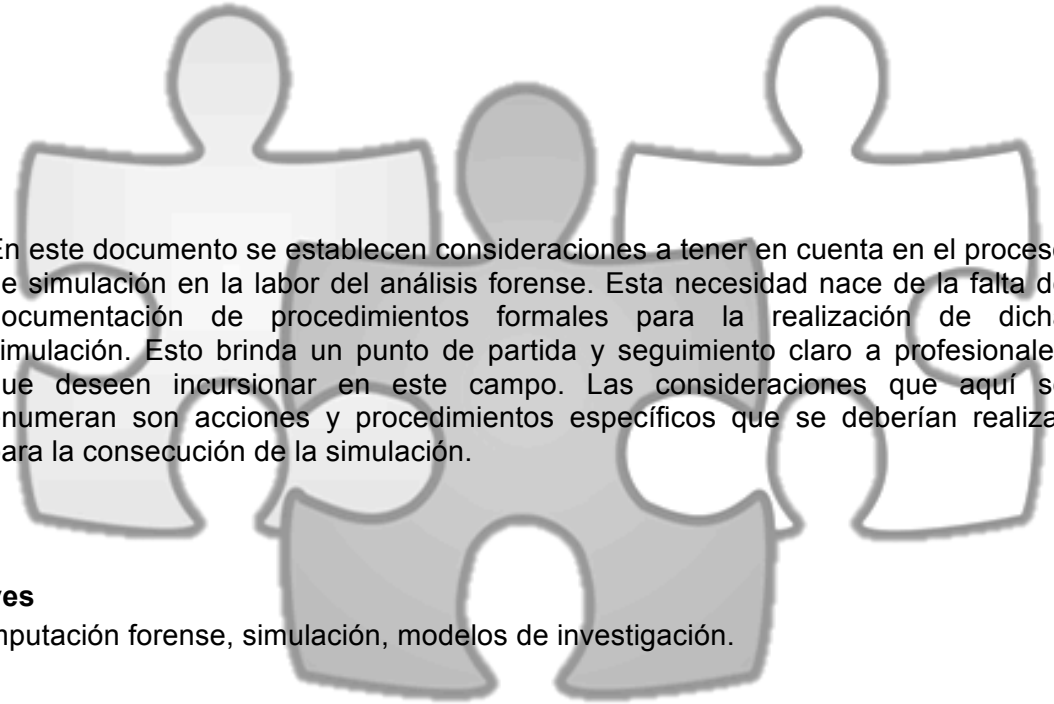
CONSIDERACIONES A TENER EN CUENTA PARA REALIZAR AMBIENTES SIMULADOS EN LA LABOR DE LA COMPUTACIÓN FORENSE.

Martin Alonso Castillo Gómez[1]

Universidad Pontificia Bolivariana
Bucaramanga, Colombia
ingmac11@gmail.com



Resumen

En este documento se establecen consideraciones a tener en cuenta en el proceso de simulación en la labor del análisis forense. Esta necesidad nace de la falta de documentación de procedimientos formales para la realización de dicha simulación. Esto brinda un punto de partida y seguimiento claro a profesionales que deseen incursionar en este campo. Las consideraciones que aquí se enumeran son acciones y procedimientos específicos que se deberían realizar para la consecución de la simulación.

Palabras claves

Computación forense, simulación, modelos de investigación.

[1] Ingeniero de Sistemas de la Universidad Cooperativa de Colombia Seccional Barrancabermeja

Abstract

This document show tips to take about the simulation process at the work of forensic analysis. This need arises from the lack of documentation of formal procedures for execute such simulation. This provides an initial point and clear tracing to professionals who wish to learn this field. The considerations listed here are specific steps and procedures should be performed to achieve the simulation

Keywords:
Computer forensics, simulation, investigation models.

1. Introducción

La simulación, en la labor de la computación forense, permite al informático forense conocer y documentar el funcionamiento de cierta herramienta sobre un ambiente determinado. Por otra parte, la simulación de un incidente sirve como apoyo a la reconstrucción de los hechos, permitiendo estudiar dicho comportamiento para esclarecer posibles dudas que se llegaran a presentar.
Los procedimientos de simulación en este ámbito los realizan los peritos informáticos teniendo como base su experticia y experiencia, mas no siguiendo algún proceso documentado o definido. En el transcurso de este documento se establecerán consideraciones generales a tener en cuenta al realizar una simulación en el proceso del peritaje informático, definiendo así un punto de partida claro para profesionales que no tengan la experiencia suficiente en este campo.
El artículo contará inicialmente una explicación del por qué y de la importancia de realizar simulaciones y como esto apoya la labor del informático forense, además se muestra el contexto dentro del cual se realiza la simulación. Seguidamente se presentan las consideraciones a tener en cuenta para la labor y finalmente se plasman las conclusiones y el trabajo futuro que queda por realizar.

2. Simulación en la labor del informático forense.

2.2 Por qué realizar una simulación.

Realizar una simulación puede tener dos objetivos, conocer el funcionamiento y comportamiento de una determinada herramienta o estudiar el comportamiento completo de un incidente, esta simulación servirá para reforzar o definir el establecimiento de la hipótesis de lo sucedido.

Al estudiar una herramienta no basta con leer solo su documentación ya que esta podría comportarse de manera diferente dependiendo del ambiente en el que se encuentre, por lo tanto, no se puede garantizar, por ejemplo, que funcionará de la misma manera en un equipo con Windows Server 2000 que en uno con Windows Server 2008 R2.

Por otra parte, al simular el incidente completo se puede tener una visión completa y global de lo que podría haber ocurrido.

2.2 La simulación dentro del proceso de cómputo forense.

En la actualidad, existen diversos modelos utilizados para realizar el proceso de computación forense. El artículo Common Phases Of Computer Forensics Investigation Models [1], establece, en orden cronológico de publicación, los modelos existentes, explicando cada uno de ellos y plasmando cuáles son sus fases comunes; fases como: identificación, recolección, análisis y presentación, por nombrar algunas. La fase de análisis es donde comienza el trabajo real y se comienza a construir las hipótesis [2], además de ser la fase que más se repite dentro de los modelos existentes. En esta fase se realiza el proceso de simulación, y ya que se han identificado y recolectado las evidencias con las cuales se trabajará y comenzará a estudiar. De este análisis saldrá la hipótesis de lo sucedido y la reconstrucción de los hechos, los cuales serán soportados por los resultados de la simulación que se realizará. La Figura 1 muestra las fases de tres modelos de investigación de cómputo forense[2]:

modelo DFRWS (Digital Forensics Research Workshop), el modelo ADFM (Abstract Digital Forensics Model); basado en el DFRWS, y el modelo DFMMIP (Digital Forensic Model based on Malaysian Investigation Process). Como se puede apreciar, la fase de análisis se encuentra presente en los tres modelos.

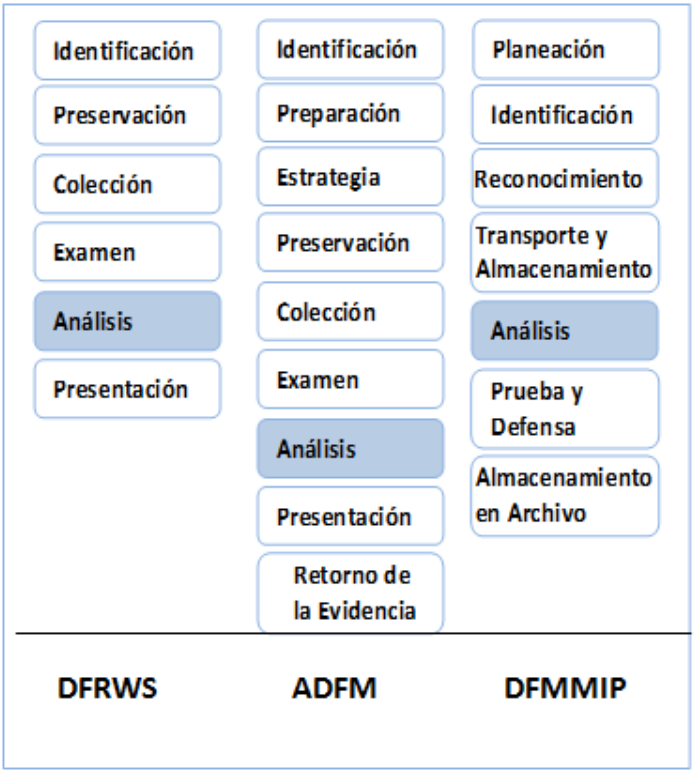


Figura 1. Modelos de Investigación en Cómputo Forense

[2] Dado que este articulo cubre solo el proceso de simulación, no se entrará en detalle en la explicación de cada modelo.

2.3 Quienes participan en el proceso

En un proceso de análisis forense, existen distintos roles que interactúan con el objetivo de llegar a encontrar la verdad de lo ocurrido. El Dr. Jeimy Cano en su libro computación forense, descubriendo los rastros informáticos [3], habla sobre los roles y responsabilidades del investigador forense en informática, definiendo ocho roles entre los cuales se encuentra el especialista en informática y el analista en informática. Estos dos roles se encargan de identificar las pruebas, detallar el modelo de investigación, examinar los datos, examinar elementos hardware o software de la escena del crimen, entre otros. Aunque la definición y establecimiento de roles dependerá finalmente de los recursos disponibles para la investigación.

3. Consideraciones en la ejecución de la simulación.

3.1 El ambiente de simulación.

Si bien es cierto que el ambiente simulado es un modelo de un ambiente real, este no necesariamente debe tener tanto detalle, ya que se puede volver costoso el reconstruirlo, y tampoco debe ser demasiado básico, pues puede arrojar resultados engañosos [4]. Se debe tener en cuenta además que "la esencia de la técnica del modelado es la abstracción y la simplificación"(Ídem)[3] , por lo tanto, si se va a realizar la simulación de un incidente ocurrido sobre un equipo de la gerencia con Windows XP, que tenía archivos confidenciales, el ambiente de simulación como mínimo debe contar con el mismo sistema operativo, antivirus (si es posible con la misma base de firmas), entre otros, pero no contaría, por ejemplo, con su programa de reproductor de música, su paquete de ofimática, etc. Es puntual definir lo que va a contener el ambiente de simulación.

3.2 El contenido del ambiente de simulación.

En el punto anterior se plasmó lo que podría incluir un ambiente simulado, pero es importante esclarecer lo qué se debe tener en cuenta a la hora definir el contenido del ambiente simulado.

Se puede dar por entendido que si el incidente se presentó en un servidor o en un computador de escritorio, lo mínimo que debería tener es el mismo sistema operativo de la maquina intervenida, ya que de allí parten el resto de atributos. Lo mismo sería si lo que se quiere es probar el funcionamiento de una determinada herramienta.

Cuando se trata de un servidor, además de su sistema operativo, se debe contar con los servicios que ofrecía, ya que estos abren puertos por donde deben funcionar, alterando la configuración inicial del sistema operativo. Si se tiene acceso a la copia de la imagen de la evidencia, se debería montar y comparar que los puertos abiertos de ésta y del ambiente

[3] El texto original dice: "The essence of the art of modeling is abstraction and Simplification".

simulado sean los mismos; con esto se asegura que al menos en las características de los puertos los dos ambientes son similares[4].

3.3 Igualando la Seguridad

Un aspecto a tener en cuenta en el ambiente de simulación, además de lo visto hasta hora, son los niveles y controles de seguridad implantados. Anteriormente se hablaba de la misma firma de antivirus, pero hay que tener en cuenta otros factores como el firewall del sistema operativo u otro Software de la misma índole.

Si la maquina afectada es un servidor Linux, se debería verificar la configuración del IPTABLES, si es un servidor web, verificar la existencia de un modulo de seguridad como Mod_security en caso del servidor web Apache[5] .

Lo importante es que el ambiente de simulación cuente, lo más cercano posible, con el nivel de seguridad del ambiente real, ya que esto afectaría el curso de la simulación del incidente y por ende la validación de la hipótesis planteada.

3.4 Planeación de la simulación

Antes de iniciar la respectiva simulación, se debería planear lo que se va a ejecutar, con el fin de tener claro las acciones a realizar, las herramientas a utilizar y el orden de ejecución de estas. La creación de un modelo conceptual o un diagrama de flujo sería un apoyo ideal para ello y que brindaría además un factor de orden en el proceso de simulación.

3.5 Estudiando las Herramientas

Es importante tener el conocimiento técnico de cómo funciona una herramienta antes de iniciar la simulación del incidente, ya que los errores de ejecución o aplicación de la herramienta al ser utilizada, podría afectar el resultado de la simulación.

Para el estudio de la herramienta es recomendable hacerlo en otro ambiente alterno al que se va a utilizar como ambiente para la simulación final, con esto se evita que se contamine el ambiente antes de su uso real.

3.6 Tener cuidado con el Antivirus.

Algunas herramientas de penetración son consideradas como archivos sospechosos por las firmas de los antivirus, incluso algunos de ellos solicitarán o exigirán que se ejecuten en modo SandBox . Es por ello que en ciertas ocasiones se deberá desactivarlo completamente o sólo el

[4] Se debe tener en cuenta que el objetivo de este artículo no es la enseñanza del uso de herramientas como las de escaneo de puertos o de estudio de imágenes de evidencia, por lo tanto si se especifica alguna situación, será solo la que aporte al tema de ambientes simulados.

[5] Tener en cuenta que un módulo como el Mod_Security tiene cientos de reglas y estas deberían ser similares en el ambiente simulado.

proceso que solicita el uso del SandBox[6]. Pero esto es únicamente para la máquina atacante, ya que la máquina víctima si deberá poseer los atributos similares a la máquina afectada real. Lo mismo sucederá en su momento con el firewall del sistema, algunos bloquearán inclusive las solicitudes de paquetes ICMP entrantes. La Figura 2 muestra un ejemplo del Antivirus Avast, solicitando ejecución en SandBox.

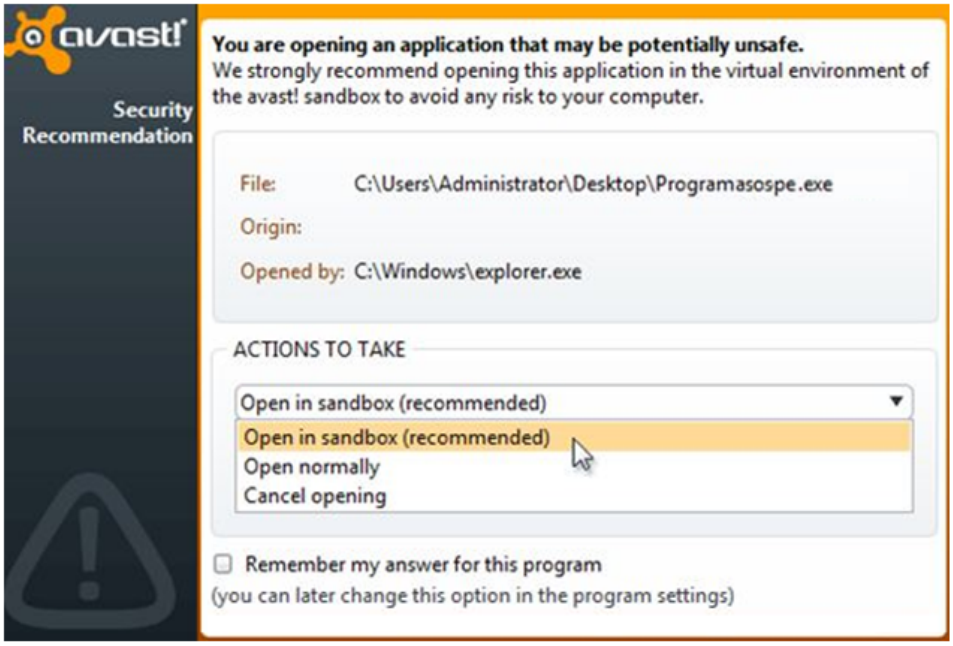


Figura 2. *SandBox* de Avast Antivirus.

3.7 El ambiente del ambiente simulado.

Cuando se realiza una simulación, esta se realiza en un ambiente alterno al cual sucedieron los hechos que requirieron la intervención de un informático forense. Este ambiente puede ser tanto virtualizado (sobre software de virtualización como VMWare o Virtual Box) o también sobre ambientes alternos similares a los reales. La virtualización se define como una tecnología que utiliza un entorno lógico para superar las limitaciones físicas en el hardware [6]. Aunque este artículo se desarrolló con prácticas y experiencias en ambientes virtualizados, lo que aquí se describe puede ser usado como referente también en otro tipo ambientes alternos.

La escogencia del tipo de ambiente alterno dependerá de varios factores como tiempo, dinero, espacio habitacional. El factor monetario es crucial ya que el costo de trabajar sobre máquinas virtuales se reduciría en comparación a la recreación de un ambiente alterno real; la adquisición de equipos, servidores, software, entre otros, aumentaría el costo de este ambiente.

[6] SandBox, es una especie de aislamiento de procesos que poseen algunos antivirus para proteger su sistema de cualquier aplicación sospechosa. Una definición general de Sandbox es: "un entorno aislado, creado para ejecutar y probar las aplicaciones que podrían ser un riesgo de seguridad." [5].

Los tiempos para conseguir los equipos necesarios, su configuración y puesta en marcha serían mayores en el ambiente alterno real; en la virtualización es cuestión de poner en marcha el software de virtualización e instalar lo necesario.

El espacio habitacional favorece al ambiente virtualizado ya que en una sola máquina se pueden instalar tantas máquinas virtuales como sea necesario[7].

3.8 Documentación al detalle.

En la ejecución de la simulación se debería ir documentando paso por paso cada una de las acciones realizadas y al mismo tiempo ir verificando qué sucede o de qué manera ha afectado al sistema; nada debe pasarse por alto. Se debe tener presente que "la documentación es de suma importancia para cualquier investigación y no debe pasarse por alto" [7], esto ayuda a tener control sobre lo que se está haciendo. Si por algún motivo se ejecuta una acción no programada o no diseñada, se puede llegar a alterar el ambiente y por ende el resultado, ya que el flujo de trabajo que se llevaba ha sido interrumpido o alterado. Si se está documentando todo detalladamente regresarse no debería ser ningún problema, aunque lo peor que podría ocurrir es que se tenga que reiniciar y reinstalar el ambiente simulado lo que acarrearía pérdida de tiempo y dinero.

Todo lo que se documente debería ser en orden cronológico, esto facilitará la construcción de la línea de tiempo del incidente o de la herramienta analizada[8].

Toda documentación que se realice debería ser etiquetada, esto asegurará la identificación de la misma en el momento que se requiera, además de un trabajo ordenado. Esta etiqueta puede ser un código que sea de fácil reconocimiento por el informático forense o puede ser también lo más explícito que se quiera, por ejemplo, podría tener la fecha, nombre de la herramienta, versión de la herramienta y sistema operativo sobre el cual se hizo la prueba[9].

3.9 Capturando lo que hay en memoria volátil.

Una de las acciones que se puede realizar es la captura de la información volátil en el transcurso de la simulación[10]. Esta información es un insumo importante en la conclusión de los resultados ya que en la variación de cada una de las tomas[11] se puede evidenciar el comportamiento del sistema así como la afectación que está causando la acción realizada ya sea manual o por alguna herramienta de penetración.

[7] Esto dependería de las características de la maquina real y de los atributos que se le den a cada máquina virtual.

[8] Recordar que el proceso de simulación puede ser tanto para el incidente completo como para estudiar el comportamiento de una determinada herramienta.

[9] Respecto al código de etiquetado, podría ser parecido a los utilizados en los sistemas de gestión de calidad para etiquetar los registros: Estos son de fácil entendimiento y ubicación.

[10] Se recuerda que este artículo es solo de ambiente simulados por lo tanto se obviará el proceso de recolección de la información volátil.

[11] Tomas hace referencia a la instancia en la cual se acaba de realizar alguna acción.

Aunque históricamente el análisis forense se ha centrado en un análisis estático, es decir, en el estudio de la imagen forense copiada bit a bit, no se puede desconocer que existe información en memoria que no se almacena en disco o que se pierde una vez apagado el equipo [8]. Dependiendo de las aplicaciones que se utilizan en la recolección de la información volátil, se pueden tener datos como: conexiones de red, datos de sesión, sesiones o conexiones activas, su duración, los servicios ejecutados, entre otros[12].

3.10 El tiempo, factor de análisis en la virtualización.

Uno de los efectos a tener muy en cuenta cuando se simula en ambientes virtualizados son las duraciones de los procesos, ya que el rendimiento en un ambiente virtualizado podría no ser el mismo que el de un ambiente real. Esto quiere decir que si en la simulación, una herramienta de penetración se demoró cierto tiempo ejecutándose, este tiempo podría ser menor o mayor en el ambiente real, por lo que hay que evitar suposiciones con respecto a la duración del ataque. El rendimiento dependerá de entre otras cosas, del método de virtualización usado, ya sea para-virtualización, virtualización completa, virtualización del servidor, entre otros. [10]

3.11 Simulando la red en un ambiente virtualizado.

Cuando se trabaja con más de una máquina virtual y se requiere conectar en red cada una de estas máquinas, es necesario tener en cuenta ciertos aspectos que puede afectar el desarrollo de las acciones posteriores.

El software de virtualización tiene tres opciones de configurar la red para cada una de sus maquinas virtuales[13]: *Bridged*, NAT, *Host Only*.

Con la opción de red en Bridged, se realiza un puente a la tarjeta de red de la máquina real, pudiéndose conectar directamente a la red de la cual hace parte la máquina anfitriona. NAT, ofrece una salida automática a Internet (en caso de que la máquina anfitriona tenga acceso) o la red real, ocultándose detrás de la IP de la máquina anfitriona, el software de virtualización asignará una dirección IP generalmente en el rango de la 10.0.0.0.

Host Only se conectará solamente con la máquina anfitriona y con otras máquinas virtuales existentes; no se conectará con redes externas, pero es una opción si se quiere recrear una red interna con diferentes máquinas virtuales.

Por lo tanto, se debe evaluar lo que realmente se quiere simular para tomar la decisión adecuada.

[12] En contraste con el entorno estático, este tipo de información corresponde a un entorno dinámico; sistemas en vivo y sistemas conectados a internet clasifican en este entorno [9].

[13] Para el desarrollo de este articulo se trabajó con VirtualBox y VMware por lo tanto cualquier característica de maquina virtual que aquí se describa está basado en estos dos programas.

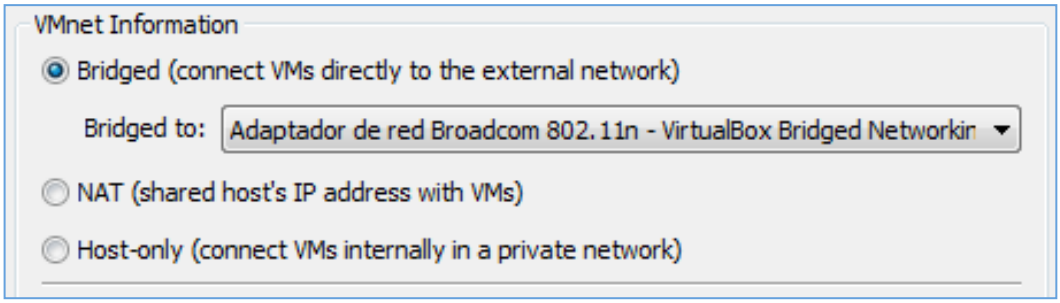


Figura 3. Editor de red virtual de VMware.

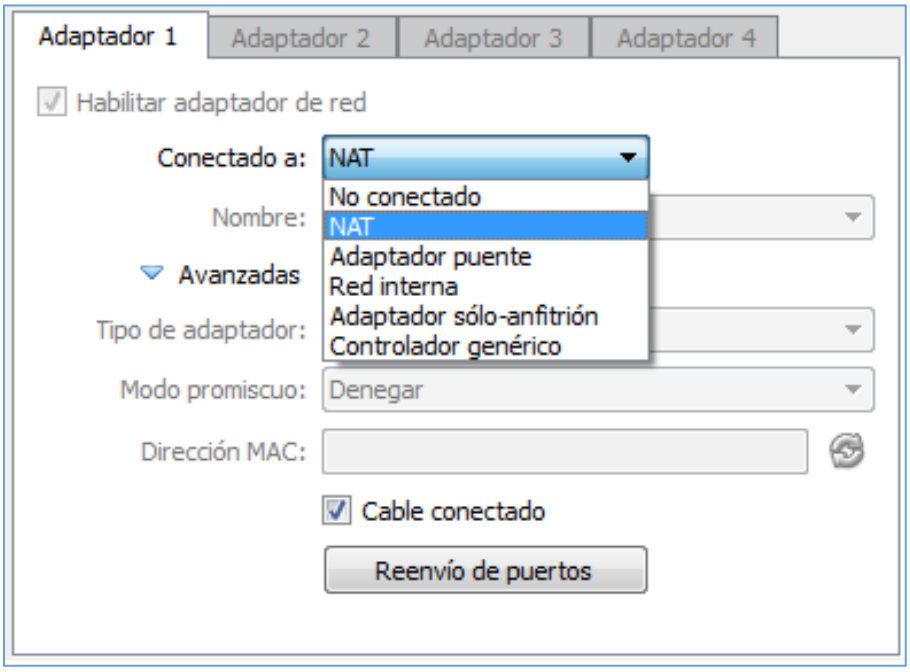


Figura 4. Editor de red virtual de VirtualBox

En las Figuras 3 y 4 se pueden apreciar las configuraciones de red antes mencionadas para el software de virtualización VMware y Oracle VirtualBox respectivamente. Cabe aclarar que la configuración se realiza para cada interfaz de red física que exista en la maquina anfitriona.

3.12 Comparando los resultados

Cada ejecución de una acción, cada acción que ejecuta una herramienta, puede producir o registrar un evento en la maquina víctima, ya sean logs del sistema o logs de la herramienta misma, modificaciones a registros, archivos o documentos del sistema; Se debe entonces comparar estos resultados con los existentes en la imagen forense y con las evidencias recolectadas. El resultado de esta comparación fortalecerá la hipótesis de lo ocurrido en el incidente o hará que se redefina dicha hipótesis.

3. Conclusiones.

El proceso de simulación ayuda a tener una visión clara de lo que podría haber ocurrido en el incidente, ya que con esto se estudia su comportamiento permitiendo así soportar las hipótesis planteadas.

Por otra parte la simulación es además una buena práctica en materia jurídica ya que tiende a reforzar un veredicto o testimonio de un suceso teniendo como fuente de sustento la simulación del incidente.

La documentación en este proceso es crítica ya que permitirá reunir información de una manera ordenada, conociendo los resultados de cada paso e ir entendiendo el comportamiento del incidente, además que puede servir como insumo de posteriores simulaciones.

4. Trabajos Futuros.

En el actual trabajo, se abordó desde una perspectiva general el proceso de simulación, brindando una serie de consideraciones a tener en cuenta para su ejecución.

Como trabajo futuro se podría plantear un modelo formal para el desarrollo de una simulación, con una serie de pasos estructurados y documentados que facilitarían aún más este proceso.

REFERENCIAS Y BIBLIOGRAFIA

[1] Yunus Yusoff, Roslan Ismail and Zainuddin Hassan, Common Phases of Computer Forensics Investigation Models, International Journal of Computer Science & Information Technology, Vol. 3, Junio 2011

[2] Peter Stephenson, A structured approach to incident postmortems, Information Systems Security, Vol. 12, Octubre 2003

[3] Jeimy J. Cano, Computación Forense, México: Alfaomega, 2009, p. 148

[4] Robert E. Shannon, Introduction to the Art and Science of Simulation, IEEE Systems, Man, and Cybernetics Society, Vol. 6, 1976

[5] John Hoopes, Virtualization for Security, Burlington - USA: Syngress, 2008.

[6] Sungsu Lim, Byeongyeong Yoo, Jungheum Park, KeunDuck Byun, Sangjin Lee, A research on the investigation method of digital forensics for a VMware Workstation's virtual machine, Mathematical and Computer Modelling, Vol. 55, 2012

[7]Keith J. Jones, Richard Bejtlich, Curtis W. Rose, Real Digital Forensics Computer Security and Incident Response, New York: Pearson Education, 2006, p 166.

[8] Hong Guo, Daoli Huang, Ying Zhang, Implication of Virtualization Technologies inn Computer Forensics, Energy Procedia Volume 13, 2011, p. 4133–4137

[9] Sarah Mocas, Common Building theoretical underpinnings for digital forensics research, Digital Investigation, Vol. 1, Feb 2004

[10] Diane Barrett, Gregory Kipper, Vittualization and Forensics, Burlington - USA: Syngress, 2010, p. 12-20

Biografía

MARTIN ALONSO CASTILLO GOMEZ, Ingeniero de sistemas de la Universidad Cooperativa de Colombia, Especialista en Auditoria de Sistemas de la Universidad Antonio Nariño.