Seguridad En Entornos Virtuales "Aplicando la Informática Forense"

Alarcón López pablo Ignacio, Ramírez Clavijo Edwin Ricardo

Universidad Piloto de Colombia

Resumen - En Colombia la virtualización es un tema que durante los últimos 4 años ha venido impactando en los datacenter de las empresas, debido a su facilidad de implementación, costos y grandes beneficios como, menos infraestructura a utilizar, rápido despliegue de máquinas, Costes en mantenimiento etc. Uno de los temas importantes es como se estállevando a cabo los procedimientos de obtención de información, tratamiento y custodia de la misma en un caso legal de acuerdo a las leyes colombianas actuales que me garanticen la confidencialidad integridad y disponibilidad de la misma. Existe una ciencia que permite obtener información valiosa a través de procedimientos realizados por personal experto y es la Informática Forense. En esta etapa se detallaran cada una de las fases y las recomendaciones a tener en el momento de adquirir y analizar información, al igual que las leyes por las cuales es regida actualmente en nuestro país.

Palabras Claves: Virtualización, Seguridad, Forense, Evidencia, Cadena de custodia, Imágenes, Hash, legislación.

I. INTRODUCCION

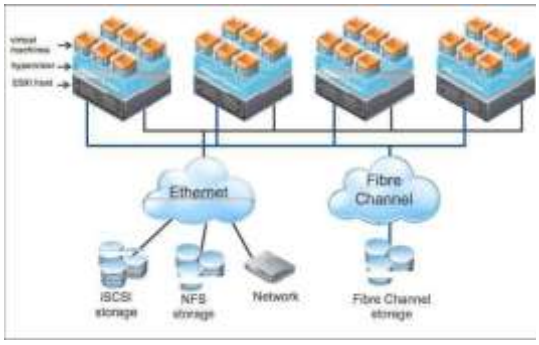
*La virtualización*de infraestructura en los Datacenterestá jugando un papel muy Importante en el campo del almacenamiento y procesamiento de información, pero ¿Cuáles son las principales líneas de actuación, con las nuevas tendencias aplicables a Data Centers? Se busca converger y unificar, todos los servicios en un lugar determinado, eliminando elementos, ahora innecesarios. LasPrincipales líneas de actuación se están centrando en: Simplificación de las arquitecturas de los Data Centers,(Re) Diseño de la infraestructura IP,Incorporación del *switching*virtual (conmutación de datos), Virtualización de sistemas, virtualización de la seguridad.La Virtualización actual se ha desviado de sus raíces originales como una herramienta de multiplexado para convertirse actualmente en una solución para hacer frente a los problemas de seguridad, con habilidad y administración. Este hecho presenta consecuencias positivas y negativas, pues por un lado la virtualización junto con sus técnicas asociadas ayudan a resolver múltiples problemas de seguridad, especialmente porque las máquinas virtuales corren sobre un único sistema, el cual puede implementar un sistema seguro multinivel con sistemas virtuales separados en cada nivel. Por otro lado la virtualización fabrica espacios para nuevas vulnerabilidades, donde los mecanismos de seguridad tradicionales no están preparados para resolver estos problemas. Esta línea de investigación se suma entonces a la búsqueda de nuevos mecanismos para combatir estos nuevos vectores de ataque. ¿Peroqué procedimiento hacer frente a un Incidente de seguridad en estos entornos virtuales, cuando se hallan pruebas que sean valederas para ser utilizadas como evidencia

ante un proceso judicial? La informática forense es una área de la criminalística que consiste en hacer bien las cosas frente a la evidencia (recoger, embalar analizar, transportar) con el objetivo de que no se pierda su valor probatorio en procesos judiciales, además de hacer experticias forenses sobre información en formato digital, equipos de cómputo, teléfonosmóviles y en general cualquier medio informático.

II. SEGURIDAD EN TECNOLOGIAS VIRTUALIZADAS.

De acuerdo a al NIST Las prácticas de seguridad recomendadas más actuales siguen siendo aplicables en entornos virtuales. La seguridad de una solución de virtualización completa que depende en gran medida de la seguridad individual de cada uno de sus componentes, desde el hipervisor y el sistema operativo anfitrión para los sistemas operativos invitados, aplicaciones y almacenamiento. Las organizaciones deben asegurar todos estos elementos y mantener su seguridad basado en prácticas de seguridad sólidas , tales como mantener el software al día con los parches de seguridad , utilizando las líneas de base de configuración de seguridad , y el uso de firewalls basados en host , el software antivirus , u otros mecanismos apropiados para detectar y detener los ataques . En general, las organizaciones deben tener los mismos controles de seguridad establecidos para los sistemas operativos virtualizados, ya que tienen los mismos sistemas operativos que se ejecutan directamente en el hardware. La seguridad de toda la infraestructura virtual se basa en la seguridad del sistema de gestión de la virtualización que controla el hipervisor y permite al operador arrancar sistemas operativos invitados, crear nuevas imágenes SO y realizar otras acciones administrativas. Debido a las implicaciones de seguridad de estas acciones, el acceso al sistema de gestión de la virtualización debe restringirse sólo a los administradores autorizados. Algunos productos de virtualización ofrecen múltiples formas de administrar los hipervisores, por lo que las organizaciones deben asegurar cada interfaz de administración, ya sea local o remotamente accesible. Para la administración remota, la confidencialidad de las comunicaciones debe ser protegida, como por uso de FIPS algoritmos y módulos criptográficos. Asegurar un hipervisor implica acciones que son estándar para cualquier tipo de software, tales como la instalación de actualizaciones a medida que estén disponibles.

Capas de la Virtualización



Aislamiento de sistemas operativos alojados

El hypervisor se encarga de asignar recursos para cada sistema operativo alojado como Procesador, Memoria, Almacenamiento lo que lo hace independiente un sistema de otro.Si un atacantepuede escaparcon éxito de unsistema

operativo alojadoytener acceso alhipervisor, el atacante podría ser capaz decomprometer la seguridadpara todos lossistemas operativos invitados, ya que el hypervisor es único punto de fallo.

Monitoreo

El hypervisor controla cada sistema operativo, así como puede incorporarcontroles de seguridadadicionales ointerfazcon los controlesde seguridad externay proporcionar informacióna los quesereunió através de la introspección. El Monitoreo de tráficode redes particularmenteimportante cuandose está realizandotrabajo en red entredossistemas operativosalojadosen el hosto entre unsistema operativo alojadoy el sistema operativohost.

Imágenes y Gestion de snapshop

Se debe Tener en cuenta queuno de los mayoresproblemas de seguridadcon imágenese snapshopes que contieneninformación confidencial(comocontraseñas, datos personales, etc.)al igual que undisco duro físico. Los snapshop puedenser másriesgosos quelas imágenesporque contienenel contenido dela memoriaRAMen el momento enquese tomó la instantánea, y esto puedeincluirinformación confidencialque ni siquiera sealmacena enla propia unidad.Se debe tener un debido control y seguimiento tanto de las imágenes como de los Snapshop en un lugar aislado y realizar periódicamente un borrado de las mismas.

Seguridad en Hypervisor

Losprogramasque controlan elhipervisordeben protegerse utilizandométodos similaresa los utilizadospara protegerotro software que funcionaen ordenadores de sobremesay servidores ya que toda la seguridad de la infraestructura virtual recae sobre esta.Algunos controles de seguridad a tener en cuenta serian: Instalar Actualización del Hypervisor, Restringir el acceso administrativo de la interface, Sincronizar la infraestructura con un servidor de horario de confianza.

Seguridad en sistemas alojados

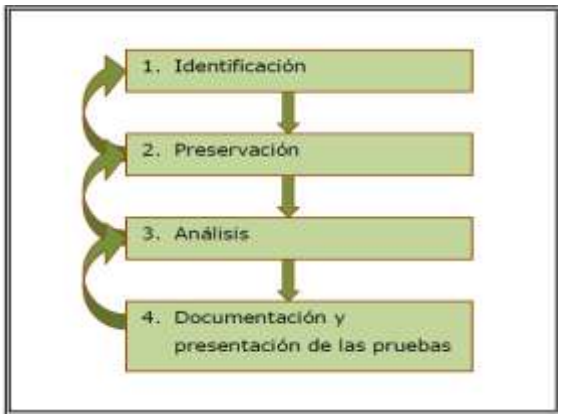
Se deben de seguir las mismas operaciones que se utilizan en entornos físicos como: Instalar las actualizaciones de sistema operativo y aplicaciones, Copias de las unidades virtuales, Desconectar Hardware que no se utilice, Utilizar solución de autenticación diferente para cada una de los sistemas operativos alojados.

III. INCIDENTES DE SEGURIDAD

Es cualquier evento que pueda provocar una interrupción o degradación de los servicios ofrecidos por el sistema o bien afectar la confidencialidad o integridad de la información. ¿Pero quién responde ante estos incidentes? Generalmente las grandes organizaciones cuentan con personal especializado en temas de incidencias de seguridad, incluso poseen su propio departamento de Respuesta de Incidentes, definiendo claramente funciones y responsabilidades para cada persona involucrada en dicho plan; esto es conocido como el CSIRT (Equipo de respuesta a Incidentes de seguridad Informática).

IV. INFORMATICA FORENSE

Metodología de AnálisisForense



Cada día que pasa, la informática forense adquiere gran importancia dentro de las tecnologías de información ya que es habitual encontrar nuevas amenazas para la seguridad informática, los delitos informáticos son cada vez más complejos, por lo cual profesionales de las tecnologías de la información deben trabajar junto con los entes judiciales para poder llevar a cabo a procesamiento a las personas que utilizan estas tecnologías para realizar estos delitos.

La informática forense es la rama de la informática relacionada con la obtención y el análisis de los datos contenidos en medios de almacenamiento tecnológicos (magnéticos, ópticos, en duro entre otros) de tal forma que su información pueda ser utilizada como EVIDENCIA PROBATORIAante un ente judicial o autoridad respectiva (Jefe, Coordinador, gerencia, entre otros) demostrando la responsabilidad sobre un hecho cuyas sanciones podrían llevar a ser penales y/o administrativas. Para ambientes virtuales como Vmware se utilizan las mismas técnicas forenses ya que un entorno virtual se tiene los mismos componentes que una maquina física (memoria, CPU, Disco duro, Sistema Operativo, etc.) Frecuentemente se publica en internet, noticias y blogs de equipos de seguridad reportes sobre vulnerabilidades, fallas humanas, errores de procedimientos y mala configuración de los equipos y aplicaciones de seguridad que presentan un escenario perfecto para que se lleven a cabo incidentes y delitos informáticos.

- *Evidencia Digital*

Es cualquier registro generado por o almacenado en un sistema computacional que puede ser utilizado como evidencia en un proceso legal

Características de la Evidencia Digital

La evidencia Digital posee las siguientes características:

- Anónima
- Volátil
- Duplicable
- Alterable
- Eliminable

Estas características son indispensables para una buena identificación y el análisis, que exige al grupo de seguridad en procedimientos, como en técnicas y herramientas tecnológicas para obtener, custodiar, revisar, analizar y presentar la evidencia en una escena del delito. Antes de realizar el proceso de análisis forense se debe considerar los siguientes elementos para mantener la idoneidad del procedimiento forense:

Esterilidad de los medios informáticos de trabajo:

Los medios informáticos utilizados deben estar libres de variaciones magnéticas, ópticas (láser) o similares. La esterilidad de los medios es una condición fundamental para el inicio de cualquier procedimiento forense en informática.

Verificación de las copias en medios informáticos:

Las copias efectuadas en los medios previamente esterilizados, deben ser idénticas al original del cual fueron tomadas, para esto, se debe utilizar algoritmos como Hash; También se recomiendacrear dos copias en caso de posibles problemas o en su análisis o que se pueda llegar a perder por algún motivo.

Documentación de los procedimientos, herramientas y resultados sobre los medios informáticos analizados:

Los resultados obtenidos del análisis de los datos, deben estar claramente documentados, describiendo entre otros las herramientas utilizadas, versiones y el paso a paso en cada una de las etapas de recolección y análisis de la información.

Mantenimiento de la cadena de custodia de las evidencias digitales:

La custodia de todos los elementos debe estar documentada por cada uno de los eventos que se han realizado con la evidencia en su poder. Quién la entregó, cuándo, en qué estado, cómo se ha transportado, quién ha tenido acceso a ella, cómo se ha efectuado su custodia.

Informe y presentación de resultados de los análisis de los medios informáticos:

Generalmente existen dos tipos de informes, los técnicos con los detalles de la inspección realizada y el ejecutivo para la gerencia y sus dependencias.

Administración del caso realizado:

Mantener un sistema automatizado de documentación de expedientes de los casos, con una adecuada cuota de seguridad y control, es labor necesaria y suficiente para salvaguardar los resultados de las investigaciones y el debido cuidado, diligencia y previsibilidad del profesional que ha participado en el caso.

Auditoría de los procedimientos realizados en la investigación:

Mantener un ejercicio de autoevaluación de los procedimientos, para contar con la evidencia de una buena práctica de investigaciones forenses, de tal manera que el ciclo de calidad: *PHVA*- Planear, Hacer, Verificar y Actuar sea mejorada cada día.

V. PROCEDIMIENTOS FORENSESAPLICADOS

- Análisis técnico- factico:

Al identificar que hay un proceso judicial y que se halla presente evidencia, se debe de utilizar una metodología para poder llevar a cabo la investigación, teniendo presente que dispositivos se han de analizar para construir la información a analizar y no indagar sobre supuestos.

- Identificación de los Medios de almacenamiento implicados en la investigación:

Identificar los medios implicados en la investigación para determinar la mejor estrategia y metodología en la utilización de herramientas para capturar los dispositivos de una forma segura

- Inicio de la Cadena de Custodia:

Se debe seguir un estándar o norma que aplique las mejores prácticas, utilizando las tecnologías necesarias desde el inicio de la investigación hasta la terminación de la misma permitiendo dar validez en cualquier país que se requiera, que garantice una cadena de custodia totalmente valida donde no se viole

los principios básicos de la información (Integridad, confidencialidad y disponibilidad).

- Captura de los Medios de Almacenamiento originales:

Se debe tener en cuenta que el proceso de captura de evidencia digital no debe de alterar el escenario objeto de análisis. Es conveniente utilizar herramientas gravadas en CD o Pendrive que se puedan ejecutar directamente y no afecten a la imagen en los discos duros del sistema. La captura de evidencia Volátil se debe de llevar a cabo primero que todo, pues al apagar el equipo informático objeto de análisis se perderá información valiosa. Entre la recolección de datos volátiles se encuentran:

1. Volcado de Memoria: Al no poder realizar un análisis en profundidad se llevara a cabo el volcado de memoria para determinar cadena de caracteres que den indicios sobre el incidente que ha afectado al equipo.

2. Procesos y Servicios: identificar cada proceso y servicio, quien lo está ejecutando para comparar la situación estable del sistema.

3. Controladores: Drivers instalados para gestionar distintos recursos de Hardware del sistema.

4. Información de la situación y configuración de los servicios y las tarjetas de Red:Muestra la Configuración de tarjetas de red, protocolos, cache de DNS y puertos entre otros.

5. Usuarios Y Grupo de usuario Activos dentro del Sistema: Obtener sesiones que se encuentran abiertas al igual que usuarios.

Una vez recolectada la evidencia volátil se procederá a tomar la imagen de los discos duros del sistema. Existen 2 tipos de imágenes:

1. *Imagen lógica: Es la imagen que yo realizo en vivo con la maquina encendida, que por el valor de la información que se maneja y los servicios que presta es imposible su apagado. Es conveniente tomar imágenes fotográficas de todas las pantallas que muestra el sistema informático durante el proceso de captura de evidencia.*

2. *Imagen Física:para la toma de imagen Física es necesario apagar la maquina desconectándola directamente de la fuente de alimentación. Seguidamente se procederá a arrancar el sistema desde un medio buteable como podría ser un Linux, o conectando los discos objeto de investigación en una maquina destinada únicamente para análisis forense a través de dispositivos de blanqueamiento ubicado en un laboratorio forense. Durante el proceso de captura se copiara bit a bit del disco utilizando herramientas que incorporen códigos de comprobación (algoritmos como SHA-1 o MD5) que permite la integridad de los datos y certificándolo legalmente con estampas cronológicas de fecha y hora de los medios de almacenamiento originales, garantizando la cadena de custodia tanto del original como de las copias tomadas.*

- Volcado de las Imágenes Forenses en el laboratorio

Una vez realizada las imágenes estás se descargaran y se comprobaran la integridad de los datos en los sistemas de información del laboratorio forense para ser posteriormente analizadas.

- Recuperación de datos Borrados y de ambiente.

El experto forense puede recuperar información que había sido borrada, para ser utilizada como pruebas para argumentar un proceso judicial.

- Filtrado y análisis de Documentos relevantes

Los expertos deben de utilizar las últimas tecnologías para filtrado y análisis de documentos que permita localizar más fácil y rápidamente la información que se requiere en dicha investigación.

- Identificación y Extracción de las pruebas.

Toda información que represente pruebas significativas para la investigación y que se pueda tomar como prueba electrónica dentro de un caso judicial.

- Reconstrucción de la Cadena de acontecimientos.

El análisis de la evidencia no busca siempre el mismo objetivo como la recuperación de información, también se basa en la obtención de hechos históricos como el borrado, impresión o eliminación de alguna información que son a veces decisivos en proceso judiciales.

- Presentación de Resultados, elaboración del informe Final o base de opinión pericial y ratificación en juicio.

Desde el momento que inicio la investigación los profesionales en seguridad informática, Peritos y/o expertos en análisis forenses deben estar preparados para ser llamados a rendir declaración en un juicio donde se presentaran las respectivas pruebas.

VI. NORMATIVIDAD Y LEGISLACION

En cuanto a la parte legal la Ley 527 de 1999 y ley 1273de 2009 son normas dentro de la ley Colombiana que nos permite penalizar un incidente de seguridad en dado caso que exista y se pueda mostrar evidencia válida y acusatoria para tal fin.

En los entornos de virtualización de infraestructura se puede llegar a dar el caso en el que se tenga que demostrar que unas de estar normas haya sido violada, para imputar una demanda hacia funcionarios de la compañía o terceros que pudieran ser los responsables del incidente de seguridad.

Los procedimientos que se deben seguir para realizar la respectivarecolección de evidencia, cadenas de custodia y análisis del mismo, para posterior mente imputar demandas penales a él o los responsables deber ser tratado exactamente igual como si se tratase de un equipo de cómputoportátil, de escritorio o servidor.

Para la ley le es indiferente el entorno en el que se encuentre la evidencia acusatoria, La correcta recolección del materia acusatorio no debe distorsionar el proceso así sea un entorno virtual o físico.

VII. CONCLUSIONES

La virtualización de infraestructura actualmenteestá dirigida a las empresas como solución de integración de servidores físicos e integrador de servicios así como también sistemas de información en una infraestructura física mucho más compacta, flexible y fácil de administrar. Por tal razón el aseguramiento de estas debe ser de gran impacto en su implementación como en su posteríosadministración.

La informáticaforense aplicada a entornos de trabajo virtual, puede llegar a ser más compleja, delicada y requiere de un nivel de experticia mayor que al de un incidente de con equipo portátil o computador de escritorio; Se debe tener un alto grado de conocimiento en seguridad en virtualización y manejo de infraestructura virtual, para poder realizar un buen análisisforense y que de igual manera sea válidaantes los estrados judiciales en dado caso que se quiera proceder con algún proceso penalen contra de alguien.

La obtención de evidencia como lo pueden ser imágenes de discos, datos volátiles, se pueden complicar un poco ya que para entornos virtuales no hay muchas herramientas forenses disponibles para realizar este tipo de procedimientos. En genera lo que se recomienda es realizar una copia completa de la máquina virtual para posteríos meteanalizarla en un estaciónforense previamente adecuada para analizar esta máquinavirtual.

Se puede determinar que esta práctica de análisisforense en entornos virtuales se puede realizar siguiendo una serie de pasos y procesos para no afectar la evidencia y su valor probatorio en un estrado judicial.

REFERENCIAS

[1.] http://www.adalidabogados.com/Pruebas%20T%E9cnicas.Pdf
[2.] http://www.adalidabogados.com/Cadena%20de%20Custodia%20E_Evidence.pdf
[3.] NIST National Institute of Standards and technology special Publication 800-125U.S Department of commerce
[4.] Guide to security for full virtualization Technologies Recommendations of the National Institute of Standards and technology
[5.] Enciclopedia de la seguridad informática 2a Edición Actualizada Álvaro Gomez Vieites Editorial Alfaomega
[6.] Poder Público - Rama LegislativaLEY 527 DE 1999(agosto 18)por medio de la cual se define y reglamenta el acceso y uso delos mensajes de datos,del comercio electrónico y de las firmas digitales, y seestablecenlas entidades de certificación y se dictan otras disposiciones.
[7.] LEY 1273 DE 2009(enero 5)por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

Autores
Pablo Alarcón, Ingeniero de Sistemas, experto en seguridad informática, con certificación en Microsoft VirtualizaciónCertificación y VMware Certified Professional 4 - Data Center Virtualización (VCP4-DCV).

Edwin Ramirez, Ingeniero de sistemas con énfasis en tele comunicaciones, Experto en seguridad informática, Experiencia en análisisforense y Penetración Testing.