

Segurizando ambientes virtuales

Autor: Diego Bruno

Edición y Corrección: Lic. Cristian Borghello, MVP - CISSP

Fecha Publicación: 01 de agosto de 2010

Publicado en [Segu-Info](http://www.segu-info.com.ar)

Introducción

Vengo leyendo últimamente varios artículos en diferentes foros en dónde se habla de la seguridad en los **Cloud Computing**, o en criollo, seguridad en la nube y quise hacer una colaboración extra a lo ya mencionado en muchos de los artículos.

Voy a hablar más bien de seguridad en la virtualización, que en definitiva, es la solución sobre la que se montan muchos de los servicios de cloud computing.

De hecho, a mi manera de verlo, el cloud computing es una evolución natural del uso de la ya bastante madura tecnología de virtualización, en relación a la mejora del negocio.

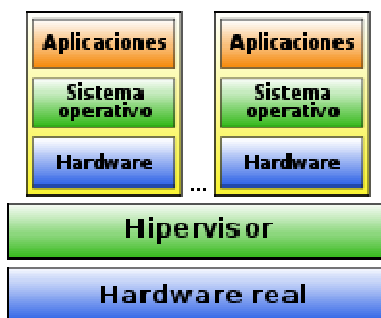
Pero sin sonar como Wan Chan Kein (¿creo que era así no? para los nostálgicos de la serie Kung Fu) *“Escucha mis palabras pequeño saltamontes”*.

Pero cómo decía Jack el destripador *“Vayamos por partes”*. Si sabemos que gran parte del escenario del cloud es la virtualización, metámonos de fondo en ella desde su concepto.

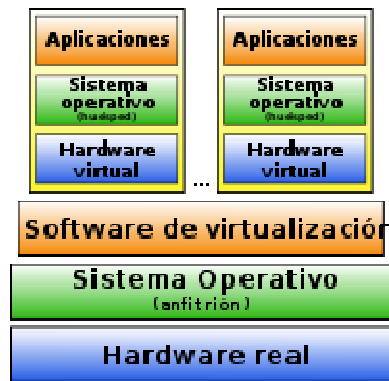
Virtulización

Sabemos que hay dos tipos de virtualización:

Una la llamada nativa o *bar-metal* la cual es una capa de software que se ejecuta directamente sobre el hardware



La segunda es la llamada *hosted*, la cual es un programa de software que corre “sobre” el sistema operativo para ofrecer la misma funcionalidad de virtualización mencionada.



En los entornos empresariales obviamente se utiliza la primera opción a través de los famosos “Hypervisors” los cuales son los que actúan directamente entre la capa de software y las virtual machines. Algunos de los ejemplos más representativos de estos productos son VMware Server ESX3I y Xen Hypervisor.

Microsoft por su parte viene ganando muchísimo terreno a gran velocidad a través de HyperV SP2 y su todo su kit de utilidades como Virtual machine manager SP2 y otros features significativos más.

Cuando hablamos de seguridad en entornos virtualizados, más allá de todos los componentes que pueden entrar o no en juego, hay, dos capas a diferenciar que existen:

Una es la infraestructura de virtualización en sí en la cual se montan las virtual machines. La segunda es sobre las virtual machines en sí misma.

Suele pasar muy seguido que se habla de cómo las virtuales deberían ser administradas y securizadas igual que un host físico real, de cómo se le deberían aplicar o no aplicar templates de seguridad de acuerdo a las políticas existentes de la compañía y un sin fin de recomendaciones válidas más que ya las mencionaremos al final, pero poco se menciona sobre los riesgos existentes en el core de la infraestructura de virtualización.

Cuando hablamos del Core de la infraestructura de virtualización estamos hablando de varios componentes en dónde la estrella es el Hypervisor en sí mismo.

¿Por qué es tan importante la seguridad del Hypervisor?

Las organizaciones que se apoyan en la virtualización tienen su fundamento en que los Hypervisors de virtualización permiten un nivel de “comunidad” si se lo quiere definir de alguna forma, entre todas las virtuales a través de todos los Hypervisors en la misma plataforma de hardware.

Cuando una máquina virtual es creada por encima de la solución de Hypervisor que se utilice, dicha máquina virtual es funcionalmente similar a otras máquinas virtuales en cuanto a términos de su composición de emulación de hardware.

Dicha funcionalidad de comunidad permite justamente que las virtuales de un host funcionen en otro cuando son recolocadas.

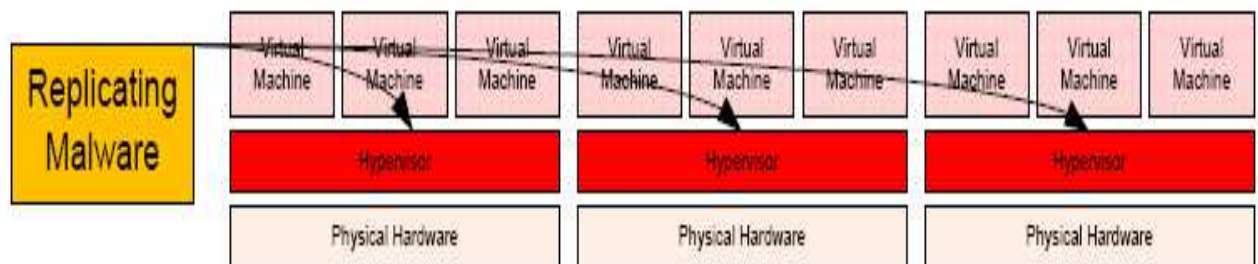
También permite a las virtual machines que son colocadas en un único host compartir los recursos físicos de dicho host mientras al mismo tiempo mantienen los límites entre las máquinas virtuales individuales.

Hasta ahora en esta introducción estamos hablando de un único Hypervisor el cual es una base de código sobre el cual residen todos los recursos virtualizados de una determinada infraestructura de IT.

¿Podría una determinada vulnerabilidad en el código base del Hypervisor ser explotada a través de un código malicioso y poner a todas y cada una de las máquinas virtuales en riesgo de caer operacionalmente? Pues sí.

La realidad es que debido a la naturaleza de los Hypervisors a través de los host virtuales, una simple pieza de código malicioso que tenga la capacidad de comprometer a una instancia de un Hypervisor, podrá también, fácilmente comprometer a otros también.

La siguiente figura ilustrativa muestra a modo de ejemplo, la introducción de una simple instancia en dónde un código dañino de malware podría rápidamente explotar a cada Hypervisor en la infraestructura de IT. El resultado de dicha replicación es la potencial caída de todas las virtual machines por arriba de los Hypervisors.



Las implicaciones de Seguridad de los Hypervisors

A pesar de que los exploits de seguridad basados en Hypervisors se mantienen en su mayoría al día de la fecha en un ambiente académico, su potencial para fallas masivas en el ambiente de TI, hacen de ellos una importante consideración para aquellos ambientes que han hecho o harán el salto a la virtualización.

Los Hypervisors son por naturaleza código de software, lo que infiere que ocasionalmente se los tiene que actualizar cómo así también patchear y proteger de vulnerabilidades que se encuentren sobre los mismos.

Ejemplos de esta necesidad ya se han visto con Hypervisors en uso hoy en ambientes productivos. Por ejemplo, al día de la fecha del presente artículo el grupo de seguridad SECUNIA ha reportado:

- 19 advisories y 128 vulnerabilidades para la plataforma VMware ESX Server 3.X
- 7 advisories y 14 vulnerabilidades para la plataforma XenSource Xen 3.X

Al igual que con los sistemas operativos tradicionales, la mayoría de las vulnerabilidades basadas en los Hypervisors, están íntimamente ligadas a la necesidad de los derechos administrativos en orden de acompañar su misión. Sin los

apropiados derechos administrativos, el Hypervisor queda fuera del alcance del código de explotación.

Sin embargo, el nivel de madurez relacionado con los derechos y privilegios en entornos de virtualización pueden no ser del mismo nivel que los que ya existen para un sistema operativo como Windows. Si el ambiente de IT no cierra apropiadamente los privilegios y las consolas de acceso a la plataforma de virtualización con el mismo nivel de cuidado que un servicio de directorio, la situación en si misma se ve exacerbada al ataque exitoso de explotación a través de software malicioso.

Ataques basados en Hypervisors: un ejemplo

Veamos un hipotético caso de un ejemplo de la vida real sobre una hipotética empresa dedicada a la salud y medicina cuya estructura de TI ha recientemente terminado una migración sustancial de muchos de sus recursos de servidores a una plataforma virtualizada.

Esta empresa ha estandarizado sus recursos en una única plataforma de virtualización, debido al ahorro de los costos asociados, como así también los beneficios asociados a los sistemas de gestión.

Todos los hosts corren la misma versión de software de solución de virtualización. Sin embargo debido a los tiempos del proyecto de virtualización los hosts fueron puestos online por un período de algunos meses.

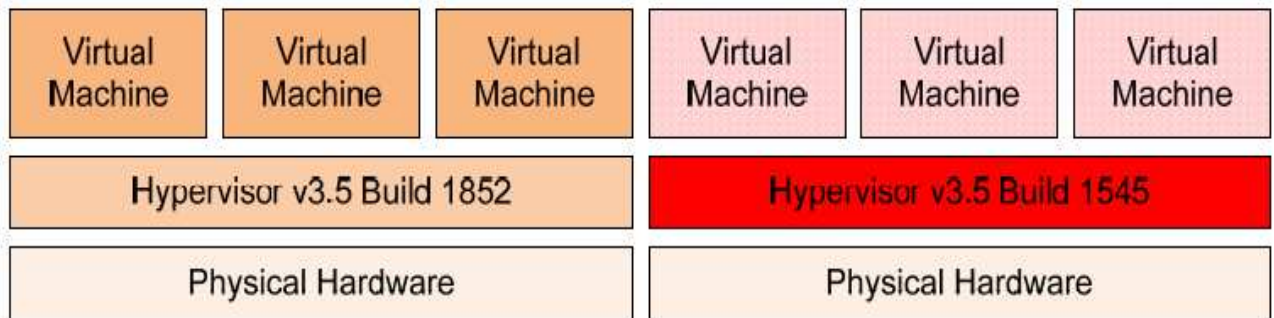
No fue planeado para este ambiente la necesidad de monitorear las versiones de código de los Hypervisors en sí mismos. Además, cómo dijimos, todos los hosts corren la misma versión de software de virtualización. Los hosts que se agregaron en forma posterior al comienzo del proyecto corren una versión (Build) del software de virtualización posterior a los hosts que inicialmente salieron a producción.

Cómo es lógico por parte de los vendors, los cambios ingresados en esta nueva versión fueron hechos para proteger al producto de vulnerabilidades ya publicadas y conocidas.

Al igual que muchas otras empresas de salud y medicina, la red de ejemplo de la empresa opera con un data center centralizado pero con un modelo operativo federado, lo que significa que múltiples oficinas y hospitales comparten los servicios de dicha red.

Debido justamente al modelo federado, los controles de seguridad no se aplican por igual en todas las áreas. En algún momento durante el transcurso de la operatoria diaria, una instancia de replicación de software malicioso es introducida a la red de virtualización infectando versiones previas del software de virtualización.

El resultado final es la pérdida de las máquinas virtuales sobre aquellos hosts que no fueron apropiadamente securizados, cómo se ve a continuación en la siguiente figura:



Previendo los ataques basados a Hypervisors

El ejemplo que estuvimos mencionando en el punto anterior es sólo uno de los tantos y que se resuelve fácilmente si se aplican correctamente los parches, pero los ataques basados a Hypervisors pueden venir de múltiples vectores. En adición a esta complejidad las vulnerabilidades existentes en el mercado de hoy son propensas a impactar cualquier solución de virtualización del mercado.

Con tantos entornos aprovechando hoy, el uso de múltiples soluciones de virtualización, las cuales dependen de la herramienta propia del proveedor para el scanning, los administradores pueden verse con un añadido importante de carga de trabajo relacionada con la verificación de la seguridad de su seguridad virtual.

En orden de reconocer y prevenir de la mejor manera los ataques basados en Hypervisors, las organizaciones de IT deberían considerar las siguientes sugerencias en pos de mejorar la seguridad de sus ambientes virtualizados:

Identificar vulnerabilidades en el Hypervisor a través de vulnerability system

Los ataques basados en Hypervisors existen en el disco y en la red de la misma manera en que el malware tradicional hace con los sistemas operativos reales, por ende, el localizar software potencialmente no requerido significa reconocer su propia heurística. Usando de forma efectiva una solución de vulnerability assessment las organizaciones pueden escanear a sus Hypervisors en busca de parches no instalados y planificar las ventanas de control de cambios para mitigar cualquier posible riesgo.

Evitar Exposición a la red

Los ambientes de virtualización normalmente gozan de un gran nivel de agilidad en términos de configuración de red. Esencialmente, hoy, con todas las soluciones de virtualización, incluyendo los componentes virtuales de networking dentro del Server virtual, es perfectamente posible restringir el tráfico de aquellas conexiones con acceso al Hypervisor.

Separar las redes de gestión

Una forma en que los puntos anteriores pueden llevarse a cabo es a través de una separación lógica de las redes de gestión de aquellas utilizadas por las máquinas virtuales en sí. Las máquinas virtuales y su respectivo tráfico de red normalmente no es necesario que tengan acceso de red directo a aquellas redes utilizadas para la gestión del Management del entorno de virtualización.

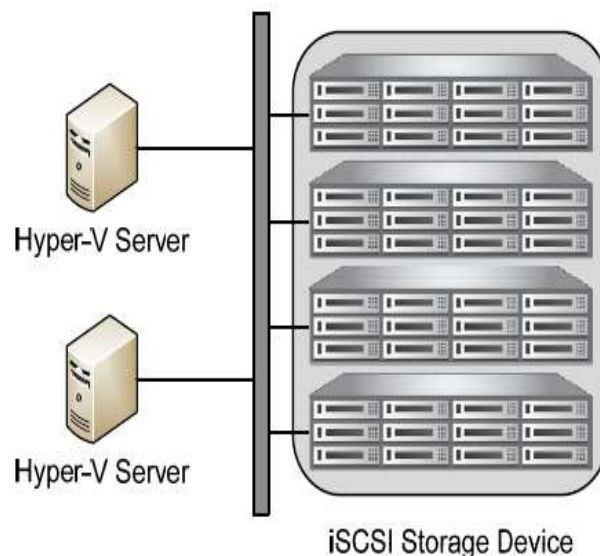
La separación de tráfico a las redes de uso exclusivo para los límites de la gestión del Hypervisor, evita en gran forma la exposición.

Se podría hablar mucho más sobre este tema ya que el mismo es gigante y se deriva a muchos otros más relacionados también a varias de las estructuras de Cloud computing, tema sobre el cual ya también les hablaré un poco más en detalle.

Para finalizar me gustaría dejarles una serie de puntos de recomendaciones a modo de resumen de todo lo hablado hasta ahora.

Resumen de recomendaciones:

- Deberán existir al menos dos Hypervisores ya que se debe hacer énfasis en la redundancia de la plataforma de la infraestructura VDI ante la posible caída de un Hypervisor, además del parcheo del mismo. Tanto en el datacenter central como en el de contingencia.



- Deberá existir una estricta política y procedimiento que la cumpla en cuanto al parcheo de la misma ya que el Hypervisor en sí mismo no deja de ser una capa de software de código que interactúa entre la capa de hardware y las virtuales en si misma. Por lo cual un código malicioso que explotara una vulnerabilidad de una instancia de un Hypervisor podría rápidamente explotar otra instancia también.
- El acceso al Hypervisor se deberá realizar solamente a través de la red de Management.
- En lo posible, el Hypervisor no debería tener una IP propia asignada en el segmento LAN.
- En el caso que si posea una dirección IP interna, la misma deberá estar filtrada sólo a los usuarios autorizados.

- Deberán estar perfectamente segregadas las funciones de quienes administran el Hypervisor de quienes administran las virtuales.
- Deberán los equipos virtuales estar segurizados con el mismo baseline con el que se seguriza a los desktops físicos.
- Se deberá evitar que las VM's tomen control de los recursos del Host.
- Se deberá utilizar plantillas (Templates) de configuración.
- Se deberá deshabilitar funciones innecesarias o superfluas.
- Se deberá monitorear el uso de la consola de administración del Hypervisor.
- Monitorear (si es posible, prevenir) la conexión de dispositivos externos al Hypervisor para ser utilizados por las VM's.
- Se deberá deshabilitar operaciones de copia/pegado entre el S.O. Guest y la consola de administración remota (En caso que aplique).
- Se deberán definir procesos de Operación, Soporte, Optimización y Cambio de la infraestructura de virtualización.
- No utilizar discos que no sean persistentes (Undo).