Entornos de trabajo forense sobre computación virtual

Hernán Herrera[1], Leopoldo Sebastián M. Gómez[1]

[1] Poder Judicial del Neuquén,
Stgo. del Estero 64, Neuquén, CP 8300, Argentina
sebastian.gomez@jusneuquen.gov.ar

Abstract. La gestión interna de un laboratorio de informática pericial requiere una infraestructura tecnológica que provea seguridad y una adecuada disponibilidad de servicios. Se hace necesario contar con un repositorio para el almacenamiento de evidencia digital e información técnica producida durante las labores periciales. Por otra parte, resulta de gran utilidad poder compartir el conocimiento adquirido mediante tareas de investigación y laboratorio, registrando los resultados en un sistema de gestión de contenidos. Focalizando las necesidades de un laboratorio pericial informático, este trabajo presenta una experiencia de virtualización para la optimización de recursos tecnológicos y un mejor aprovechamiento de las herramientas habituales de trabajo. Se expone la implementación de una arquitectura conformada por servidores virtuales que proveen servicios informáticos al personal del laboratorio. En el ámbito jurisdiccional, las labores periciales demandan el uso de distintos sistemas operativos como plataforma de ejecución de aplicaciones forenses. La implementación de puestos de trabajo con máquinas virtuales facilita a los investigadores la utilización de un mayor número de recursos de software en forma simultánea.

1 Introducción

El concepto de virtualización refiere a una capa de abstracción que separa el hardware del sistema operativo, optimizando y flexibilizando de esta manera la utilización de los recursos computacionales. Este paradigma permite que múltiples máquinas virtuales con sistemas operativos heterogéneos puedan funcionar simultáneamente en la misma computadora. Cada máquina virtual tiene asignado un conjunto propio de recursos de hardware sobre el que pueden funcionar diferentes aplicaciones.

A principio de los años sesenta el concepto de virtualización se aplicó en los grandes mainframes. En la década del ochenta, con el advenimiento de las computadoras personales, el procesamiento de la información fue cambiando paulatinamente desde lo centralizado a lo distribuido, y la virtualización fue quedando en desuso. En los años noventa, los investigadores comenzaron a estudiar como la virtualización podría resolver ciertos problemas asociados con la proliferación del hardware de bajo costo, tales como la baja reutilización de los recursos, el manejo de la escalabilidad y las vulnerabilidades crecientes en los sistemas de computación.

Actualmente la virtualización ha resurgido, brindando a las organizaciones la posibilidad de mejorar sus infraestructuras informáticas en cuanto a escalabilidad, seguridad y una variedad de modalidades en la administración de servidores.

Los beneficios de la virtualización [1] pueden ser apreciados sobre tres aspectos de alto impacto para la administración de sistemas, a saber: particionamiento, aislamiento y encapsulación. El primero de ellos permite que múltiples aplicaciones y sistemas operativos puedan compartir el mismo hardware. Los servidores pueden ser consolidados dentro de máquinas virtuales, logrando escalabilidad vertical al agregar recursos tecnológicos a una determinada computadora y horizontal mediante la incorporación de nuevos nodos o servidores. Otra ventaja de la virtualización se logra respecto al aislamiento de componentes. Las máquinas virtuales funcionan de forma aislada entre si, y respecto a la máquina anfitriona. Por lo expuesto, si una máquina virtual falla esta situación no afecta al funcionamiento de las restantes. Las máquinas virtuales se comunican entre si a través de una red de la misma manera que lo hacen las máquinas reales. Adicionalmente, la encapsulación permite que una máquina virtual pueda almacenarse en un simple archivo facilitando el backup de la misma, la copia, o el traslado. La estandarización del hardware virtualizado garantiza la compatibilidad.

2 Tecnologías de virtualización

Las herramientas de virtualización actúan como monitores de otros sistemas operativos que se instalan sobre esta infraestructura como máquinas virtuales. Estas tecnologías utilizan un software o firmware pequeño llamado hypervisor para alcanzar un alto grado de granularidad al compartir recursos en forma dinámica. Existen dos clases de hypervisores. Los llamados Tipo 1 se ejecutan directamente sobre el hardware y son más eficientes. Los hypervisores Tipo 2 tienen menos rendimiento por estar instalados sobre el sistema operativo anfitrión [1].

La oferta de herramientas de virtualización ha aumentado debido a las altas prestaciones que brindan estos productos. Actualmente VMware [2] es la herramienta comercial más popular del mercado y cuenta con una versión de producto perteneciente al Tipo 1. Versiones anteriores de VMware utilizan una técnica conocida como “binary translation”, donde las instrucciones privilegiadas son reemplazadas con fragmentos de código que simulan las mismas, afectando el rendimiento de las máquinas virtuales.

Xen [3] es un software libre con hypervisor de Tipo 1, que utiliza una técnica llamada “ring deprivileging”. Mediante este método, el sistema operativo es modificado para reducir el nivel de privilegios de accesos al procesador dejando el nivel más elevado para Xen. Este esquema de usos de niveles es conocido como paravirtualización. Actualmente, las nuevas tecnologías de virtualización de Intel y AMD permiten mantener el nivel de privilegio del sistema operativo sin necesidad de modificación alguna, dejando un nivel de privilegio especial para el hypervisor.

[1] http://www.vmware.com/virtualization/
[2] http://www.vmware.com/
[3] http://xensource.com/

Aprovechando los avances en las arquitecturas de hardware, han surgido nuevas versiones de Xen que no requieren realizar modificaciones en los sistemas operativos virtualizados.

3 Desarrollo de la infraestructura virtual de servicios

Un servidor clásico ejecuta un sistema operativo sobre el cual determinados servicios son ofrecidos a la red, por ejemplo comunicaciones, aplicaciones, almacenamiento de archivos e impresión. En un entorno informático de mediana complejidad es posible encontrar uno o más servidores cumpliendo las tareas mencionadas anteriormente. En ocasiones, los servicios que se entregan a la red funcionan en el mismo sistema operativo, pero si las aplicaciones que los gestionan se ejecutan en sistemas operativos distintos obliga a contar con dos o más servidores físicos. Situaciones similares a la expuesta precedentemente pueden incrementar el número de servidores físicos y la adición de nuevos elementos de conectividad, provocando un aumento en la demanda de energía eléctrica y en el espacio de los racks e instalaciones.

Si se aplica el paradigma de virtualización a la situación planteada, ciertos servidores físicos se convierten en virtuales, instalándolos en una plataforma de virtualización que puede funcionar en uno de los servidores existentes, con un aumento moderado de recursos de hardware. Entre los principales beneficios de este cambio tecnológico se encuentra la simplicidad en la reconstrucción de un servidor ante posibles fallas de hardware o software. Asimismo, al disminuir el número de computadoras en funcionamiento se reduce el espacio y el consumo. Como consecuencia de la consolidación, los mayores costos de adquisición de nuevos servidores pueden ser absorbidos mediante la ejecución de máquinas virtuales en los equipos existentes [2].

3.1 El cambio de paradigma

La virtualización realizada en el laboratorio de informática pericial del Poder Judicial del Neuquén se inició a partir de un servidor multipropósito que brindaba servicios de acceso a Internet, publicación de información técnica interna y almacenamiento de archivos. Transformando al servidor descrito precedentemente en un conjunto de servidores virtuales se logra una infraestructura de servicios con mayor seguridad, tolerancia a fallos y escalabilidad.

3.2 Creación de servidores virtuales

La implementación de servicios internos virtuales comenzó con un reemplazo del sistema operativo del servidor multipropósito por una distribución de Linux CentOS para actuar como sistema operativo anfitrión. Posteriormente se instaló el software de virtualización, cuya elección recayó en VMware Server por ser una herramienta consolidada en el mercado y de libre utilización.

Mediante esta plataforma de operaciones, se crearon las siguientes máquinas virtuales:

- Servidor Web: Sistema operativo Linux CentOS, ofreciendo servicios web a través del software Apache, y con un servidor de aplicaciones ZOPE sobre el que se ejecuta el CMS Plone, en el cual se publican los resultados de las investigaciones.
- Servidor de Archivos: Sistema operativo Linux CentOS, ejecutando el software Samba para compartir archivos entre sistemas operativos Linux y Windows.
- Firewall: Sistema operativo Linux CentOS utilizando el sistema de IPtables vinculado al kernel de Linux, funcionando como puerta de enlace, y ejecutando el servicio proxy mediante Squid

3.3 Topología de servidores y dispositivos de red

Las máquinas virtuales de VMware se conectan a otras máquinas a través de switchs virtuales [3].

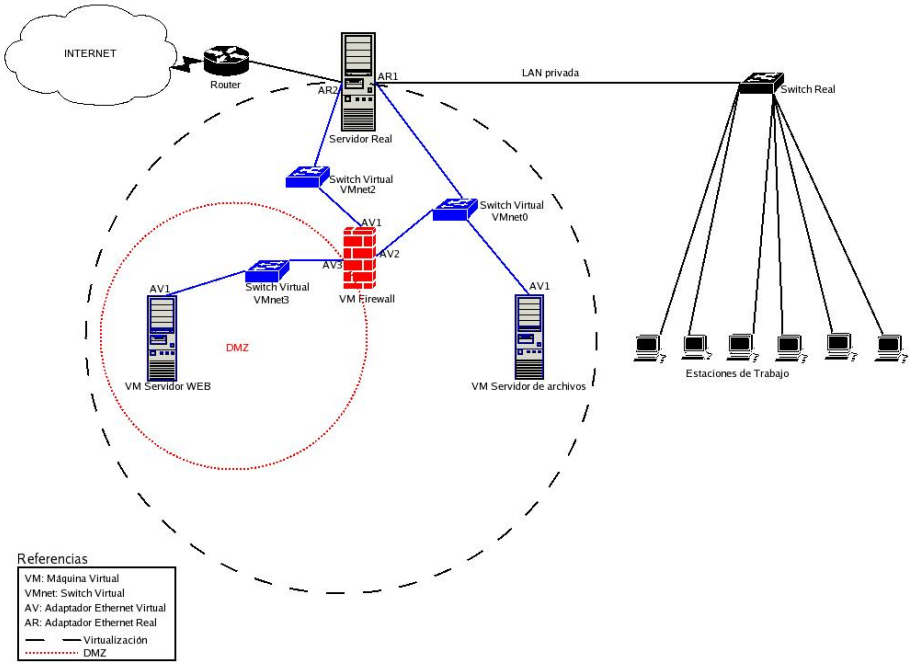

Figura 1. Topología de red obtenida una vez aplicado el paradigma de virtualización

Existen tres modos de conectividad de los switchs, a saber: a) Bridge: permite conectar una máquina virtual a una red física. Este tipo de conectividad posibilita que la máquina virtual sea vista por el resto de los equipos como una máquina real. b) Host Virtual Adapter: permite que una máquina virtual tenga conectividad con el equipo anfitrión. Se dispone de un switch virtual específico para realizar este enlace. c) NAT Device: permite conectar una máquina virtual a la red física usando la

dirección IP del equipo anfitrión. VMware Server cuenta con un servicio de NAT que permite llevar a cabo la tarea mencionada a través de un switch virtual específico.

Para la virtualización del laboratorio pericial informático (Figura 1), la red quedó configurada de la siguiente forma:

- Se utilizaron tres switchs virtuales para posibilitar el modo de conexión Bridge a las diferentes máquinas virtuales.
    - Switch VMnet0: Conecta el VM Firewall y el VM Servidor de Archivos a la red física (LAN privada).
    - Switch VMnet2: Conecta el VM Firewall al Router.
    - Switch VMnet3: Conecta la Zona Desmilitarizada (DMZ) al VM Firewall.
- En la DMZ se depositó el VM Servidor Web.
- La LAN privada accede a INTERNET a través del VM Firewall.
- Todo el tráfico proveniente de Internet es derivado a la máquina virtual VM Firewall.

3.4 Extendiendo las funcionalidades en los puestos de trabajo

En los puestos de trabajo del laboratorio pericial informático se analiza la evidencia digital utilizando aplicaciones forenses tales como EnCase[4], Autopsy[5], FTKImager[6] y AIR[7]. Las herramientas mencionadas no son multiplataforma. EnCase y FTKImager operan bajo Windows y las demás bajo Linux, impidiendo utilizarlas al mismo tiempo en un mismo equipo.

Aplicando el paradigma de virtualización se pueden crear máquinas virtuales con diferentes sistemas operativos y de esta manera lograr que aplicaciones que no son multiplataforma operen en paralelo.

Como caso de aplicación en el laboratorio pericial informático, cada puesto de trabajo utiliza el software de virtualización VMware Server como plataforma de operaciones, funcionando sobre el sistema operativo anfitrión Windows XP. Se cuenta con una máquina virtual con sistema operativo Linux, sobre la que es posible ejecutar las aplicaciones AIR y Autopsy. Las ventajas de la virtualización son evidentes, ya que con esta plataforma de operaciones es posible efectuar una adquisición remota de un disco rígido mediante AIR y luego abrir la imagen forense para efectuar alguna operación en particular con el software FTK Imager -ejecutando sobre el sistema operativo anfitrión- sin necesidad de cambiar el entorno habitual de trabajo.

[4] http://www.guidancesoftware.com/
[5] http://www.sleuthkit.org/autopsy/
[6] http://www.accessdata.com/
[7] http://air-imager.sourceforge.net/

4 Trabajos relacionados con computación forense virtual

Siempre fue un deseo de los investigadores en informática forense poder visualizar en forma directa el área de trabajo de la computadora de un imputado, sabiendo además que usualmente las personas utilizan software propietario, sin el cual no es posible acceder a la información. El método más rudimentario consiste en clonar el dispositivo de almacenamiento original y luego instalar esta copia en un hardware de laboratorio o incluso sobre la computadora original, si se dispone de ella. Este procedimiento no es muy recomendado, ya que usualmente se presentan problemas de incompatibilidad con el hardware cuando se utiliza una computadora de laboratorio, y además es conveniente no manipular demasiado la computadora del sospechoso, sin contar que finalmente deberá realizarse otra imagen para el análisis forense, ya que la primera será modificada durante la inspección.

Con la aparición de herramientas de virtualización como VMware, surgieron las primeras aproximaciones para intentar recrear el entorno de trabajo del sospechoso [4], pero persistía la necesidad de mantener una imagen adicional del dispositivo original para análisis forense, ya que en sus inicios dichas virtualizaciones no mantenían la integridad de los dispositivos, al permitir la modificación de la información almacenada.

Actualmente ha surgido en el mercado de informática forense la herramienta comercial VFC [8], mediante la cual es posible crear una maquina virtual ejecutable y luego inicializarla con VMware. Al combinarla con el software comercial MountImage Pro v2 [9] permite montar imágenes forenses soportando diferentes formatos en un entorno Windows. VFC puede crear máquinas virtuales a partir de archivos Encase (*.e01) o Smart (*.s01) utilizando Mount Image Pro v2, o bien directamente desde los dispositivos de almacenamiento originales (debiendo bloquearse contra escrituras). También es posible convertir imágenes de discos realizadas mediante el comando de Unix “dd” o similares, e imágenes Vogon (*.img). Si bien la combinación de Mount Image Pro v2 y VFC permite trabajar sobre un mayor número de formatos de archivos imagen, LiveView! [10] continúa siendo una herramienta indispensable por estar orientada al trabajo forense, su simplicidad de uso y la libre disponibilidad del software.

Se han reportado experiencias en el ámbito universitario utilizando laboratorios virtuales de seguridad e informática forense. Integrando un servidor de almacenamiento de máquinas virtuales a la red interna de la institución educativa se ha facilitado a los estudiantes e investigadores tener acceso a entornos sobre los cuales poder obtener experiencia práctica [5], [6].

[8] http://www.md5.uk.com/
[9] http://www.mountimage.com/
[10] http://liveview.sourceforge.net/

5 Conclusiones

La virtualización permite instalar servidores dedicados sobre un mismo hardware subyacente, así como también la configuración de distintas topologías de red mediante la conexión de máquinas virtuales y reales. Realizando los procedimientos habituales para el resguardo de datos sensibles, en caso de fallos de hardware o software, esta tecnología facilita una posterior restauración de los servicios mediante copias de servidores virtuales preconfigurados, asegurando efectividad y celeridad en la ejecución de un plan de contingencias.

En el ámbito estatal es habitual contar con recursos financieros mínimos para la adquisición de tecnología. El trabajo con servidores virtuales simplifica la escalabilidad vertical y horizontal, mediante el aprovechamiento eficiente del equipamiento informático existente y la incorporación gradual de recursos tecnológicos.

Aplicando este paradigma a un laboratorio pericial informático, se ha definido una arquitectura orientada a servicios acorde a los estándares actuales de seguridad informática y sin requerir inversiones costosas. Finalizada la implementación y configuración de la plataforma operativa, el entorno de trabajo forense del laboratorio pericial informático ha incorporado componentes virtualizados que brindan seguridad en el acceso a la información, permiten el almacenamiento de documentos de trabajo y proveen los medios de acceso compartido a Internet.

Es importante destacar el aumento de la productividad en el trabajo cotidiano al utilizar múltiples aplicaciones forenses en paralelo por medio de máquinas virtuales. El sistema operativo ha dejado de ser un punto de inflexión para el aprovechamiento de recursos informáticos en las actividades periciales.

Esta experiencia fue realizada exitosamente en el Poder Judicial del Neuquén. El laboratorio pericial informático cuenta con servicios tecnológicos internos y entornos de trabajo forense completamente atomizados en máquinas virtuales.

Referencias

[1] “IBM SystemsVirtualization Version 2 Release 1”, (2005). Extraído de: http://publib.boulder.ibm.com/infocenter/eserver/v1r2/topic/eicay/eicay.pdf

[2] Greene, D., “Virtualization:Transforming the IT Landscape”, (2006), VMware. Extraído de: http://www.vmware.com/pdf/wp_transformingtheitlandscape.pdf

[3] VMware, “VMware Server Virtual Machine Guide”,.(2006). Extraído de: http://www.vmware.com/pdf/server_vm_manual.pdf

[4] Baca, E., “Using Linux, VMware and SMART to Create a Virtual Computer to Recreate a Suspect's Computer”, (2002). Extraído de: http://www.infosecwriters.com/text_resources/andrewrosen/SMARTForensics.pdf

[5] Hay B., Nance K., “Evolution of the ASSERT Computer Security Lab”, (2006), Proceedings of the 10th Colloquium for Information Systems Security Education, University of Maryland, University College Adelphi, MD June 5-8.

[6] Hay B., Nance K. and Hecker C., “Promoting Digital Forensics Awareness through the University of Alaska – Fairbanks ASSERT Center”, (2007), Proceedings of the 40th Hawaii International Conference on System Sciences.