por ellas, presionando F5 en su navegador varias veces por segundo?

En un primer momento, Curiosity envió imágenes de relativamente baja resolución, sólo 1200x1200 pixeles. Luego se le realizó en forma remota (y por suerte para nosotros, exitosa) una actualización de su software, gracias al cual comenzó a enviar archivos notablemente mejor definidos, y por ende más grandes.

Y lo que es mejor, esta información estuvo siempre disponible en cada punto del mundo donde fue solicitada. Eso significó un tráfico de cientos de gigabytes por segundo a cientos de miles de pedidos concurrentes alrededor del mundo.

La NASA decidió que lo mejor que podían hacer era usar una tecnología que ellos mismos en algún momento ayudaron a construir, y que es ni más ni menos que el concepto de nube. Contrataron Amazon Web Services (AWS), empresa gracias a la cual NASA/JPL (JPL es la sigla de la división “Jet Propulsion Laboratory”) pudo diseñar, construir, probar y desplegar sus propias soluciones de alojamiento web y streaming en vivo de video en sólo algunas semanas de arduo trabajo.

Un esquema de la solución implementada es el siguiente:



Como podemos observar, hay varias tecnologías de código abierto que se han utilizado para poder brindar este servicio. Entre ellas tenemos las siguientes:

- Nginx: Un servidor http rapidísimo, así como un proxy reverso. Sitios como NetFlix, Zinga, o GitHub hacen uso de este servidor web.

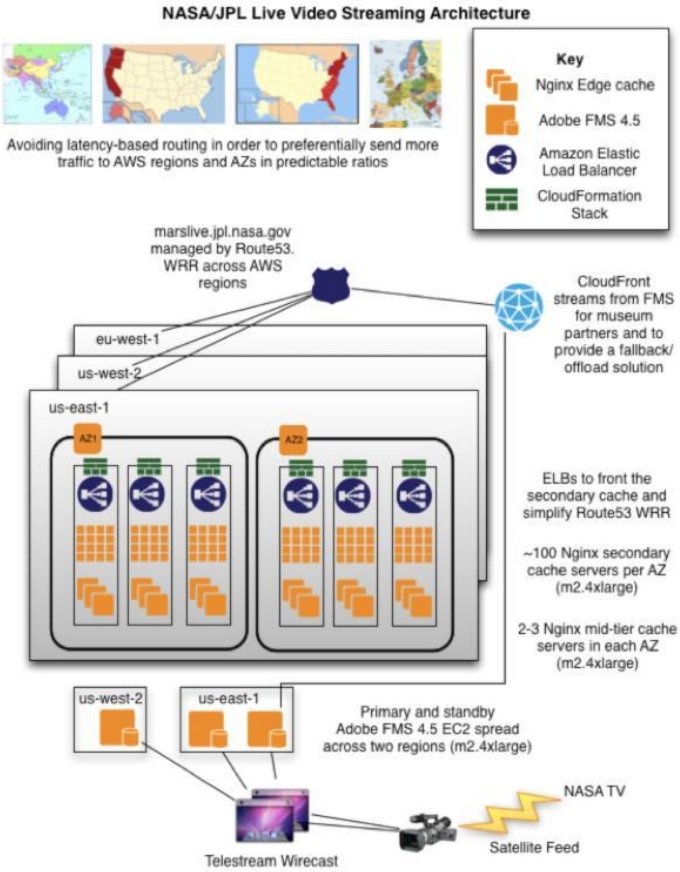
Se configuraron varias AZ ("Availability Zones" de Amazon, o zonas de disponibilidad) desplegando en cada una de ellas 2 ó 3 Nginx para servir como caché de capa media.

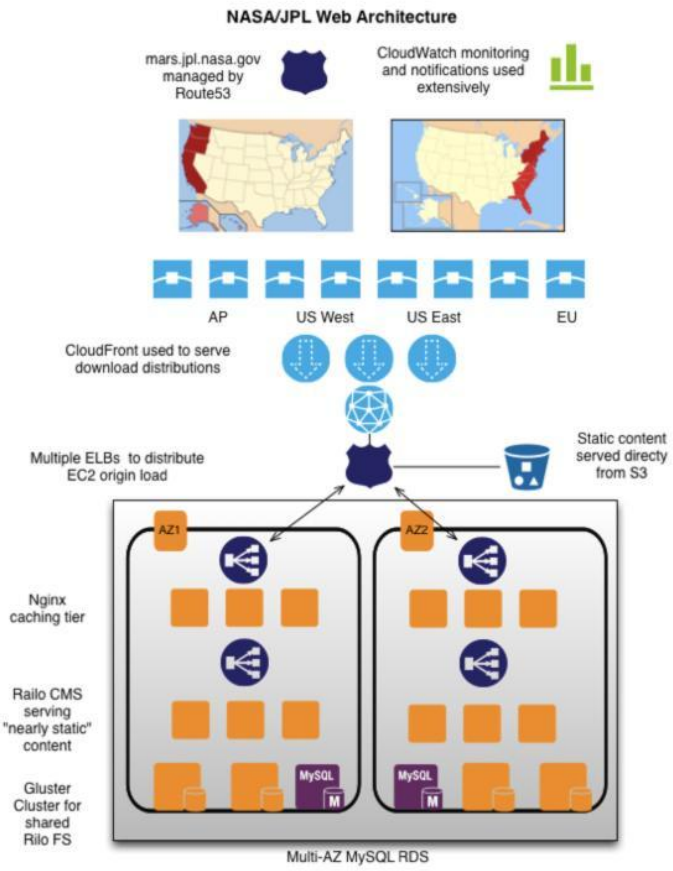
En cada AZ se implementaron 100 Nginx como servidores caché secundarios.

- Railo CMS: Un framework de desarrollo de aplicaciones de código abierto famoso por haber implementado el lenguaje CFML ("ColdFusion Markup Language"), y por ser parte del proyecto JBoss.org (sí, de la versión comunitaria, la corporativa está varios kilómetros atrás de la mayoría de los servidores de aplicaciones comerciales y libres).

- GlusterFS: Es un sistema de archivos distribuido entre varias máquinas, que permite su uso en soluciones de diversa índole. Ha sido adquirido por Red Hat, si bien las "malas lenguas" dicen que para este caso se debió continuar con el uso de la versión comunitaria. Punto para el código 100% abierto. Entre los sitios conocidos que hacen uso de esta tecnología encontramos a la gran cadena de radio en línea, Pandora.

- MySQL RDS: Es el famoso motor de bases de datos relacionales MySQL, pero con una configuración especial. En este caso, se utilizó una topología Multi-AZ, que permite la rápida replicación de datos entre instancias de bases de datos, alivianando la labor de las soluciones de un único nodo, así como asegurando que si un sistema activo sufre alguna caída, su replicación ya ocurrió y se puede continuar con la sesión en curso en otro.





Claro que sería injusto si quisiera mencionar sólo las soluciones de código abierto, dejando de lado las privativas. Muchas tecnologías privativas se utilizaron en la implementación de esta solución, tales como Adobe Flash Media Server, Amazon Elastic Compute Cloud, Elastic Load Balancer, Amazon Route 53, y Amazon CloudFront. Pero de ellas hablarán las personas que las representan, que claramente no es mi (nuestro) caso.

Espero que estos temas les gusten tanto como a mí. ¡Nos leemos en un mes!

Hernán "HeCSa" Saltiel
AOSUG leader
CaFeLUG Member
hsaltiel@gmail.com
http://www.aosug.com.ar

Síguenos también en Facebook

Me gusta

La esperanza del desbloqueo

POR **CLAUDIO DE BRASI**

Un caso que se dio recientemente en Argentina es sobre la disposición de un Juez acerca de bloqueo de páginas Web que se referían al tema del desbloqueo de las Netbooks de los planes "Conectar Igualdad" y el "Plan Sarmiento".

Como siempre ocurre con estas medidas de bloqueo de las direcciones Web. Ni bien se bloquearon los sitios, otros usuarios que habían copiado la información, lo replicaron en varios lugares más. No llevó más de 5 minutos encontrar toda la información que se quiso ocultar. Demostrando lo lento e ineficiente de tomar medidas de censura tradicional sobre las tecnologías modernas y el obvio desconocimiento de las mismas.

Las voces que proclamaban por este bloqueo de información decían que era para evitar la manipulación de equipos, la malversación de los mismos, la posibilidad de ser usados por personas a las que no debía destinarse los mismos, hasta alguien dijo que era una violación de acceso no autorizada a los sistemas. Algunas son comprensibles, otras exageradas. Pero lo interesante del punto es que los chicos hicieron estos vídeos e instructivos.

Los chicos no quieren límites. Que el equipo se bloquee después de un periodo de 15 días a 3 meses es un incordio para ellos que les trae más molestias innecesarias. Los vídeos e instructivos muestran cómo con 2 destornilladores un poco de tiempo y luego algunas modificaciones mínimas en el hardware y/o en el software se puede desbloquear el equipo.

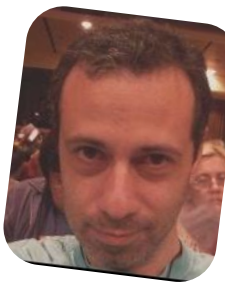
Para alguien que sabe un poco más que lo básico de electrónica, que los chicos hayan hecho estas modificaciones sin elementos de descarga electrostática, (ESD), es de terror. Podrían fácilmente haber “quemado” el System Board del equipo. (El repuesto vale casi un tercio del valor total del equipo).

Pero en medio de la discusión sobre la legalidad del bloqueo de Web o del bloqueo de los equipos, algo me dio una esperanza muy gratificante. Los chicos NO QUIEREN LIMITES. Pero no sólo ello. Vieron el problema, buscaron cómo solucionarlo por cuenta propia y luego difundieron ese conocimiento sin esperar más que sólo un comentario de agradecimiento. Todo un comportamiento del más puro altruismo Hacker, (En el correcto sentido de la palabra), que comparte con la filosofía del software libre.

El día de mañana, estos chicos van a ver los problemas que presenta el software privativo de esos equipos y otra vez buscarán una solución. Así que en un tiempo, terminaran descartando el sistema operativo privativo para poder seguir usando su equipo. (Allí está mi esperanza).

Si ven a algún mayor que usa un equipo destinado a los chicos, que no sea docente o alguien relacionado con el que la debería usar, se lo debería encarar a él en forma legal para que explique por qué usa un equipo en forma indebida. Pero perseguir a los menores por difundir cómo solucionar un problema para ellos es casi una contradicción de lo que se espera de ellos, que estén listos para los problemas del futuro y que puedan solucionarlos.

Claudio De Brasi
twitter: @doldraug



PD: Sres y Sras Mayores, Comprendan a los menores, atiendan sus reclamos. Porque si los ignoran o los prohíben se van a ver sobrepasados.

Privacidad
en Internet
¿realmente es posible?

POR **JOSE MARÍA SCHENONE**

Cada vez es más común enterarnos por la radio, televisión o diarios sobre violaciones a la privacidad de famosos (y no tan famosos también) de los que se filtran fotos y/o videos no autorizados, mensajes de texto, o información privada de cualquier tipo.

Ya es casi normal que esto suceda, y la verdad es que pocos hacen algo al respecto para solucionarlo.

Ahora, alguien realmente se preguntó ¿cómo y por qué sucede esto?

Con el gigantesco avance tecnológico en el que estamos sumergidos, es moneda corriente ver a personas disfrutando de sus smartphones a toda hora y en cualquier lugar. Publican mensajes en las redes sociales, toman y comparten fotos, descubren y marcan lugares; todo esto navegando desde puntos de acceso wireless pseudo gratuitos. Éstas son actividades ya normales en nuestras vidas.

Pero no creamos que sólo le sucede a los usuarios de un smartphone, cualquier persona conectada a internet por medio de una computadora cae también en esta problemática.

¿Pero qué tiene de malo todo esto?

En realidad nada, salvo que estamos exponiendo nuestros datos personales, ¡datos que deberían ser privados! (Salvo que deseemos compartir todo con todos).

El primer factor por el que suceden estas cosas es la desinformación o falta de educación por parte de los usuarios sobre lo importantes que son los datos personales o laborales. Actualmente la información de los usuarios conectados a internet es uno de los activos que mejor cotizan económicamente; e increíblemente pocos son los que tratan de protegerlos como es debido.

Si realizamos una encuesta entre nuestros familiares, compañeros de estudio o trabajo sobre si saben qué tan expuestos están al utilizar internet, seguramente se alarmarán de las respuestas que pueden llegar a recibir.

Tampoco es que hay que volverse paranoico al extremo de no utilizar más internet o smartphones, porque no es la solución. Éstas son herramientas que sabiendo utilizarlas mejoran nuestra calidad de vida. Una técnica muy efectiva para los delincuentes durante la época de vacaciones es la utilización de internet para buscar información (también denominada footprinting) de sus nuevas víctimas.

Veamos un ejemplo para entenderlo mejor

Tenemos a nuestro querido Miguel X, que es un importante gerente de una empresa textil. Miguel además es un excelente esposo de Victoria y padre de dos hermosos hijos, María y Julián.

Miguel y su familia están planificando sus próximas vacaciones utilizando internet. Luego de unas horas todos acuerdan irse a recorrer las costas Argentinas. Es tal la felicidad que tienen todos, que María y Julián

escriben en sus redes sociales que se van a la playa. Victoria publica en su Facebook que necesita comprarse ropa para los 20 días que estarán de vacaciones. Por último, Miguel X publica en su cuenta de Twitter @MiguelX que el 20 de noviembre se toma unos días de descanso. Con toda esta información, un delincuente ya tiene una nueva posible víctima.

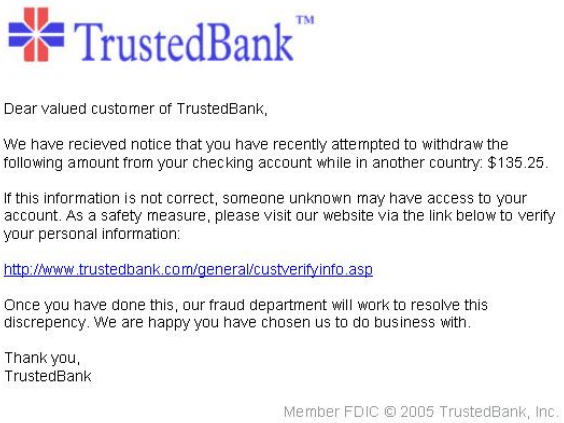
Lo primero que hace el malhechor es buscar en la guía telefónica (también disponible en internet) si la dirección de MiguelX figura en ella. En caso de encontrar la dirección queda hacer un pequeño trabajo de inteligencia por el barrio para validar que Miguel X es gerente de una empresa y esta casado con Victoria y es padre de María y Julián.

No hay que ser muy inteligente para darse cuenta que nuestro delincuente ya sabe que a partir del 20 de noviembre y hasta el 9 de diciembre la casa estará vacía y la familia de Miguel se encontrará a muchos kilómetros de distancia. Todo esto fue posible porque Miguel, Victoria, María y Julián expusieron información sensible.

Otra técnica muy efectiva es la “ingeniería social”, por la cual es muy simple obtener información confidencial. La ingeniería social es una técnica que utilizan muchas personas, como investigadores privados, criminales, o crackers, para obtener información privada o confidencial, acceso o privilegios en sistemas informáticos de forma que les permitan realizar algún acto que perjudique o exponga a la persona, empresa u organismo comprometido.

El principio que sustenta la ingeniería social es que en cualquier sistema "los usuarios son el eslabón más débil de la seguridad".

En la práctica, un ingeniero social usará comúnmente el teléfono o internet para engañar a la gente, fingiendo ser, por ejemplo, un empleado de algún banco o alguna otra empresa, un compañero de trabajo, un técnico o un cliente. El criminal utilizará un sitio web o el envío masivo de correos electrónicos, para invitarnos a renovar una contraseña que ha caducado, o para activar un nuevo servicio de homebanking, consiguiendo así que el usuario revele información sensible, o viole las políticas de seguridad a veces inexistentes.


TrustedBank™

Dear valued customer of TrustedBank,

We have recieved notice that you have recently attempted to withdraw the following amount from your checking account while in another country: $135.25.

If this information is not correct, someone unknown may have access to your account. As a safety measure, please visit our website via the link below to verify your personal information:

http://www.trustedbank.com/general/custverifyinfo.asp

Once you have done this, our fraud department will work to resolve this discrepency. We are happy you have chosen us to do business with.

Thank you,
TrustedBank

Member FDIC © 2005 TrustedBank, Inc.

Correo electrónico falso del TrustedBank

Con estos métodos, los ingenieros sociales aprovechan la tendencia natural de la gente a reaccionar de manera predecible en ciertas situaciones, por ejemplo proporcionando detalles financieros a un aparente empleado de un banco.

Aquellos que utilizan Internet frecuentemente, reciben mensajes que solicitan contraseñas o información de tarjeta de crédito, con el motivo de "crear una cuenta", "reactivar una configuración", u otra operación; a este tipo de ataques se los llama **phishing** (pesca).

Un ejemplo muy actual de un ataque de ingeniería social, es el uso de archivos adjuntos en los correos electrónicos, ofreciendo, por ejemplo, fotos "íntimas" de alguna persona famosa o algún programa "gratuito". Estos correos, aparentemente provienen de alguna persona que conocemos. Al abrir estos archivos adjuntos estamos permitiendo que se ejecute código malicioso (por ejemplo, tomar el control de nuestra máquina en donde se activa la webcam y se comienza a grabar todo lo que hacemos).

La ingeniería social también se aplica al acto de manipulación cara a cara para obtener acceso a los sistemas. La principal defensa contra la ingeniería social es la capacitación y entrenamiento de los usuarios, en la implementación de políticas de seguridad y en ser más precavidos al momento de compartir información en las redes sociales.

Uno de los ingenieros sociales más famosos de los últimos tiempos es **Kevin Mitnick** a quien pueden seguir en su cuenta de Twitter https://twitter.com/kevinmitnick. Según su opinión, la ingeniería social se basa en estos cuatro principios:

1. Todos queremos ayudar.
2. El primer movimiento es siempre de confianza hacia el otro.
3. No nos gusta decir “No”.
4. A todos nos gusta que nos alaben.

A continuación comparto con ustedes algunos de los engaños más conocidos para que a partir de ahora estemos más prevenidos.

La Estafa nigeriana

La estafa nigeriana, timo nigeriano o timo 419, es un fraude, un engaño. Se lleva a cabo principalmente por correo electrónico no solicitado. Adquiere su nombre del número de artículo del código penal de Nigeria que viola, ya que buena parte de estas estafas provienen de ese país.

Esta estafa consiste en ilusionar a la víctima con una fortuna inexistente y persuadirla para que pague una suma de dinero por adelantado, como condición para acceder a la supuesta fortuna. Las sumas solicitadas son bastante elevadas, pero insignificantes comparadas con el monto que las víctimas esperan recibir.

Variantes

Existen numerosas variantes de la estafa. Las más comunes son una herencia vacante que la víctima adquirirá, una cuenta bancaria abandonada, una lotería que la víctima ha ganado, un contrato de obra pública o simplemente una gran fortuna que alguien desea donar generosamente antes de morir. Algunos sostienen que la excusa de la lotería es la más común de todas.

Por ejemplo, la víctima podría recibir un mensaje del tipo "Soy una persona muy rica que reside en Nigeria y necesito trasladar una suma importante al extranjero con discreción. ¿Sería posible utilizar su cuenta bancaria?". Las sumas normalmente suelen estar cerca de decenas de millones de dólares. A la víctima se le promete un determinado porcentaje, como el 10 o el 20 por ciento.

El trato propuesto se suele presentar como un delito de guante blanco inocuo con el fin de disuadir a las víctimas -los supuestos inversionistas- de llamar a las autoridades. Los timadores enviarán algunos documentos con sellos y firmas con aspecto oficial, normalmente archivos gráficos adjuntados a mensajes de correo electrónico, a quien acepte la oferta.

A medida que prosiga el intercambio, se pide a la víctima que envíe dinero, con la excusa de supuestos honorarios, gastos, sobornos, impuestos o comisiones. Se va creando una sucesión de excusas de todo tipo, pero siempre se mantiene la promesa del traspaso de una cantidad millonaria. A menudo se ejerce presión psicológica, por ejemplo alegando que la parte nigeriana tendría que vender todas sus pertenencias y pedir un préstamo para poder pagar algunos gastos y sobornos. A veces, se invita a la víctima a viajar a determinados países africanos, entre ellos Nigeria y Sudáfrica. Esto es especialmente peligroso, porque en ocasiones el supuesto inversor puede acabar secuestrado o incluso asesinado por el timador.

En cualquier caso, la transferencia nunca llega, pues las millonarias sumas de dinero jamás han existido.

Las operaciones están organizadas con gran profesionalidad en países como Nigeria, Sierra Leona, Costa de Marfil, Ghana, Togo, Benín y Sudáfrica. Cuentan con oficinas, números de fax, teléfonos celulares y a veces con sitios fraudulentos en internet.

Últimamente, gran cantidad de estafadores provenientes del África Occidental se han establecido en diversas ciudades europeas, especialmente Ámsterdam, Londres, Madrid, etc, como también en Dubái. A menudo se persuade a las víctimas a viajar allí para cobrar sus millones.

José María Schenone
twitter: @joseschenone
Consultor en Seguridad y Sistemas GNU/Linux
http://www.joseschenone.com.ar

Linux Containers

POR **MARCELO GUAZZARDO**

Esta es otra tecnología de virtualización, que ya viene nativa en el kernel, y podría ser como una evolución de OpenVZ. La diferencia con OpenVZ es que openvz necesita un kernel especial para funcionar, en cambio LXC (Linux Containers) no.

La verdad es que para levantar proyectos que querramos aislar, como puede ser un lamp, o un desarrollo que queremos aislar de la máquina principal (Host), es sorprendente lo bien que anda.

Si bien no es virtualización propiamente dicha, podemos correr otros Linux dentro de los contenedores (Debemos usar los templates, ya existen templates de Ubuntu, Fedora, y Debian). En el caso de Debian, el template que se usa, es un debootstrap, dentro de una jaula chroot.

Para hacer una analogía, esto es similar a las Jails de BSD, y a las zonas de Solaris. Fíjense que en las zonas de Solaris, no se necesita correr otro kernel para poder Instalarlas.

Ventajas de esta tecnología:

Se pueden levantar muchas máquinas contenedoras usando muy poca memoria

No hace falta para correr un OS de 64 bits, contar con la tecnología AMD V o Intel VT.

Desventajas:

No tiene (Al menos por ahora), una administración gráfica como Virtualbox, Vmware, o HyperV.

(Se dice que se puede conectar con virt-manager, debería probarlo)

Se pueden correr desde templates de containers las vm's, se necesita un conocimiento más amplio para armar un propio template si quisiéramos hacer un deployment.

Bueno, hecha la introducción, manos a la obra.

Nota: Esta demo, está basada en Debian Squeeze.

En el host:

Vamos a necesitar instalar las userspace tools de lxc (Ya que a nivel Kernel no necesitamos nada), y el debootstrap (Para los que no saben el debootstrap es un mini sistema Debian bajado en una jaula chroot).

Luego, yo quiero que mi máquina guest (Mi sistema operativo que correrá dentro del contenedor), tome IP de un dhcp, entonces, le voy a tener que asignar un placa en modo bridge al host.

Esto se realiza haciendo el siguiente cambio en el /etc/network/interfaces:

Nota: Yo voy a hacer bridge por la interfaz eth0.

```
auto lo
iface lo inet loopback
auto br0
iface br0 inet static
        bridge_ports eth0
        address 192.168.0.10
        broadcast 192.168.0.255
        netmask 255.255.255.0
        gateway 192.168.0.1
```

Y a la vez, nuestra máquina HOST, recibe DHCP del Servidor 192.168.0.1. Nuestra máquina contenedora se va a conectar por el HOST al dhcp 192.168.0.1, y va a tomar una ip de ese rango.

Comenzando:

```
apt-get install bridge-utils libvirt-bin
debootstrap lxc
```

Luego, es importante montar el cgroups. Esto es una nueva característica del kernel para poder manejar mejor los recursos de nuestro hardware, pero no será explicado aquí.

```
echo "cgroup                  /sys/fs/cgroup
cgroup  defaults        0       0

" >> /etc/fstab
```

Lo agregamos al fstab, y luego, para que lo monte, tipeamos

```
mount -a
```

Creando el template de instalación de Squeeze:

Para crear el template de instalación de Squeeze, vamos a modificar uno que ya está dentro de las herramientas de UserSpace de LXC, pero que le vamos a cambiar, por que ese era para LENNY. Haremos algunos cambios para que quede para squeeze. Básicamente, vamos a establecer que la arquitectura sea Squeeze en vez de Lenny, que el cliente de DHCP ha cambiado el nombre

```
cd /usr/lib/lxc/templates

sed s/lenny/squeeze/g lxc-debian > /tmp/squeeze

sed s/dhcp-client/isc-dhcp-client/g
/tmp/squeeze > lxc-squeeze
```

Luego, deberíamos si queremos, desactivar las ttys 4,5,6 en el inittab.

Vamos a generar nuestro primer contenedor:

```
lxc-create -n myfirstcontainer -t squeeze
```

Con esto generamos el contenedor, usando el template de squeeze.

Una vez que generamos el contenedor, vamos a ver dentro del directorio, dos ficheros. Un fichero config, y un directorio rootfs, que es la jaula chroot.

En el fichero config, vamos a configurar la red, para que salga como un cliente DHCP, a través de la placa en modo bridge del host.

Les muestro como quedó mi configuración:

```
lxc.tty = 4
lxc.pts = 1024
lxc.rootfs =
/var/lib/lxc/myfirstcontainer/rootfs  ## Aca es
donde va a tomar la Jaula
lxc.cgroup.devices.deny = a
# /dev/null and zero
lxc.cgroup.devices.allow = c 1:3 rwm
lxc.cgroup.devices.allow = c 1:5 rwm
# consoles
lxc.cgroup.devices.allow = c 5:1 rwm
lxc.cgroup.devices.allow = c 5:0 rwm
lxc.cgroup.devices.allow = c 4:0 rwm
lxc.cgroup.devices.allow = c 4:1 rwm
# /dev/{,u}random
lxc.cgroup.devices.allow = c 1:9 rwm
lxc.cgroup.devices.allow = c 1:8 rwm
lxc.cgroup.devices.allow = c 136:* rwm
lxc.cgroup.devices.allow = c 5:2 rwm
# rtc
lxc.cgroup.devices.allow = c 254:0 rwm

# mounts point
lxc.mount.entry=proc
/var/lib/lxc/myfirstcontainer/rootfs/proc proc
nodev,noexec,nosuid 0 0
lxc.mount.entry=devpts
/var/lib/lxc/myfirstcontainer/rootfs/dev/pts
devpts defaults 0 0
lxc.mount.entry=sysfs
/var/lib/lxc/myfirstcontainer/rootfs/sys sysfs
defaults  0 0


## Network
lxc.utsname = myfirstcontainer
lxc.network.type = veth
lxc.network.flags = up

# that's the interface defined above in host's
interfaces file
lxc.network.link = br0

# name of network device inside the container,
# defaults to eth0, you could choose a name
freely
# lxc.network.name = lxcnet0
lxc.network.hwaddr = 00:FF:AA:00:00:01
# the ip may be set to 0.0.0.0/24 or skip
this line
# if you like to use a dhcp client inside
the container
#lxc.network.ipv4 = 192.168.0.140/24
```

Bueno, ahí está toda la configuración, se puede extender mucho más, pero es un ejemplo simple.

Lo que podemos hacer, ahora es entrar a la jaula, poner el comando chroot, y cambiar por ejemplo:

La clave de root (Que por omisión es root)

El nombre del host (Que por omisión es myfirstcontainer)

Y algunas otras configuraciones, por ejemplo, instalar el ssh.

```
root@squeeze:/var/lib/lxc/myfirstcontainer/
rootfs# pwd
/var/lib/lxc/myfirstcontainer/rootfs
root@squeeze:/var/lib/lxc/myfirstcontainer
/rootfs#
```

Nos fijamos que estamos parado correctamente, y lanzamos el chroot.

```
root@squeeze:/# chroot  .
root@squeeze:/# echo "lala" > /etc/hostname
root@squeeze:/# apt-get install mc
Reading package lists... Done
Building dependency tree
Reading state information... Done
# Sigue….
```

Recuerden siempre hacer un apt-get clean para no dejar paquetes ocupando espacio en /var/cache/apt/archives

Bueno, yo también me instalé un apache server, esto era sólo una muestra.

Arrancando el contenedor

```
lxc-start -n myfirstcontainer -d
```

El –d es para que corra en modo demonio, en background.

Si queremos ver todo el proceso de “booteo” de nuestro contenedor, lo hacemos sin el –d

```
lxc-start -n myfirstcontainer
```

Ahora, cuando terminamos de correr el proceso de booteo, queremos entrar a nuestro contenedor.

```
root@squeeze:/var/lib/lxc/myfirstcontainer/root
fs# lxc-start -n myfirstcontainer
INIT: version 2.88 booting
Using makefile-style concurrent boot in
runlevel S.
Activating swap...done.
Cleaning up ifupdown....
Setting up networking....
Activating lvm and md swap...done.
Checking file systems...fsck from util-linux-ng
2.17.2
done.
Mounting local filesystems...done.
Activating swapfile swap...done.
Cleaning up temporary files....
Setting kernel variables ...done.
Configuring network interfaces...Internet
Systems Consortium DHCP Client 4.1.1-P1
Copyright 2004-2010 Internet Systems
Consortium.
All rights reserved.
For info, please visit
https://www.isc.org/software/dhcp/

Listening on LPF/eth0/00:ff:aa:00:00:01
Sending on   LPF/eth0/00:ff:aa:00:00:01
Sending on   Socket/fallback
DHCPREQUEST on eth0 to 255.255.255.255 port 67
DHCPREQUEST on eth0 to 255.255.255.255 port 67
DHCPDISCOVER on eth0 to 255.255.255.255 port 67
interval 8
DHCPOFFER from 192.168.0.1
DHCPREQUEST on eth0 to 255.255.255.255 port 67
DHCPACK from 192.168.0.1
bound to 192.168.0.116 -- renewal in 34257
seconds.
done.
Cleaning up temporary files....
INIT: Entering runlevel: 3
Using makefile-style concurrent boot in
runlevel 3.
Starting web server: apache2apache2:
apr_sockaddr_info_get() failed for
yfirstcontainer
apache2: Could not reliably determine the
server's fully qualified domain name, using
127.0.0.1 for ServerName
.
Starting OpenBSD Secure Shell server: sshd.

Debian GNU/Linux 6.0 myfirstcontainer console

myfirstcontainer login:
```

Acá por omisión la clave de root, es root. Entramos, y podemos hacer lo que quisiéramos, como si fuera una virtual machine.

Vamos a entrar por ssh a esta máquina, desde el HOST

En el contenedor, averiguamos qué IP tomó.

```
root@myfirstcontainer:~# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:ff:aa:00:00:01
          inet addr:192.168.0.113  Bcast:192.168.0.255  Mask:255.255.255.0
          inet6 addr: fe80::2ff:aaff:fe00:1/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:34 errors:0 dropped:0 overruns:0 frame:0
          TX packets:22 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:3717 (3.6 KiB)  TX bytes:2968 (2.8 KiB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
```

Ok, vemos que tomó la IP 192.168.0.113. Entraremos por ssh

```
root@myfirstcontainer:~# w
 20:48:43 up 1 day, 25 min,  2 users,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM              LOGIN@   IDLE   JCPU   PCPU WHAT
root     console                   20:47   18.00s  0.01s  0.00s -bash
root     pts/0    192.168.0.109    20:48    0.00s  0.00s  0.00s w
```

Acá vemos que estamos como root desde la consola, y que también entramos vía ssh.

Podríamos hacer muchas pruebas más, pero eso se los dejo a su criterio.

Para apagar el contenedor.

Desde el HOST

```
lxc-halt -n myfirstcontainer
```

Desde el contenedor:

```
halt
```

Luego, para que el HOST autoinicie las vm's,

Ponerlas en el /etc/default/lxc

Sin lugar a dudas, es un tema donde existe poca documentación, yo probé varios tutoriales, y algunos dicen una cosa, otros otras, y bueno, tuve que hacer un mixed. Estoy probando de generar unos nuevos templates, y haciendo benchmarks, para ver el rendimiento.

A la vez, viendo cómo se puede integrar esto con libvirt, pero la verdad, que por lo pronto, este proyecto se las trae.

Fuentes: http://wiki.debian.org/LXC

¡Saludos a todos!

Marcelo Guazzardo
Senior Admin Linux / Senior Security Consultant
Fedora Ambassador for Argentina
Oracle Linux Certified
Mguazzardo76@gmail.com

Empaquetamiento RPM (parte I)

POR **EDUARDO ECHEVARRIA**

En Fedora nos sentimos orgullosos cada vez que ingresa un nuevo colaborador a nuestras filas, por lo tanto siempre esperamos que personas con talento, proactivas e innovadoras como tú quieran colaborar en pro del desarrollo de nuestra distribución.

Por esta razón y como parte de una iniciativa de la comunidad de Fedora LATAM y conjuntamente con el proyecto RPMDEV http://rpmdev.proyectofedora.org/ (Proyecto latinoamericano dedicado al empaquetamiento y desarrollo de nuevas aplicaciones en software libre), queremos brindar a los lectores de TUXINFO una serie de artículos dedicados al Empaquetamiento RPM donde podrás conocer todos los aspectos técnicos que forman parte del empaquetado de aplicaciones en Fedora y el proceso necesario para poder ingresar al “Grupo de Mantenedores de Paquetes”; nuestra proyección a futuro es tener una presencia latinoamericana numerosa en este grupo y contamos contigo para lograrlo. :)

¿Qué necesito?

1. Lo primero y obviamente lo más importante, utilizar Fedora, cualquier versión reciente es válida

2. Tener conocimientos básicos de programación y manejo de comandos de Linux, esto no es limitativo, y créeme lo aprenderás rápidamente.

3. Tener un dominio básico del idioma inglés.

4. Tener espíritu de emprendimiento, persistencia para resolver problemas, humildad para aceptar consejos y sobre todo ganas de trabajar en grupo.

Preparando mi PC

El software necesario que necesitarás para empezar a empaquetar está contenido en estas tres simples órdenes de consola, ejecútalas como usuario root.

```
# yum groupinstall "Development Tools"
# yum install rpmdevtools
# yum install rpmlint
```

Luego añade un usuario a tu sistema Fedora para trabajar con los paquetes, no te recomiendo trabajar ni con tu usuario personal ni mucho menos con tu cuenta de root, de esa forma si algo va mal simplemente puedes eliminar ese usuario y volver a empezar.

```
# useradd makerpm
```

Ingresa con tu usuario recién creado y ejecuta el siguiente comando

```
# rpmdev-setuptree
```

El programa "rpmdev-setuptree" creará el directorio "rpmbuild" en tu directorio $HOME, En dicha estructura existen una serie de subdirectorios tales como:

Nombre	Ubicado en	Propósito
Directorio especificaciones	~/rpmbuild/SPECS	Archivos de especificaciones RPM (.spec).
Directorio fuente	~/rpmbuild/SOURCES	Paquete fuente prístina (e.g., tarballs) y parches.
Directorio de construcción	~/rpmbuild/BUILD	Archivos fuente son desempacados y compilados en un subdirectorio bajo este directorio.
Directorio raíz de construcción	~/rpmbuild/BUILDROOT	Los archivos son instalados bajo este directorio durante la etapa de instalación (%install) .
Directorio binario RPM	~/rpmbuild/RPMS	Los binarios RPM son creados y almacenados bajo este directorio.
Directorio fuente RPM	~/rpmbuild/SRPMS	Los fuente RPM son creados y almacenados bajo este directorio.

Este árbol de directorios es el que utilizarás para crear tus paquetes. también se creara el archivo "~/.rpmmacros" que contiene algunas definiciones comunes de macros para hacer archivos SPEC (del cual hablaremos en un momento)

Una vez que hayas ejecutado estos comandos en tu PC, estará lista para el empaquetamiento de aplicaciones en RPM.

¿Qué puedo empaquetar?

Puedes encontrar aplicaciones para empaquetar en Fedora en repositorios de software libre reconocidos como freecode, github, sourceforge, o en cualquier forja de software libre de tu localidad (te sorprendería saber cuántos desarrolladores en tu país podrían estar brindando sus aplicaciones bajo licencias libres; una forma de apoyarlos y agradecerles su trabajo es empaquetar sus creaciones).

Debes asegurarte que la aplicación(es), que estés empaquetando no se encuentre disponible actualmente en Fedora, para ello sigue estos pasos:

Ejecuta

```
# yum search nombredelprograma
```

Si la salida del comando no te muestra el nombre explícito de la aplicación tal vez pueda ser empaquetado, pero todavía hay otras formas de verificación que debes tomar en cuenta.

- Busca en Google “NOMBREDELPROGRAMA Fedora rpm”

- Busca en bugzilla.redhat.com, las peticiones de revisión de aplicaciones “Progress Review Requests”

- Busca en https://admin.fedoraproject.org/pkgdb utilizando el formulario previsto para tal fin

Una excepción a la regla sería tratar de empaquetar paquetes huérfanos o en inglés “Orphan Packages”, estos paquetes por alguna razón han dejado de ser mantenidos por sus empaquetadores y están disponibles, esperándote para nuevamente ser incluidos en la distribución si quieres aceptar el reto.

Puedes encontrar una lista completa en https://admin.fedoraproject.org/pkgdb/acls/orphans

Para terminar esta sección me gustaría plantear una interesante definición disponible en las directrices de empaquetamiento de Fedora, disponible en inglés en http://fedoraproject.org/wiki/Packaging:Guidelines

Diferencia entre código y contenido

Es importante hacer una distinción entre el código ejecutable por ordenador y contenido. Si bien en Fedora se permite código (suponiendo, por supuesto, que

cuenta con una licencia de código abierto compatible, que no sea legalmente cuestionable, etc), sólo algunos tipos de contenido son permitidos.

La regla es la siguiente, si el contenido mejora la experiencia de usuario del sistema operativo, el contenido se considera correcto para ser empaquetado en Fedora, Esto significa, por ejemplo que cosas, como fuentes, imágenes prediseñadas, fondos de pantalla son permitidos.

El contenido tiene que ser revisado para su inclusión. Debe tener una licencia de código abierto compatible, no deben ser jurídicamente cuestionable. Además, hay varias restricciones adicionales para el contenido

- El contenido no debe ser pornográfico, o que contengan algún tipo de desnudez, ya sea animado, simulado o fotografiado.

- El contenido no debe ser ofensivo, discriminatorio o peyorativo. Si no estás seguro de si una parte del contenido es una de estas cosas, probablemente lo es.

Algunos ejemplos de contenido abajo listados son permitidos:

- Paquetes de documentación y archivos de ayuda

- Clipart para su uso en las suites de oficina

- Imágenes de fondo de escritorio (de tipo no ofensivo, discriminatorio, y con permiso para redistribuir libremente)

- Fuentes (bajo una licencia de código abierto, sin ninguna propiedad / problemas legales)

- Sonido o gráficos incluidos con el paquete fuente (sin ninguna propiedad / problemas legales) que utiliza el programa o el tema

- Juegos (bajo una licencia de código abierto, sin ninguna propiedad / problemas legales)

- Música del juego o contenido de audio siempre y cuando el contenido es de libre distribución sin restricciones, y el formato no es patentado.

Algunos ejemplos de contenidos que no son permitidos serían

- Historietas

- Textos religiosos

- Archivos MP3 (formato patentado)

La magia de los SPECS

El archivo que hará posible la creación de paquetes rpm es el spec, estos deben ser ubicados en el directorio "~/rpmbuild/SPECS". Debes nombrarlo de acuerdo al nombre canónico del programa, ej. "programa.spec", que normalmente es publicado por el autor del software.

Primero crea un archivo en blanco con el editor vi (el cual te proporcionará una plantilla muy funcional de un spec básico)

```
$ vi nombredelprograma.spec
```

o con el comando:

```
$ rpmdev-newspec nombredelprograma
```

Un ejemplo básico de un spec:

```
Name:           f2fs-tools
Version:        1.0.0
Release:        3%{?dist}
Summary:        Tools for Flash-Friendly File System (F2FS)
License:        GPLv2+
URL:            http://sourceforge.net/projects/f2fs-tools/
Source0:        http://downloads.sourceforge.net/project/%{name}/%{name}-%{version}.tar.gz
BuildRequires:  autoconf
BuildRequires:  automake

%description
NAND flash memory-based storage devices, such as SSD, and SD cards,
have been widely being used for ranging from mobile to server systems.
Since they are known to have different characteristics from the
conventional rotational disks,a file system, an upper layer to
```

```
the storage device, should adapt to the changes
from the sketch.

F2FS is a new file system carefully designed for the
NAND flash memory-based storage devices.
We chose a log structure file system approach,
but we tried to adapt it to the new form of storage.
Also we remedy some known issues of the very old log
structured file system, such as snowball effect
of wandering tree and high cleaning overhead.

Because a NAND-based storage device shows different characteristics
according to its internal geometry or flash memory management
scheme aka FTL, we add various parameters not only for configuring
on-disk layout, but also for selecting allocation
and cleaning algorithms.

%prep
%setup -q

%build
autoreconf --install
%configure
make %{?_smp_mflags}

%install
make DESTDIR=%{buildroot} INSTALL="install -p" CP="cp -p" install

%files
%doc COPYING AUTHORS ChangeLog
%{_bindir}/mkfs.f2fs
%{_mandir}/man8/mkfs.f2fs.8*

%changelog
* Mon Oct 22 2012 Eduardo Echeverria  <echevemaster@gmail.com> - 1.0.0-3
- Change to the correct license GPLv2+
- Remove README file to the section doc
* Mon Oct 15 2012 Eduardo Echeverria  <echevemaster@gmail.com> - 1.0.0-2
- Add Changelog AUTHORS files to section doc
- Add wilcard to the manpages section.

* Sun Oct 07 2012 Eduardo Echeverria  <echevemaster@gmail.com> - 1.0.0-1
- Initial packaging
```

A continuación, daré una breve explicación de qué significan estas etiquetas o “tags”

Disponible en:

http://fedoraproject.org/wiki/How_to_create_an_RPM_package/es#Explicando_las_partes_de_un_archivo_spec

Name: Es el nombre (base) del paquete. Debe estar conforme a las normas o directrices de nombrado de paquetes http://fedoraproject.org/wiki/Packaging:NamingGuidelines . En la mayoría de los casos será todo en letras minúsculas. En cualquier lugar del archivo spec puedes referirte al nombre utilizando el macro %{name} de esa forma, si el nombre cambia, el nuevo nombre será utilizado por esas otras ubicaciones donde se utiliza. Este nombre debería coincidir con el nombre de archivo del archivo spec.

Version: El número de versión aguasarriba (upstream). Si la versión no es numérica (contiene marcas que no son números o dígitos), puede que necesites incluir caracteres no numéricos adicionales en el campo release. Si aguasarriba se usan fechas completas para distinguir las versiones, considere usar números de versión de la forma yy.mm[dd] (de tal forma que la liberación 2008-05-01 se convierte en 8.05). En cualquier lugar del archivo spec, puedes referirte a este valor como %{version}.

Release: El valor inicial de release debería normalmente ser "1%{?dist}". Entonces, incrementa el número cada vez que libere un nuevo paquete para la misma versión

de software. Si se está empaquetando y liberando una nueva versión del software, el número de versión debería ser cambiado para reflejar la nueva versión de software y el número de liberación (release) debería ser restablecido a 1. Usa %{release} para reutilizar este valor.

Summary: Una breve, de una línea, descripción del paquete. Usa Inglés Americano, y no termines con punto.

Group: Este debe ser un nombre de grupo existente, como "Applications/Engineering", ejecuta "less /usr/share/doc/rpm-*/GROUPS" para ver la lista completa. Si creas un subpaquete, "...-doc" con documentation, use el grupo "Documentation".

License: La licencia, para software, debe ser una licencia de fuente abierta. Use las abreviaciones estándar, ej. "GPLv2+". Intente ser específico, por ejemplo use "GPLv2+" (GPL version 2 or greater) en vez de sólo "GPL" o "GPLv2" cuando esto sea cierto. Vea Licensing y los lineamientos en Licensing Guidelines para más información. Usted puede listar múltiples licencias combinándolas con "and" y "or", como en "GPLv2 and BSD". Llame a esta marca "License", no use la marca antigua "Copyright".

URL: El URL para conseguir más información acerca del programa, por ejemplo, el sitio web del proyecto. Nota: Este NO es de donde provino el código fuente original.

Source0: El URL para conseguir el archivo comprimido que contiene los fuentes (originales) prístinas, como se ha liberado aguas arriba. "Fuente" es sinónimo de "Source0". Si defines un URL completo (y debería), su nombre base será utilizado cuando se busque en el directorio SOURCES. Si es posible, agregue %{name} y %{version}, así los cambios a cualquiera de ellas irá al lugar adecuado. Alerta: Source0: y URL: son diferentes , normalmente ambos son URLs, pero la entrada "URL:" apunta al sitio web del proyecto, mientras que "Source0:" apunta al archivo que contiene el código fuente (y es típicamente un archivo .tar.gz). Cuando descargues fuentes, parches, etc, considere usar un cliente que preserve las marcas de tiempo aguas arriba. Por ejemplo wget -N o curl -R. Para hacer el cambio algo global para wget, agrega lo siguiente a tu ~/.wgetrc: timestamping = on, and for curl, agregue a su ~/.curlrc: -R."

Si existe más de un fuente, nómbralos como Source1, Source2, y así. Si estás agregando nuevos archivos completos además de las fuentes prístinas, puedes listar cada uno como fuentes también, pero lístalos después de las fuentes prístinas. Una copia de cada una de estas fuentes serán incluidas en cualquier paquete fuente que cree (a menos que específicamente le indique lo contrario). Vea "Packaging/SourceURL"https://fedoraproject.org/wiki/Packaging/SourceURL para más información de casos especiales (uso de control de revisión, cuando aguas arriba usa código prohibido, etc).

Patch0: El nombre del primer parche que aplicará al código fuente. Si necesita parchar los archivos después de descomprimir, usted debería editar los archivos, salvar sus diferencias como archivo "patch" en su directorio ~/rpmbuild/SOURCES. Los parches deberían hacer un único cambio lógico, así que es muy probable que tenga múltiples archivos de parches (patch).

BuildRequires: Una lista separada por comas de paquetes requeridos para construir (compilar) el programa. Estos no son determinados automáticamente, así que usted debe incluir todo lo necesario para construir el programa. Hay algunos pocos paquetes que son tan comunes en las compilaciones que usted no necesitará mencionarlos, tal como "gcc"; vea Packaging Guidelines para ver la lista completa de paquetes que puede omitir.

También puede especificar versiones mínimas requeridas, si es necesario, así: "ocaml >= 3.08". Usted puede tener más de una línea de BuildRequires (en cuyo caso son todas ellas requeridas para compilación). Si necesita el archivo /EGGS, se puede obtener tu paquete corriendo "rpm -qf /EGGS"; si EGGS es un programa, Se determina el paquete rápidamente ejecutando rpm -qf `which EGGS`".

Intenta especificar la menor cantidad posible de paquetes necesarios para construir apropiadamente el paquete ya que cada uno desacelerará el proceso de construcción, ten cuidado, algunas aplicaciones deshabilitan permanentemente funciones si el paquete no es detectado durante la compilación, en dichos casos puede que necesite incluir dichos paquetes adicionales.

Requires: Una lista de paquetes separados por coma que son requeridos cuando el programa es instalado.

Note que la lista de paquetes para Requires (lo que es requerido cuando se instala/ejecuta)

y BuildRequires (lo que se requiere para compilar el RPM binario) son independientes, un paquete puede estar presente en una lista pero no en la otra o pudiera estar en ambas listas.

Las dependencias de los paquetes binarios son en muchos casos automáticamente detectadas por rpmbuild así que es común el caso de que no se requiere especificar Requires para nada. Pero si deseas resaltar algunos paquetes como requeridos, o requerir algún paquete que rpm no pueda detectar, entonces agrégalo aquí.

%description - Una descripción más larga del programa, multilínea. Use Inglés Americano. Todas las líneas deben ser de ochenta (80) caracteres o menos. Se asume que las líneas en blanco son párrafos separados.

Algunos programas de instalación GUI reformatearán los párrafos, la líneas que comienzan con un espacio en blanco, tales como espacio o tabulador, serán tratados como texto preformateado y lo mostrarán tal cual es, normalmente con una fuente de ancho fijo (de acuerdo a RPM Guide).

%prep - Comandos guión para "preparar" el programa, esto es, descomprimirlo tal que esté listo para construcción (compilación). Típicamente es sólo "%setup -q" o alguna variación, una variación común es "%setup -q -n NAME" si el archivo fuente desempaca en NAME.

%build - Comandos guión para "construir" el programa, esto es, compilarlo y alistarlo para instalación. El programa debería venir con instrucciones de cómo hacerlo.

%check - Comandos guión para auto-probar el programa. Estos se ejecutan justo después de %build y antes de %install, así que deberías colocarlo si utilizas dicha sección.

A menudo simplemente contiene "make test" o "make check". Esto es aparte de %build así que las personas pueden saltarse la auto-prueba si lo desean. Esto no está documentando en muchas partes.

%install - Comando guión para "instalar" el programa. Los comandos deben copiar los archivos desde el "directorio de construcción" %{_builddir} (que estaría debajo de ~/rpmbuild/BUILD) en el directorio raíz de construcción, %{buildroot} (que normalmente estaría bajo /var/tmp). Vea la sección "%install" abajo para más detalles.

%files - la lista de archivos que serán instalados

%changelog - Cambios en el paquete.

ExcludeArch: Si el paquete no compila exitosamente, construye o funciona en una o más arquitecturas dadas, entonces dichas arquitecturas deberían ser listadas en el spec con la marca ExcludeArch.

Para la próxima entrega del taller, una explicación detallada con ejemplos de los diferentes tags y la forma de construir tu primer RPM

Eduardo Echeverria
Licenciado en Educación
Fedora Package Maintainer
Fedora Ambassador


TUX
INFO
WWW.TUXINFO.COM.AR