CAPÍTULO V

La ciencia humana consiste más en destruir errores que en descubrir verdades.
Sócrates (470 AC-399 AC)

METODOLOGÍA DE TRABAJO PARA INVESTIGACIÓN

5.1. Metodología de trabajo para investigación en informática forense.

5.2. Fase de identificación.

5.3. Fase de preservación.

5.4. Fase de análisis.

5.5. Fase de documentación y presentación de las pruebas.

5.1. METODOLOGÍA DE TRABAJO PARA INVESTIGACIÓN EN INFORMÁTICA FORENSE

En la actualidad existen muchas metodologías para llevar a cabo un análisis informático forense.

A continuación se presenta un modelo a seguir, elegido por la practicidad y eficiencia que ofrece, dicha metodología se divide en cuatro fases. Estas son:

1. Identificación
2. Preservación
3. Análisis
4. Documentación y presentación de las pruebas

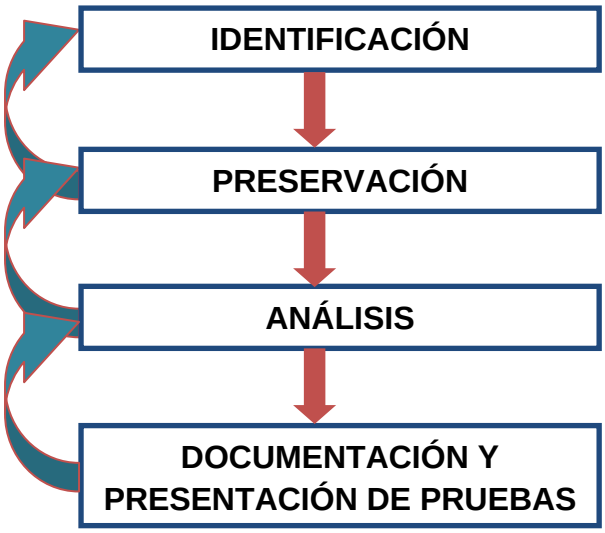

Figura. 5.1. Metodología de trabajo para análisis informático forense

5.2. FASE DE IDENTIFICACIÓN

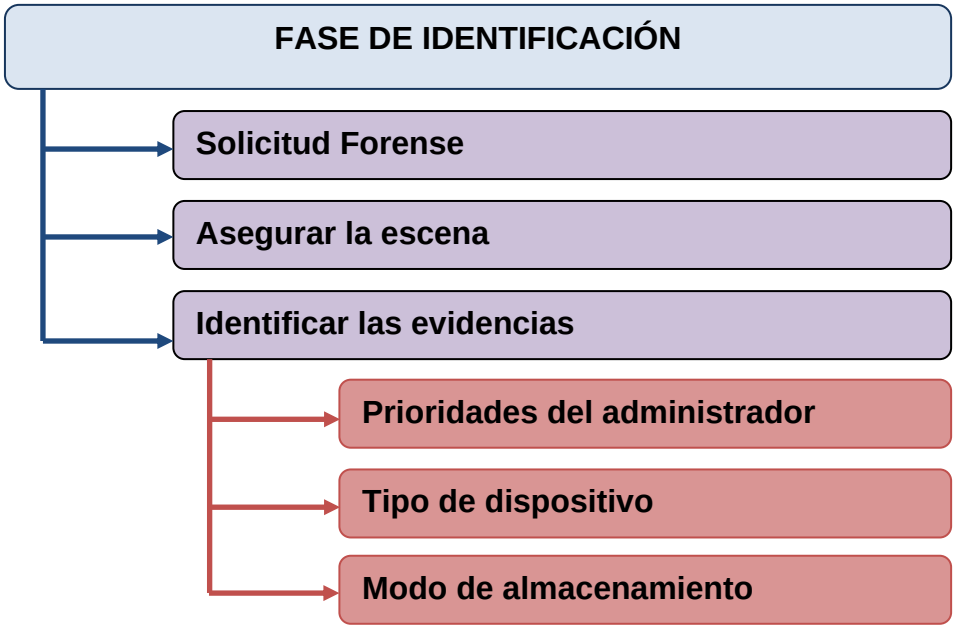

Figura. 5.2. Componentes Fase de Identificación

La fase de identificación se refiere a la recopilación de información necesaria para trabajar sobre la fuente de datos presentada por el administrador de los servidores (solicitud forense). Aquí se pregunta:

- ¿Qué información se necesita?
- ¿Cómo aprovechar la información presentada?
- ¿En qué orden ubico la información?
- ¿Acciones necesarias a seguir para el análisis forense?

El producto final de esta fase, debe entregar un documento detallado con la información que permita definir un punto de inicio para la adquisición de datos y para la elaboración del documento final.

La identificación debe prever los desafíos que se pasarán durante los procesos de las fases de preservación y extracción. Esta fase culmina con un Plan a seguir.

5.2.1. Solicitud Forense

La solicitud forense es un documento donde el administrador del equipo afectado notifica de la ejecución de un incidente y para ello solicita al equipo de seguridad la revisión del mismo, donde incluye toda la información necesaria para dar inicio al proceso de análisis. La información incluida en el documento debe ser la siguiente:

- DESCRIPCIÓN DEL DELITO INFORMÁTICO
  - ✓ Fecha del incidente
  - ✓ Duración del incidente
  - ✓ Detalles del incidente
- INFORMACIÓN GENERAL
  - ✓ Área
  - ✓ Nombre de la dependencia
  - ✓ Responsable del sistema afectado
    - ❖ Nombres y Apellidos
    - ❖ Cargo
    - ❖ E-mail
    - ❖ Teléfono
    - ❖ Extensión
    - ❖ Celular
    - ❖ Fax
- INFORMACIÓN SOBRE EL EQUIPO AFECTADO
  - ✓ Dirección IP
  - ✓ Nombre del equipo
  - ✓ Marca y modelo
  - ✓ Capacidad de la RAM
  - ✓ Capacidad del disco duro
  - ✓ Modelo del procesador
  - ✓ Sistema operativo (nombre y versión)
  - ✓ Función del equipo
  - ✓ Tipo de información procesada por el equipo

Toda la información del incidente, la evidencia digital, copias o imágenes de la escena del crimen.

Reconocer un incidente mediante indicadores y determinar su tipo. Esto no está incluido dentro del análisis forense, pero es significativo en los siguientes pasos.

Esta fase está dividida en dos procesos iniciales que son:

5.2.2. Asegurar la escena

Para asegurar que tanto los procesos como las herramientas a utilizar sean las más idóneas se debe contar con un personal competente a quien se le pueda asignar la conducción del proceso forense, para ello el equipo de seguridad debe estar capacitado y entender a fondo la metodología.

5.2.3. Identificar las evidencias

El siguiente paso y muy importante es la identificación de la evidencia presentada que es la escena del crimen, la misma que estará sujeta a todos los procesos necesarios para la presentación de resultados finales. La evidencia se clasificará según:

5.2.3.1. Prioridades del administrador

Las evidencias se pueden clasificar según la prioridad del administrador, las mismas están basadas en la criticidad de los daños producidos por el incidente, una forma de clasificar los daños producidos es saber que tan críticos son, y se lo encuentra aplicando la siguiente fórmula:

CRITICIDAD DE LOS DAÑOS	**=**	**Extensión de daños producidos**	**+**	**Criticidad de los recursos afectados**

La extensión de los daños producidos es:

- Graves.- Que el incidente produjo daños muy severos sobre los servicios o información.
- Moderados.- Que el incidente causo molestias y pérdida de información.
- Leves.- Que el incidente producido no tiene mayor importancia, no se produjo ningún tipo de pérdida pero si un corte o molestia en los servicios.

La criticidad de los recursos afectados es:

- Alta.- Los recursos afectados son muy importantes dentro de la institución y como tal comprometen el normal funcionamiento y prestación de servicios.
- Media.- Los recursos afectados causan molestias solo a cierta área de la institución.
- Baja.- Los recursos afectados causan ciertas molestias pero se puede seguir con el normal funcionamiento de los equipos.

En este punto se deben enumerar todas las funciones y servicios que el área realiza y deben ser priorizados de acuerdo a la razón de ser de la institución o ente afectado. Para cada prioridad se debe señalar cuál es el tiempo máximo de espera para ser reanudados, adicionalmente, identificar los registros de datos e información vital para la operación de las funciones y servicios.

Un claro ejemplo de cómo obtener el valor critico de los daños producidos es utilizando las siguientes tablas:

Efectos del incidente y Recursos afectados						
Incidente	Daños producidos			Criticidad de los recursos afectados		
	Graves	Moderados	Leves	Alta	Media	Baja
Acceso no autorizado						
Servidor Web	**X**			**X**		
Servidor de archivos		**X**			**X**	
Servidor de aplicaciones	**X**			**X**		
Infección de virus						
Servidor			**X**		**X**	
Estación de trabajo	**X**					**x**
Etc.						

Tabla. 5.1. Efectos del incidente y recursos afectados

Estado de los recursos				
		Criticidad de los recursos afectados		
		Alta	**Media**	**Baja**
Daños producidos	**Graves**	Muy Grave	Grave	Moderado
	Moderados	Grave	Moderado	Leve
	Leves	Moderado	Leve	Leve

Tabla. 5.2. Estado de los recursos

Prioridad del administrador	
Estado	**Prioridad**
MUY GRAVE	10
GRAVE	7
MODERADO	4
LEVE	1

Tabla. 5.3 Prioridad del administrador

5.2.3.2. Tipo de dispositivo

A las evidencias también se las puede clasificar según el tipo de dispositivo donde se las encuentre como:

- Sistemas informáticos
- Redes
- Redes Inalámbricas
- Dispositivos móviles
- Sistemas embebidos[1]
- Otros dispositivos

5.2.3.3. Modo de almacenamiento

A las evidencias también se las clasifica según el medio de almacenamiento. Como pueden ser:

- Volátiles.- Aquellas que se perderán al apagar el equipo como la hora del sistema y desfase de horario, contenido de la memoria, procesos en ejecución, programas en ejecución, usuarios conectados, configuración de red, conexiones activas, puertos abiertos, etc.

- No volátiles.- medios físicos de almacenamiento como memorias flash, CD, discos duros.

Entonces el primer proceso del análisis forense comprende la identificación, búsqueda y recopilación de evidencias. Se debe identificar qué cosas pueden ser evidencias, dónde y cómo está almacenada, qué sistema operativo se está utilizando. A partir de este paso, el equipo de seguridad puede identificar los procesos para la recuperación de evidencias adecuadas, así como las herramientas a utilizar.

[1]La denominación de Sistemas embebidos (embedded) refleja que son una parte integral (interna) del sistema, y en general son dispositivos utilizados para controlar o asistir la operación de diversos equipamientos.

5.3. FASE DE PRESERVACIÓN

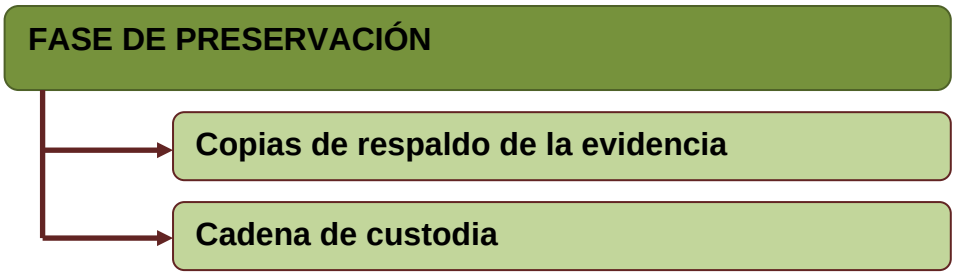

Figura. 5.3. Componentes Fase de Preservación

Aunque el primer motivo de la recopilación de evidencias sea la resolución del incidente, puede ser que posteriormente se necesite iniciar un proceso legal contra los atacantes y en tal caso se deberá documentar de forma clara cómo ha sido preservada la evidencia tras la recopilación.

En esta fase, es imprescindible definir los métodos adecuados para el almacenamiento y etiquetado de las evidencias. Una vez que se cuenta con todas las evidencias del incidente es necesario conservarlas intactas ya que son las “huellas del crimen”, se deben asegurar estas evidencias a toda costa. Para ello se sigue el siguiente proceso.

5.3.1. Copias de la evidencia

Como primer paso se debe realizar dos copias de las evidencias obtenidas, generar también una suma de comprobación de la integridad de cada copia mediante el empleo de funciones hash[2] tales como MD5 o SHA1. Incluir estas firmas en la etiqueta de cada copia de la evidencia sobre el propio medio de almacenamiento como CD o DVD etiquetando la fecha y hora de creación de la copia, nombrar cada copia, por ejemplo “COPIA A”, “COPIA B” para distinguirlas claramente del original.

[2]En informática, Hash se refiere a una función o método para generar claves o llaves que representen de manera casi unívoca a un documento, registro, archivo, etc.

Si además se extrae los discos duros del sistema para utilizarlos como evidencia, se debe seguir el mismo procedimiento, colocando sobre ellos la etiqueta “EVIDENCIA ORIGINAL”, incluir además las correspondientes sumas hash, fecha y hora de la extracción del equipo, datos de la persona que realizó la operación, fecha, hora y lugar donde se almacenó, por ejemplo en una caja fuerte.

Tener en cuenta que existen factores externos como cambios bruscos de temperatura o campos electromagnéticos que pueden alterar la evidencia. Toda precaución es poca, incluso si decide enviar esos discos a que sean analizados por empresas especializadas.

5.3.2. Cadena de custodia

Otro aspecto muy importante es la cadena de custodia, donde se establecen las responsabilidades y controles de cada una de las personas que manipulen la evidencia. Se debe preparar un documento en el que se registren los datos personales de todos los implicados en el proceso de manipulación de las copias, desde que se tomaron hasta su almacenamiento. El documento debe contener la siguiente información:

- Dónde, cuándo y quién examinó la evidencia, incluyendo su nombre, su cargo, un número identificativo, fechas y horas, etc.
- Quién estuvo custodiando la evidencia, durante cuánto tiempo y dónde se almacenó.
- Cuando se cambie la custodia de la evidencia también se deberá documentar cuándo y cómo se produjo la transferencia y quién la transportó.

Todas estas medidas harán que el acceso a la evidencia sea muy restrictivo quedando claramente documentado, posibilitando detectar y pedir responsabilidades ante manipulaciones incorrectas, intentos de acceso no autorizados o que algún otro dispositivo electromagnético se use dentro de un determinado radio.

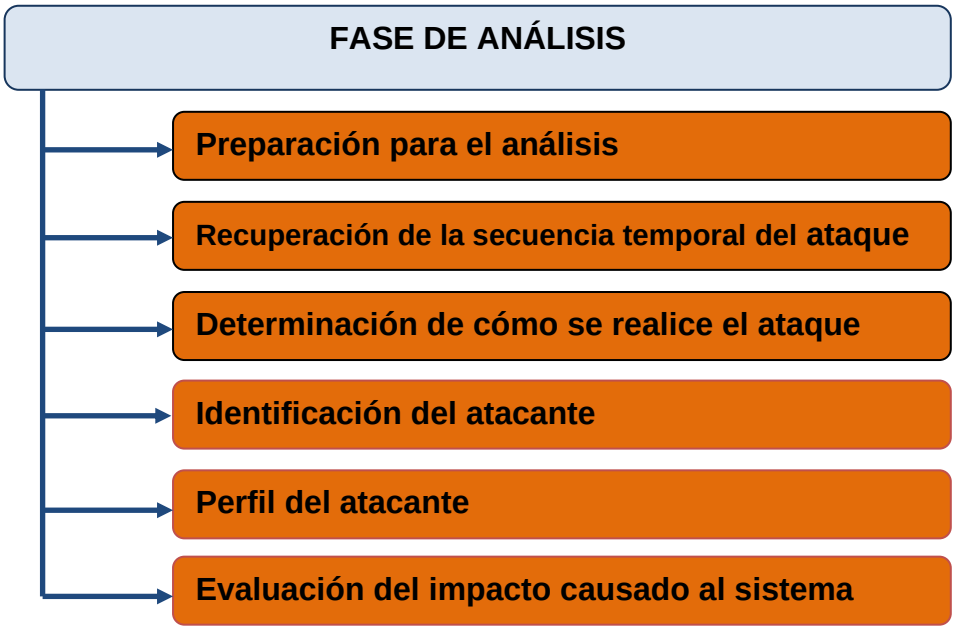

Figura. 5.4. Componentes Fase de Análisis

5.4. FASE DE ANÁLISIS

Antes de iniciar esta fase se deben preparar las herramientas, técnicas, autorizaciones de monitoreo y soporte administrativo para iniciar el análisis forense sobre las evidencias obtenidas o presentadas por el administrador de los servidores. Una vez que se dispone de las evidencias digitales recopiladas y almacenadas de forma adecuada, se inicia la fase más laboriosa, el Análisis Forense propiamente dicho, cuyo objetivo es reconstruir con todos los datos disponibles la línea temporal del ataque, determinando la cadena de acontecimientos que tuvieron lugar desde el inicio del ataque, hasta el momento de su descubrimiento.

Este análisis se dará por concluido cuando se descubra cómo se produjo el ataque, quién o quienes lo llevaron a cabo, bajo qué circunstancias se produjo, cuál era el objetivo del ataque, qué daños causaron, etc. En el proceso de análisis se emplean las herramientas propias del sistema operativo (anfitrión) y las que se prepararon en la fase de extracción y preparación.

5.4.1. Preparación para el análisis

Antes de comenzar el análisis de las evidencias se deberá:

1. Acondicionar un entorno de trabajo adecuado al estudio que se desea realizar.
2. Trabajar con las imágenes que se recopiló como evidencias, o mejor aún con una copia de éstas, tener en cuenta que es necesario montar las imágenes tal cual estaban en el sistema comprometido.
3. Si se dispone de recursos suficientes preparar dos estaciones de trabajo, una de ellas contendrá al menos dos discos duros.
4. Instalar un sistema operativo que actuará de anfitrión y que servirá para realizar el estudio de las evidencias. En esta misma estación de trabajo y sobre un segundo disco duro, instalar las imágenes manteniendo la estructura de particiones y del sistema de archivos En otro equipo instalar un sistema operativo configurado exactamente igual que el equipo atacado, además mantener nuevamente la misma estructura de particiones y archivos en sus discos duros. La idea es utilizar este segundo equipo como “conejillo de Indias” y realizar sobre él pruebas y verificaciones conforme vayan surgiendo hipótesis sobre el ataque.

Si no se dispone de estos recursos, se puede utilizar software como VMware, que permitirá crear una plataforma de trabajo con varias máquinas virtuales[3]. También se puede utilizar una versión LIVE[4] de sistemas operativos como Linux, que permitirá interactuar con las imágenes montadas pero sin modificarlas. Si se está muy seguro de las posibilidades y de lo que va a hacer, se puede conectar los discos duros originales del sistema atacado a una estación de trabajo independiente para intentar hacer un análisis en caliente del sistema, se deberá tomar la

[3]VMware es un sistema de virtualización por software. Un sistema virtual por software es un programa que simula un sistema físico con unas características de hardware determinadas.
[4]Live Distro es un sistema operativo almacenado en un medio extraíble, tradicionalmente un CD o un DVD, que puede ejecutarse desde éste sin necesidad de instalarlo en el disco duro de una computadora.

precaución de montar los dispositivos en modo sólo lectura, esto se puede hacer con sistemas anfitriones UNIX/Linux, pero no con entornos Windows.

5.4.2. Reconstrucción de la secuencia temporal del ataque

Si ya se tienen montadas las imágenes del sistema atacado en una estación de trabajo independiente y con un sistema operativo anfitrión de confianza, se procede con la ejecución de los siguientes pasos:

1. Crear una línea temporal o timeline de sucesos, para ello se debe recopilar la siguiente información sobre los archivos:

   - ✓ Marcas de tiempo MACD (fecha y hora de modificación, acceso, creación y borrado[5]).
   - ✓ Ruta completa.
   - ✓ Tamaño en bytes y tipo de archivo.
   - ✓ Usuarios y grupos a quien pertenece.
   - ✓ Permisos de acceso.
   - ✓ Si fue borrado o no.

   Sin duda esta será la información que más tiempo llevará recopilar, pero será el punto de partida para el análisis, podría plantearse aquí el dedicar un poco de tiempo a preparar un script que automatizase el proceso de creación del timeline, empleando los comandos que proporciona el sistema operativo y las herramientas utilizadas.

2. Ordenar los archivos por sus fechas MAC, esta primera comprobación, aunque simple, es muy interesante pues la mayoría de los archivos tendrán la fecha de instalación del sistema operativo, por lo que un sistema que se instaló hace meses y que fue comprometido recientemente presentará en los archivos

[5] Timestamps, **M**odification date and time, **A**ccess, **C**reation, **D**eleted

nuevos, fechas MAC muy distintas a las de los archivos más antiguos.

La idea es buscar archivos y directorios que han sido creados, modificados o borrados recientemente, o instalaciones de programas posteriores a la del sistema operativo y que además se encuentren en rutas poco comunes. Hay que pensar que la mayoría de los atacantes y sus herramientas crearán directorios y descargarán sus "aplicaciones" en lugares donde no se acostumbra buscar, como por ejemplo en los directorios temporales.

Primero hay que centrarse en buscar los archivos de sistema modificados tras la instalación del sistema operativo, averiguar después la ubicación de los archivos ocultos, de qué tipo son, identificar también los archivos borrados o fragmentos de éstos, pues pueden ser restos de logs y registros borrados por los atacantes. Aquí cabe destacar la importancia de realizar imágenes de los discos, pues se puede acceder al espacio residual que hay detrás de cada archivo, (recordar que los archivos se almacenan por bloques cuyo tamaño de clúster depende del tipo de sistema de archivos[6] que se emplee), y leer en zonas que el sistema operativo no ve. Pensar que está buscando "una aguja en un pajar", por lo que se deberá ser metódico, ir de lo general a lo particular, por ejemplo partir de los archivos borrados, intentar recuperar su contenido, anotar su fecha de borrado y compararla con la actividad del resto de los archivos, puede que en esos momentos se estuviesen dando los primeros pasos del ataque.

3. Comenzar a examinar con más detalle los archivos logs y registros que se examinaron durante la búsqueda de indicios del ataque, intentar buscar una similitud temporal entre eventos. Pensar que

[6]Es un método para el almacenamiento y organización de archivos de computadora y los datos que estos contienen, para hacer más fácil la tarea encontrarlos y accederlos

los archivos log y de registro son generados de forma automática por el propio sistema operativo o por aplicaciones específicas, conteniendo datos sobre accesos al equipo, errores de inicialización, creación o modificación de usuarios, estado del sistema, etc. Por lo que se tendrá que buscar entradas extrañas y compararlas con la actividad de los archivos. Editar también el archivo de contraseñas y buscar la creación de usuarios y cuentas extrañas sobre la hora que se considere como inicio del ataque en el sistema.

4. Examinar los fragmentos del archivo /var/log/messages (UNIX), que es donde se detectan y registran los accesos FTP, esto nos permitirá descubrir si sobre esa fecha y hora se crearon varios archivos bajo el directorio /var/ftp de la máquina comprometida[7], además se debe tener presente que este directorio puede ser borrado por el atacante y deberá ser recuperado.

5.4.3. Determinación de cómo se realizó el ataque

Una vez obtenida la cadena de acontecimientos que se han producido, se deberá determinar cuál fue la vía de entrada al sistema, averiguando qué vulnerabilidad o fallo de administración causó el agujero de seguridad y que herramientas utilizó el atacante para aprovecharse de tal brecha.

Estos datos, al igual que en el caso anterior, se deberán obtener de forma metódica, empleando una combinación de consultas a archivos de logs, registros, claves, cuentas de usuarios, etc. El siguiente proceso permitirá conocer que acciones realizó el atacante:

1. Revisar los servicios y procesos abiertos que se recopilaron como evidencia volátil, así como los puertos TCP/UDP[8] (IANA) y conexiones que estaban abiertas cuando el sistema estaba aún

[7] directorio raíz del servicio ftp en sistemas UNIX/Linux
[8] Protocolos de transporte de datos, TCP (orientado a conexión), UDP (protocolo no orientado a conexión), los 2 pertenecen a la capa de transporte del modelo TCP/IP.

funcionando. Examinar con más detalle aquellas circunstancias que resultan sospechosas cuando se buscó indicios sobre el ataque, y realizar una búsqueda de vulnerabilidades a través de Internet, emplear Google o utilizar páginas específicas donde se encuentran perfectamente documentadas ciertas vulnerabilidades.

2. Si ya se tiene claro cuál fue la vulnerabilidad que dejó el sistema desprotegido, es necesario ir un paso más allá y buscar en Internet algún exploit[9] anterior a la fecha del incidente, que utilice esa vulnerabilidad. Generalmente se encontrará en forma de rootkit[10] y un buen lugar donde comenzar la búsqueda es, nuevamente, Google aunque también será de ayuda utilizar la información presentada en la corrección de vulnerabilidades sobre reportes de este tipo, así como la siguiente dirección: http://packetstorm.rlz.cl.
3. Reforzar cada una de las hipótesis empleando una formulación causa-efecto, también es el momento de arrancar y comenzar a utilizar la máquina preparada como “conejillo de Indias”. Probar sobre la máquina los exploits que se encontró, recordar que en el análisis forense un antecedente es que los hechos han de ser reproducibles y sus resultados verificables, por lo tanto comprobar si la ejecución de este exploit sobre una máquina igual que la afectada, genere los mismos eventos que ha encontrado entre sus evidencias.

Una forma de ganar experiencia y estar listos ante cualquier eventualidad es recurrir a las bases de datos sobre ataques de los honeypots[11], herramientas de seguridad informática, cuya intención es atraer a crackers o spammers, simulando ser sistemas vulnerables o

[9]Es una pieza de software, un fragmento de datos, o una secuencia de comandos con el fin de automatizar el aprovechamiento de un error, fallo o vulnerabilidad, a fin de causar un comportamiento no deseado o imprevisto en los programas informáticos, hardware, o componente electrónico.
[10] Estas herramientas sirven para esconder los procesos y archivos que permiten al intruso mantener el acceso al sistema, a menudo con fines maliciosos.
[11]Software o conjunto de computadores cuya intención es atraer a crackers o spammers, simulando ser sistemas vulnerables o débiles a los ataques.

débiles a los ataques, esto permite recoger información sobre los atacantes y las técnicas empleadas.

5.4.4. Identificación del atacante

Si ya se logró averiguar cómo entraron en el sistema, es hora de saber quién o quiénes lo hicieron. Para este propósito será de utilidad consultar nuevamente algunas evidencias volátiles que se recopiló en las primeras fases, revisar las conexiones que estaban abiertas, en qué puertos y qué direcciones IP las solicitaron, además buscar entre las entradas a los logs de conexiones. También se puede indagar entre los archivos borrados que se recuperó por si el atacante eliminó alguna huella que quedaba en ellos.

Si se tiene pensado llevar a cabo acciones legales o investigaciones internas, se debe realizar este proceso caso contrario se debe saltar y empezar con la recuperación completa del sistema atacado y mejorar su seguridad. Pero si se decide perseguir a los atacantes, se deberá realizar algunas investigaciones como parte del proceso de identificación.

Primero intentar averiguar la dirección IP del atacante, para ello revisar con detenimiento los registros de conexiones de red y los procesos y servicios que se encontraban a la escucha. También se podría encontrar esta información en fragmentos de las evidencias volátiles, la memoria virtual o archivos temporales y borrados, como restos de correo electrónico, conexiones fallidas, etc.

1. Al tener una IP sospechosa, comprobarla en el registro RIPE NCC (www.ripe.net)[12]o en LACNIC (http://www.lacnic.net)[13]a quién pertenece. Pero por ningún motivo hay que apresurarse y sacar conclusiones prematuras, muchos atacantes falsifican la dirección

[12]El Centro de Coordinación de redes IP europeas (Réseaux IP Européens Network Coordination Centre (RIPE NCC)) es el Registro Regional de Internet (RIR) para Europa, Oriente Medio y partes de Asia Central.
[13]Registro Regional de Internet para América Anglosajona, varias islas de los océanos Pacífico y Atlántico.

IP con técnicas de spoofing[14]. Otra técnica de ataque habitual consiste en utilizar "equipos zombis", éstos son comprometidos en primera instancia por el atacante y posteriormente son utilizados para realizar el ataque final sin que sus propietarios sepan que están siendo cómplices de tal hecho. Por ello, para identificar al atacante se tendrá que verificar y validar la dirección IP obtenida.

2. Utilizar técnicas hacker pero solo de forma ética, para identificar al atacante, por si el atacante dejó en el equipo afectado una puerta trasera o un troyano, está claro que en el equipo del atacante deberán estar a la escucha esos programas y en los puertos correspondientes, bien esperando noticias o buscando nuevas víctimas. Aquí entra en juego nuevamente el equipo "conejillo de indias".
3. Si se procede de esta forma, se puede usar una de las herramientas como nmap[15], para determinar qué equipos se encuentran disponibles en una red, qué servicios (nombre y versión de la aplicación) ofrecen, qué sistemas operativos (y sus versiones) ejecutan, qué tipo de filtros de paquetes o cortafuegos se están utilizando y muchas más características que poseen los equipos.

5.4.5. Perfil del atacante

Otro aspecto muy importante es el perfil de los atacantes, y sin entrar en muchos detalles se podrá encontrar los siguientes tipos:

- ✓ ***Hackers:*** Son los más populares y se trata de personas con conocimientos en técnicas de programación, redes, Internet y sistemas operativos. Sus ataques tienen motivaciones de tipo ideológico (pacifistas, ecologistas, anti globalización, anti Microsoft, etc.) o simplemente lo consideran como un desafío intelectual.

[14]Spoofing, en términos de seguridad de redes hace referencia al uso de técnicas de suplantación de identidad.
[15]Mapeador de redes de código abierto, sirve para exploración de redes y auditoría de seguridad.

- ✓ ***ScriptKiddies:*** Son delincuentes informáticos muy jóvenes, que con unos conocimientos aceptables en Internet y programación emplean herramientas ya fabricadas por otros para realizar ataques y ver qué pasa. Su nombre viene de su corta edad y del uso de los scripts, guías de ataques que encuentran por Internet.

- ✓ ***Profesionales:*** Son personas con muchísimos conocimientos en lenguajes de programación, en redes y su equipamiento (routers, firewall, etc.), Internet y sistemas operativos tipo UNIX. Este tipo de criminales realizan los ataques bajo encargo, por lo que su forma de trabajar implica una exhaustiva preparación del mismo, realizando un estudio minucioso de todo el proceso que llevará a cabo, recopilando toda la información posible sobre sus objetivos, se posicionará estratégicamente cerca de ellos, realizará unas pruebas con ataques en los que no modificará nada ni dejará huellas cuando lo tenga todo bien definido entonces atacará, este tipo de atacantes se encuentra muy poco y además se dedica a dar grandes golpes.

5.4.6. Evaluación del impacto causado al sistema

Para poder evaluar el impacto causado al sistema, el análisis forense ofrece la posibilidad de investigar qué es lo que han hecho los atacantes una vez que accedieron al sistema. Esto permitirá evaluar el compromiso de los equipos y realizar una estimación del impacto causado.

Generalmente se pueden dar dos tipos de ataques:

- ▪ ***Ataques pasivos.-*** En los que no se altera la información ni la operación normal de los sistemas, limitándose el atacante a fisgonear por ellos.

- ▪ ***Ataques activos***.- En los que se altera y en ocasiones seriamente, tanto la información como la capacidad de operación del sistema.

Se deberá tener en cuenta, además otros aspectos del ataque como los efectos negativos de tipo técnico que ha causado el incidente, tanto inmediatos como potenciales además de lo crítico que eran los sistemas atacados. Por ejemplo ataques a los cortafuegos, el router de conexión a Internet o Intranet, el servidor Web, los servidores de bases de datos, tendrán diferente repercusión según el tipo de servicio que presta la empresa o institución y las relaciones de dependencia entre los usuarios.

5.5. FASE DE DOCUMENTACIÓN Y PRESENTACIÓN DE LAS PRUEBAS

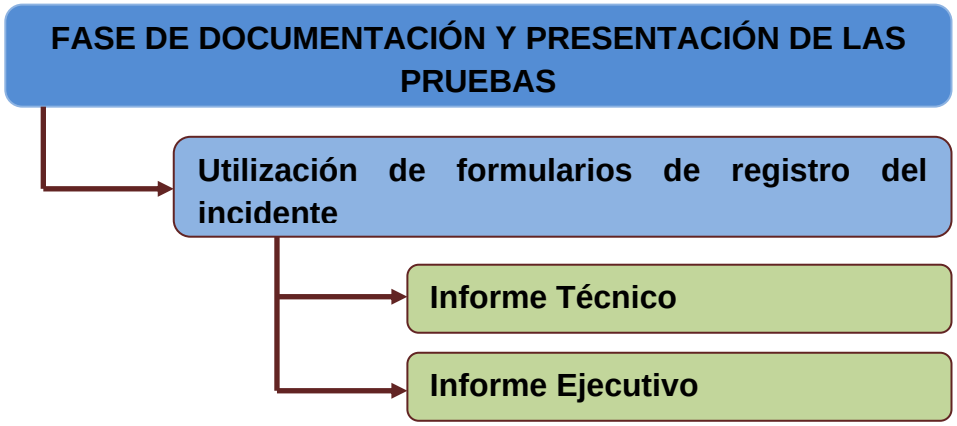

Figura. 5.5. Componentes Fase de Documentación y Presentación de las Pruebas

Es muy importante comenzar a tomar notas sobre todas las actividades que se lleven a cabo. Cada paso dado debe ser documentado y fechado desde que se descubre el incidente hasta que finaliza el proceso de análisis forense, esto permitirá ser más eficiente y efectivo al tiempo que se reducirá las posibilidades de error a la hora de gestionar el incidente.

5.5.1. Utilización de formularios de registro del incidente

Es importante que durante el proceso de análisis se mantenga informados a los administradores de los equipos y que tras la resolución del incidente se presenten los informes Técnico y Ejecutivo. El empleo de

formularios puede ayudar bastante en este propósito. Éstos deberán ser completados por los departamentos afectados o por el administrador de los equipos. Alguno de los formularios que se deben preparar son:

- Documento de custodia de la evidencia
- Formulario de identificación de los equipos y componentes
- Formulario de incidencias tipificadas
- Formulario de publicación del incidente
- Formulario de recogida de evidencias
- Formulario de discos duros.

5.5.1.1. Informe Técnico

Este informe consiste en una explicación detallada del análisis efectuado. Deberá describir en profundidad la metodología, técnicas y hallazgos del equipo forense. A modo de orientación, deberá contener, al menos, los siguientes puntos:

- ✓ Introducción
- ✓ Antecedentes del incidente
- ✓ Recolección de los datos
  - ❖ Descripción de la evidencia
- ✓ Entorno del análisis
- ✓ Descripción de las herramientas
- ✓ Análisis de la evidencia
  - ❖ Información del sistema analizado
    - ➢ Características del SO
    - ➢ Aplicaciones
    - ➢ Servicios
    - ➢ Vulnerabilidades
    - ➢ Metodología
- ✓ Descripción de los hallazgos
  - ❖ Huellas de la intrusión

- ❖ Herramientas usadas por el atacante
- ❖ Alcance de la intrusión
- ❖ El origen del ataque

✓ Cronología de la intrusión
✓ Conclusiones
✓ Recomendaciones específicas
✓ Referencias
✓ Anexos

5.5.1.2. Informe Ejecutivo

Este informe consiste en un resumen del análisis efectuado pero empleando una explicación no técnica, con lenguaje común, en el que se expondrá los hechos más destacables de lo ocurrido en el sistema analizado. Constará de pocas páginas, entre tres y cinco, y será de especial interés para exponer lo sucedido al personal no especializado en sistemas informáticos, como pueda ser el departamento de Recursos Humanos, Administración e incluso algunos directivos. En este informe debe constar lo siguiente:

✓ ***Introducción***.- Descripción del objetivo del análisis del sistema previamente atacado y comprometido, también se incluye la información de la evidencia proporcionada.

✓ ***Análisis.-*** Descripción del entorno de trabajo y de las herramientas de análisis forense seleccionadas así como la cantidad de tiempo empleado en el mismo.

✓ ***Sumario del incidente.-*** Resumen del incidente tras el análisis de la evidencia aportada.

✓ ***Principales Conclusiones del análisis.-*** Detalle de las conclusiones a las que se llegó una vez terminado el proceso de análisis.

- ✓ ***Solución al incidente.-*** Descripción de la solución para recuperación del incidente.

- ✓ ***Recomendaciones finales.-*** pasos que se deben realizar para garantizar la seguridad de los equipos y que el incidente no vuelva a suceder.

5.6. BIBLIOGRAFÍA

Internet

[1] IANA. (s.f.). *Internet Assigned Numbers Authority*. Recuperado el 4 de Abril de 2010, de http://www.iana.org/assignments/port-numbers

[2] Metodologías sobre Análisis Forense. Recuperado el 3 de Abril de 2010, de http://www.kungfoosion.com/2007/07/metodologas-sobre-anlisis-forense.html

[3] Metodología Básica de Análisis Forense. Recuperado el 7 de abril de 2010, de http://www.soyforense.com/2009/09/14/metodologia-basica-de-analisis-forense-%E2%80%93-parte-1-de-4/

[4] Análisis Forense de sistemas. Recuperado el 7 de Abril de 2010, de http://www.scribd.com/doc/3627783/Analisis-Forense-de-Sistema

[5] Análisis Forense Informático. Recuperado el 12 de Abril de 2010, de http://www-2.dc.uba.ar/materias/crip/docs/ardita01.pdf

[6] Cómo la Interpol verificó la información de los equipos de Reyes. Recuperado el 15 de Abril de 2010, de http://www.dragonjar.org/como-la-interpol-verifico-la-informacion-de-los-equipos-de-reyes.xhtml

[7] Reto de Análisis Forense. Recuperado el 20 de Abril de 2010, de http://www.sec-track.com/reto-de-analisis-forense-digital-de-la-comunidad-dragonjar-escenario-e-implementacion

[8] American Academy of Forensic Sciences. Recuperado el 25 de Abril de 2010, de http://www.aafs.org/

Tesis

[9] Guía Metodológica para el Análisis Forense Orientado a Incidentes en Dispositivos Móviles GSM. Recuperado el 17 de Abril de 2010, de http://www.criptored.upm.es/guiateoria/gt_m142h1.htm

[10] V. Villacís, “Auditoria Forense: Metodología, Herramientas y Técnicas Aplicadas en un siniestro informático de una empresa del sector comercial” (Tesis, Instituto de Ciencias Matemáticas, Escuela Superior Politécnica del Litoral, 2006).

[11] Universidad Católica de Loja. Esquema de Seguridad de Datos. Recuperado el 25 de Abril de 2010, de http://www.utpl.edu.ec/eva/descargas/material/140/INFAII21/G218902.pdf

Libros

[12] Miguel López Delgado. Análisis Forense Digital, edición 2ª Junio de 2007. Recuperado el 17 de Abril de 2010, de http://www.oas.org/juridico/spanish/cyb_analisis_foren.pdf

[13] Gutiérrez Abraham, 1998, Métodos y técnicas de investigación, Segunda edición, Mc Graw Hill, México, páginas 12-65.