1. Manual de uso

El siguiente manual de uso está diseñado para brindarle al usuario un instrumento guiado para poder utilizar y replicar este piloto experimental, para el análisis de una muestra de malware.

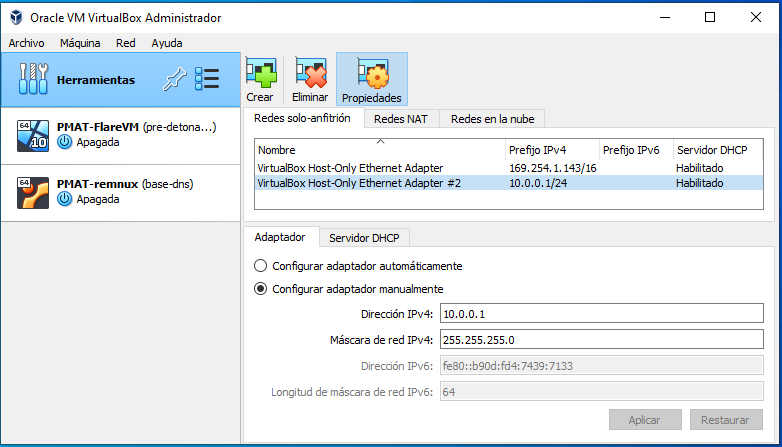
Primero debemos comprender que necesitamos 2 máquinas virtuales, las cuales se puedan comunicar entre sí, pero que no tengan acceso a la red. De esta forma impedimos que al ejecutar un espécimen de malware pueda utilizar capacidades de redes para propagarse y ejecutarse.

Una de las maquinas será infectada o será donde se ejecute el malware, y la otra máquina prestara servicios, para poder analizar el trafico cuando el malware tiene la capacidad de comunicarse con un C&C (Command & Control). La herramienta que utilizaremos como máquina que presta servicios en una distribución de Linux creada específicamente para análisis de malware llamada Remnux.

Para realizar la instalación del laboratorio virtual primero seguimos los pasos explicados en el Anexo A. Luego debemos configurar la red para que las 2 máquinas virtuales se comuniquen:

Configuramos la red que utilizaremos, para poder ejecutar el malware sin poner en riesgo nuestro host físico. Es muy peligroso ejecutar malware en un área de la red que pueda alcanzar nuestro host físico. Colocaremos las 2 máquinas virtuales en una red separada físicamente de nuestro host. Pero que estén lógicamente conectadas, para que se puedan comunicar.

Como el host físico donde se encuentra instalado el entorno virtual está en la red 192.168.x.x. Creamos un nuevo adaptador de red “**Ethernet Adapter #2**” y configuramos el rango de dirección IP de las máquinas virtuales de forma que sea notablemente diferente de la red de mi área. Para esto configuramos la dirección IP en “**10.0.0.1/24**”.



**Fuente:** Elaboración propia

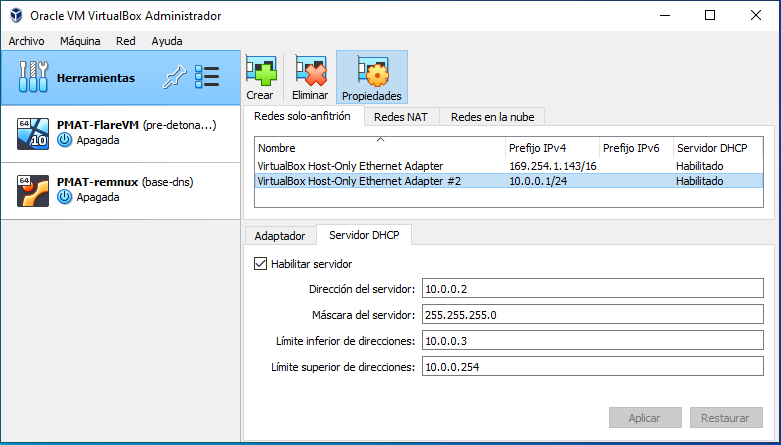
Luego en la pestaña de “**Servidor DHCP**” configuramos los siguientes parámetros:

Dirección del servidor: 10.0.0.2

Mascara del servidor: 255.255.255.0

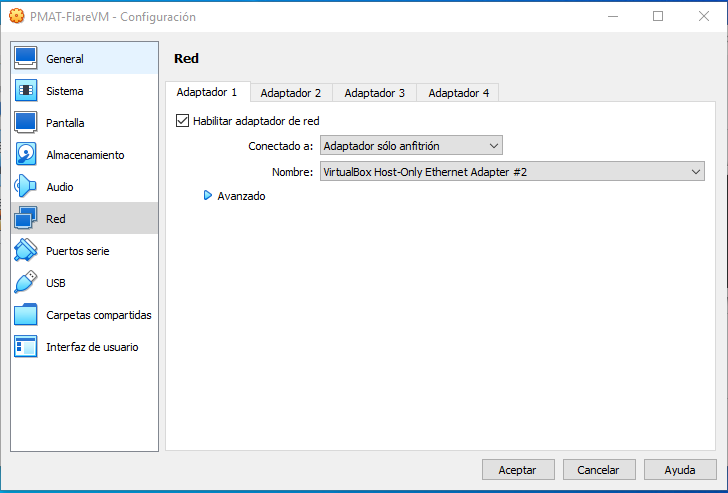
Límite inferior de direcciones: 10.0.0.3

Límite superior de direcciones: 10.0.0.254



**Fuente:** Elaboración propia

Luego seleccionamos la máquina Flare VM -> seleccionamos configuración -> Red -> Cambiamos el adaptador de red de conectado a “**NAT**” a conectado a “**Adaptador solo anfitrión**”. Si dejamos el adaptador en NAT (Network Address Translation), la máquina virtual puede enrutar tráfico hasta el host físico, o hacia internet a través del adaptador físico. Además, seleccionamos el adaptador de red que creamos “**Ethernet Adapter #2**”, el cual está configurado con la dirección IP “**10.0.0.1/24**”.



**Fuente:** Elaboración propia

Luego debemos confirmar que “**Adaptador 1”** este habilitado y que “**Adaptador 2”**, “**Adaptador 3”,** “**Adaptador 4”** estén deshabilitados.

Repetimos estos mismos pasos para la máquina REMnux.

Culminado este paso debemos elegir la muestra de malware que analizaremos, ya sea que obtenida de un equipo en particular, de una red o dispositivo de una organización o empresa. También se pueden obtener muestras de repositorios en internet gratuitos done podemos obtener copias de malware real. Un repositorio donde se puede acceder a otras copias de malware actual, las cuales son publicadas con fines educativos es TheZoo, que también es conocido como Malware DB. Esta base de datos nos permite acceder a muestras reales, algo que en ocasiones suele ser bastante complicado. Otro repositorio donde se pueden encontrar muestras reales es

TheZOO: <https://github.com/ytisf/theZoo>

MalwareBazaar: <https://bazaar.abuse.ch/>

Luego de obtenida la muestra de malware, debemos ingresarla al equipo de Flare VM a través de una memoria USB, recordar que la muestra debe estar comprimida, y con contraseña. Normalmente la contraseña utilizada es “infected”, descomprimimos la muestra de malware, y se procede a comenzar con el análisis.

Antes de continuar mencionaremos los roles involucrados en este piloto experimental.

Un Centro de operaciones de seguridad (SOC, por sus siglas en inglés), a veces denominado Centro de operaciones de seguridad de la información (ISOC), es un equipo interno o subcontratado de profesionales de seguridad de TI que supervisa toda la infraestructura de TI de una organización, 24/7 (las 24 horas, 7 días a la semana), para detectar incidentes de ciberseguridad en tiempo real y abordarlos de la forma más rápida y eficaz posible.

Un SOC también selecciona, opera y realiza el mantenimiento de las tecnologías de ciberseguridad de la organización y analiza continuamente los datos de amenazas para encontrar formas de mejorar la situación de seguridad de la organización.

El principal beneficio de tener o de subcontratar un SOC es que unifica y coordina las herramientas y las prácticas de seguridad y las respuestas a los incidentes de seguridad de una organización. Esto generalmente resulta en una mejora de las medidas preventivas y de las políticas de seguridad, una detección más rápida de amenazas y una respuesta más rápida, más efectiva y más rentable a las amenazas de seguridad. Un SOC también puede mejorar la confianza de los clientes, así como simplificar y reforzar el cumplimiento de la normativa de privacidad por parte de la organización a nivel sectorial, nacional y global (IBM, s.f.).

Estar al día. El SOC debe dominar las últimas soluciones y tecnologías de seguridad, y la última información sobre amenazas (noticias e información sobre ciberataques y sobre los piratas informáticos que los perpetran) recopilándola de las redes sociales, de fuentes del sector y de la web oscura.

Analistas de seguridad, también llamados investigadores de seguridad o personal de respuesta ante incidentes, que son esencialmente los primeros en responder a las amenazas o incidentes de ciberseguridad. Los analistas detectan, investigan y clasifican (priorizan) las amenazas; después identifican los hosts, los puntos finales y los usuarios que se han visto afectados y toman las acciones apropiadas para mitigar y contener el impacto de la amenaza o el incidente. (En algunas organizaciones, los investigadores y los miembros del personal de respuesta ante incidentes tienen roles separados, clasificados como analistas de Nivel 1 y Nivel 2 respectivamente).

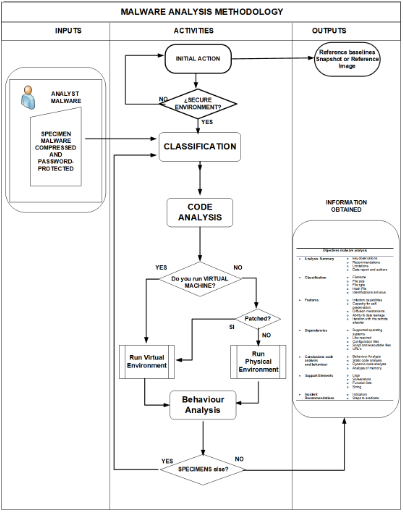
Los cazadores de amenazas (también llamados expertos en seguridad) están especializados en detectar y contener amenazas avanzadas (nuevas amenazas o variantes de amenazas que consiguen pasar las defensas automáticas) (IBM, s.f.).

Equipo de contenido que son los encargados de las siguientes funciones:

* Ajuste de las reglas del o los SIEM, para remediar las alertas de seguridad de falsos positivos.
* Crear casos de uso de seguridad y mapearlos en línea con las fases de MITRE ATTACK y Cyber Kill Chain.
* Creación proactiva de casos de uso de seguridad para la supervisión de la explotación de vulnerabilidades conocidas y colaboración con el equipo interno para su corrección.

Para que este proceso de análisis de malware sea ordenado y alcanzar resultados fidedignos y replicables aplicamos la metodología SAMA (Systematic Approach to Malware Analysis).

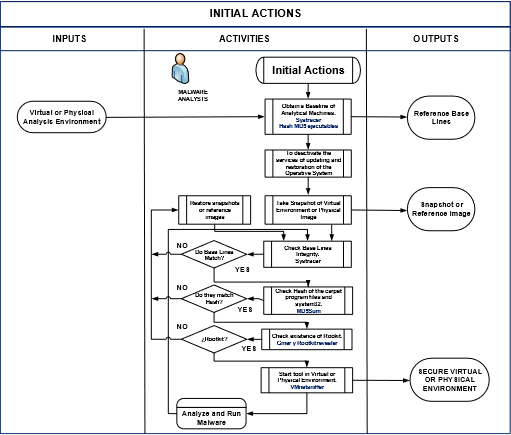
Comenzamos con las acciones iniciales las cuales podemos ver en la siguiente figura:



**Fuente:** Obtenido desde el artículo Systematic Approach to Malware Analysis (Bermejo Higuera y otros, Systematic Approach to Malware Analysis (SAMA), 2020).

Luego procedemos con las acciones iniciales:

Acciones iniciales. Consiste en realizar una serie de acciones principalmente para obtener un registro de la configuración de las máquinas involucradas en el análisis, con el fin de obtener una referencia que nos permita comparar el estado de las mismas antes y después de ejecutar el malware objeto de estudio (Bermejo Higuera y otros, Systematic Approach to Malware Analysis (SAMA), 2020).



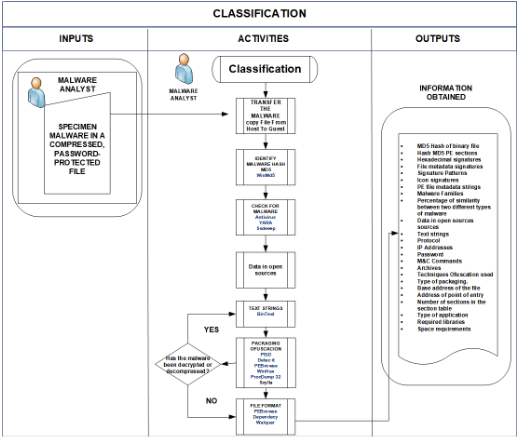
**Fuente:** Obtenido desde el artículo Systematic Approach to Malware Analysis (Bermejo Higuera y otros, Systematic Approach to Malware Analysis (SAMA), 2020).

Las tareas ejecutadas en esta fase son:

* Transferir el malware
* Identificar el malware
* Comprobar la familia del malware
* Encontrar información sobre el malware en código abierto
* Analizar las cadenas del binario del malware
* Analizar técnicas utilizadas en la ofuscación de malware
* Analizar el formato de archivo

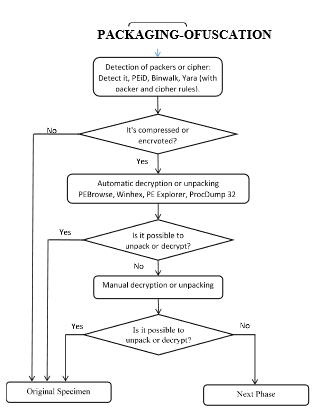
(Bermejo Higuera y otros, Systematic Approach to Malware Analysis (SAMA), 2020).

Luego de finalizada la etapa anterior procedemos con la clasificación:



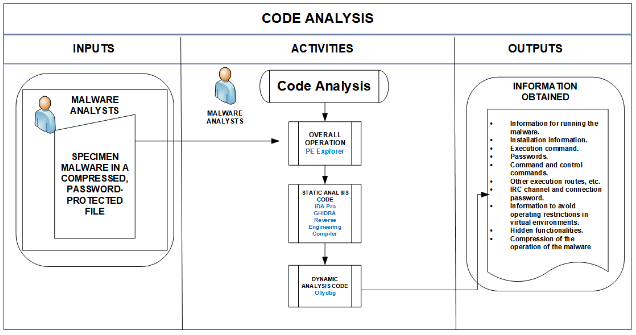
**Fuente:** Obtenido desde el artículo Systematic Approach to Malware Analysis (Bermejo Higuera y otros, Systematic Approach to Malware Analysis (SAMA), 2020).

En caso de que el malware se encuentre ofuscado, seguir los siguientes pasos:



**Fuente:** Obtenido desde el artículo Systematic Approach to Malware Analysis (Bermejo Higuera y otros, Systematic Approach to Malware Analysis (SAMA), 2020)

Pasamos a la fase de análisis de código:

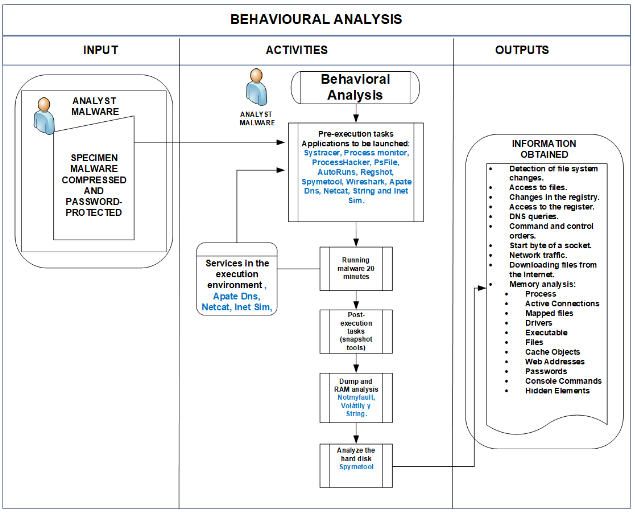


**Fuente:** Obtenido desde el artículo Systematic Approach to Malware Analysis (Bermejo Higuera y otros, Systematic Approach to Malware Analysis (SAMA), 2020).

Los objetivos y la información específica que debe obtenerse en este paso son los siguientes:

* Información para ejecutar el malware.
* Información de instalación.
* Comando de ejecución.
* Contraseñas.
* Comandos de mando y control.
* Otras rutas de ejecución, etc.
* Canal IRC y contraseña de conexión.
* Información para evitar restricciones de funcionamiento en entornos virtuales.
* Funcionalidades ocultas.
* Comprensión del funcionamiento del malware.

Fase de análisis de comportamiento:



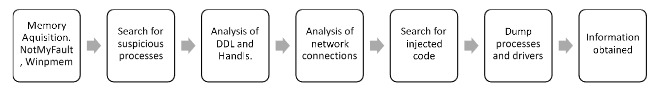
**Fuente:** Obtenido desde el artículo Systematic Approach to Malware Analysis (Bermejo Higuera y otros, Systematic Approach to Malware Analysis (SAMA), 2020).

En esta fase se analiza la implementación de malware en un laboratorio que simula un entorno real, la finalidad es observar el comportamiento del malware, el tráfico de red generado y, por tanto, las acciones que se realizan en el sistema objetivo (modificaciones del registro, archivos, etc.).

Los objetivos y la información específica que se obtendrá en este paso serán:

* Detección de cambios en el sistema de archivos
* Acceso a archivos
* Cambios en el registro
* Consultas DNS
* Órdenes de mando y control
* Byte de inicio de un socket
* Tráfico de red
* Descarga de archivos de Internet
* Análisis de la memoria
* Proceso
* Conexiones activas
* Archivos mapeados
* Controladores
* Ejecutable
* Archivos
* Objetos de caché
* Direcciones web
* Cadenas de texto

A los demás análisis se añade la comprobación de la memoria RAM que puede realizarse con las herramientas volatility o memorize de la siguiente manera:



**Fuente:** Obtenido desde el artículo Systematic Approach to Malware Analysis (Bermejo Higuera y otros, Systematic Approach to Malware Analysis (SAMA), 2020)

La metodología SAMA pretende servir de base para llevar a cabo un proceso sistemático y metodológico de análisis de malware complejo y flexible que puede requerir ligeros cambios o variaciones en cuanto a las tecnologías utilizadas, esto debido al gran número de tipos de malware existentes. Sin embargo, esta situación no cambia la estructura general.