**Reporte Investigación Forense Empresa Wayne Enterprises**

**-------------------------------------------------------------**

|  |
| --- |
| **Número de Caso: FDYN-123** |
| **Fecha: Septiembre 30 de 2021.** |

**Autor:**

**Ingeniero Informático, Especialista en Investigación Forense.**

**Analista Forense Nivel IV Empresa Certified Offensive and Defensive Security Forensic (CODSF)**

**--- Certified Offensive and Defensive Security Forensic (CODSF) ---**

**“Expertos en Investigación y Computación Forense”**

**Tabla de contenidos.**

***Item***  ***Página***

1. Introducción 1
2. Alcance 2
3. Objetivos y propósito del informe 3

3.1 Objetivos General 3

3.2Objetivos específicos 3

1. Metodología 4

4.1 Estándares 5

1. Descripción de la situación 7
2. Resumen ordenado de las incidencias 8
3. Evidencias y soportes 10
4. Detalle de situaciones 18
5. Hipótesis y reconstrucción de hechos 20
6. Conclusiones 22
7. Recomendaciones 23
8. Diccionario de datos 25
9. Documentos Anexos 28

**1. Notas del Autor y/o aclaratorios del Reporte.**

* La Metodología utilizada, Hallazgos, Evidencias y conclusiones presentadas en el presente informe, el cual es resultante de un proceso de investigación forense realizado a la empresa **Wayne Enterprises**, a razón de una incidencia presentada en los sistemas de información, son orientadas y soportadas en el buen juicio, ética y experiencia profesional del personal de Ingenieros de seguridad especialistas en seguridad informática y computación forense de la empresa **Certified Offensive and Defensive Security Forensic,**, con lo cual se busca identificar, evidenciar y reconstruir las situaciones y hechos que soportan la incidencia presentada en los sistemas informáticos de la empresa Wayne Enterprises, los cuales representan actos ilícitos utilizando las tecnologías de la información en los sistema informáticos de la empresa en mención, por lo que otros evaluadores, auditores y peritos forenses, especializados en investigación digital para situaciones ilícitas presentadas con el uso de las tecnologías de la información, podrían investigar, analizar, y reportar la situación de la incidencia presentada en los sistemas de información de la empresa Wayne Enterprises ,de forma diferente, y llegando a hipótesis, resultados conclusiones y recomendaciones similares, complementarias o diferentes a las planteadas por el equipo de analistas forenses de la empresa **Certified Offensive and Defensive Security Forensic.**
* La presentación del reporte, el cual se soporta en una labor de investigación forense que va desde el entendimiento de la incidencia presentada, el impacto, la recolección de evidencias, hasta el análisis, la reconstrucción de situaciones, hipótesis y presentación de reportes, no implica que los sistemas informáticos sobre los cuales se ha realizado la investigación, queden inmunes ante otro tipo de ataques o situaciones ilícitas similares, que puedan reputarse en todo el espacio de tiempo que dure la investigación forense, soportada en la incidencia inicial.
* Dependiendo del tipo de investigación forense aplicado (Investigación sistemas Online, o Post Mortem), se han podido presentar y registrar nuevas situaciones relacionadas con incidencias y actos ilícitos iniciales.
* **Altamente importante** tener en cuenta que este reporte se soporta en metodologías de recolección y análisis de evidencia , las cuales soportan y dan respuesta a situaciones que se presentaron a razón de actividades ilícitas utilizando las tecnologías de la información, y las cuales se recolectaron de forma ordenada, secuencial, y de **forma LEGAL**, y en ningún momento están en contra o atentan contra los derechos a la intimidad, derechos de autor, leyes relacionadas con delitos informáticos, datos personales, manuales de convivencia, reglamentos o políticas empresariales.

**2. Introducción.**

El presente reporte contiene registrado de forma general y detallada, los resultados del proceso de investigación forense llevado a la práctica entre el 15 de Junio de 2021, y el 22 de Junio de 2021, por parte del personal de Ingenieros expertos en computación forense e investigación digital de la empresa **Certified Offensive and Defensive Security Forensic (CODSF**), en las instalaciones de la empresa **Wayne Enterprise**, localizada en la dirección: **Avenida 44 a- Número 89-34**, Cuidad Gótica, a razón de la incidencia presentada en el sistema de información y redes informáticas de la empresa **Wayne Enterprises**, representada en **fuga y venta ilegal de información** perteneciente a proyectos especiales, y la realización de ataques informáticos y actos ilícitos por medio de la utilización, y en contra del sistema y redes informáticas de la empresa en mención.

El trabajo y por consecuente los resultados de la investigación se soportan en el trabajo de campo realizado en las instalaciones físicas de la red informática y sistema de información de la empresa **Wayne Enterprises**, con el complemento de trabajos en campo y entrevistas con empleados de los proveedores de servicios a Internet que tienen contratos actuales con la empresa Wayne Enterprises, que para el caso son: **OSCORP TELECOM, Y T-AVENGERS comunicaciones.**

**2.1 Objetivos:**

* Identificar y comprender la situación que soporta el proceso de investigación forense.
* Recolectar y analizar todas las evidencias respecto a la incidencia presentada en la red informática de la empresa Cliente **Wayne Enterprise**
* Presentar por medio de un reporte, en el cual se registre todo el trabajo realizado de la investigación forense.
* Respetar la Evidencia, cadena de custodia, siempre preservando la protección de la misma para su preservación en el Tiempo.
* Presentar por medio de un reporte la explicación de forma puntual o por medio de hipótesis, al respecto de lo que ha causado la incidencia o acto ilícito utilizando las tecnologías de la información.

**2.2 Descripción de la situación:**

La situación que da origen al proceso de investigación forense que soporta todo los contenidos, evidencias y anexos del presente reporte, se soporta en la incidencia presentada en la empresa Wayne Enterprises, la cual se describe respecto a:

* Copias ilegales de documentos altamente confidenciales al respecto de proyectos especiales relacionados con diseños y modelos de nuevos prototipos.
* Ventas ilegal y no controlada de documentos altamente confidenciales al respecto de proyectos especiales relacionados con diseños y modelos de nuevos prototipos.
* Infecciones de software ilegal de monitoreo y control remoto de sistemas informáticos
* Ataques indiscriminados internos y externos a los servidores principales de la red informática de la empresa Wayne Enterprise.

**2.3 Metodología, estándares y buenas prácticas:**

Durante toda la ejecución del ciclo de investigación forense y digital, en lo que respecta al caso de las situaciones ilícitas presentadas en la empresa Wayne Enterprise, se utilizó la siguiente metodología y/o fases de ejecución:

* Identificar y/o Evaluar la situación
* Adquisición de la evidencia. (Para esta fase se usó el estándar RFC 3227)
* Aseguramiento y manejo la evidencia
* Análisis de evidencias y datos
* Presentación y justificación de reportes

**4.1 Herramientas utilizadas en la Investigación:**

A continuación, se presenta un listado de las herramientas nivel Hardware y Software utilizadas en la investigación forense de la incidencia presentada en el sistema de información de la empresa **Wayne Enterprise.**

***Nivel Hardware:***

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ***Id Herramienta*** | ***Nombre*** | ***N. serie*** | ***Modelo*** | ***Propiedad*** | ***Instalación*** |
| 1 | TableAU Forensic Duplicator | 2547XCSFFF-58699 | TD2 | Empresa CODSF | Laboratorio Forense CODSF, sesión 1, Lab2 |

***Nivel Software:***

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ***Id Herramienta*** | ***Nombre*** | ***Versión*** | ***Licencia*** | ***Propiedad*** | ***Instalación*** |
| 1 | AccessData FTK Imager | 3.2.0.0 | FDKY-2154-RE23 | Empresa CODSF | - Pcmaligno1  -Pcmaligno2  -PCanalista1 |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ***Id Herramienta*** | ***Nombre*** | ***Versión*** | ***Licencia*** | ***Propiedad*** | ***Instalación*** |
| 2 | X-Ways Forensics | 18.3 | 85DKY-YY2154-8523 | Empresa CODSF | -PCanalista2 |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ***Id Herramienta*** | ***Nombre*** | ***Versión*** | ***Licencia*** | ***Propiedad*** | ***Instalación*** |
| 3 | Volatility Framework | 2.6 | 78985DKY-YY2154-8523 | Empresa CODSF | -PCanalista2  -PCanalista2 |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ***Id Herramienta*** | ***Nombre*** | ***Versión*** | ***Licencia*** | ***Propiedad*** | ***Instalación*** |
| 4 | Autopsy | 4.18.0 | 78985DKY-YY2154-G25T | Empresa CODSF | -PCanalista2  -PCanalista2 |

**5. Evidencias:**

**5.1 Adquisición de Evidencias:**

Las siguientes son las evidencias recolectadas durante el proceso de investigación digital y forense, respecto a las incidencias, acciones ilícitas e ilegales, presentadas en los sistemas de información de la empresa **Wayne Enterprise**.

Listado resumido de evidencias:

|  |  |
| --- | --- |
| **ID Evidencia** | **Nombre:** |
| FDYN-001 | Discos duros físico extraído servidor NIST HACKING CASE (001, 002, 003, 004, 005 y E01) |
| FDYN-002 | Captura Memoria RAM |
| FDYN-003 | Imagen tipo replica Disco físico extraído servidor |

Listado detallado de evidencias:

FDYN-001

NIST HACKING CASE

Para dar Inicio al estudio de los HDD que Nos facilitaron Nuestros Colaboradores y esta fueron las Imágenes que nos suministraron para la Realización del Estudio y Análisis de cada Imagen

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

Para ello Usando el Software Autopsy 4.18.0, usamos la Imagen de cada HDD para su correspondiente análisis

Tabla

Descripción generada automáticamente

FDYN-001 - 001

NIST HACKING CASE

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

Para ello vamos a analizar lo que contiene el Vol2 NTFS, esto nos plantea que la Imagen 001 tiene Metadatos y que el mismo volcado tiene Información para su Análisis la cual vanos a ver a continuación.

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

A Nivel General vemos que contiene Muchos Archivos y viendo por encima podemos deducir u Analizar de que este equipo pertenece a un usuario que posee herramientas de Hacking; una de ellas es CAIN el cual consiste en la encriptación/desencriptación de HASHES

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

Además de una gran cantidad de TROJANOS

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

Además, extrajimos los Documentos del HDD

Interfaz de usuario gráfica, Texto, Correo electrónico

Descripción generada automáticamente

Para hacer un resumen podemos ver en el siguiente Grafico

Texto

Descripción generada automáticamente

Con un 23.4 % de Documentos y un 25.0% de Ejecutables, analizando la Mayoría de los Archivos podemos identificar que son Diccionarios, los cuales sirven para atacar vulnerabilidades como usuarios y password

Interfaz de usuario gráfica, Tabla

Descripción generada automáticamente con confianza media

Y una carpeta de Exploits

Interfaz de usuario gráfica, Tabla

Descripción generada automáticamente

Y Resumida cuenta y analizando miles de Archivos y Documentos, además de ver sus Historial y Búsquedas por Internet podemos Llegar a esta conclusión.

FDYN-001 – 002

NIST HACKING CASE

Podemos ver que el HDD 002 ha sido Eliminado en su gran totalidad, pero este mismos quedo mal eliminado dejando rastros de su S.O. y sus correspondientes elementos

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

Lo que se logró Ver, Identificar y Analizar son dos Softwares (pwddump, Netcat)

Texto

Descripción generada automáticamente

El PWDUMP Software usado para extraer credenciales

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

Como podemos ver en la Imagen Corroboramos que es NETCAT el cual sirve para abrir puertos

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

También en el siguiente Grafico podemos ver que la mayoría son archas Desconocidos

Gráfico, Gráfico circular

Descripción generada automáticamente

También veo que hay demasiados Archivos como Documentos los cuales al Hacer una Búsqueda en el HDD

Tabla

Descripción generada automáticamente

FDYN-001 – 003

NIST HACKING CASE

En este HDD sucede lo Mismo que en el Anterior y eso lo podemos ver en la Imagen

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

Vemos que hay un software vnc

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

También vemos un NMAP

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

Volvemos a ver un complemento de los HDD Anteriores, es un disco que también posee herramientas de Hacking

Gráfico, Gráfico circular

Descripción generada automáticamente

FDYN-001 – 004

NIST HACKING CASE

Hemos encontrado más Software y además unos archivos eliminados dentro del HDD

Gráfico

Descripción generada automáticamente con confianza baja

Luego usamos el Buscador del software Autopsy, para ver que mas encontramos, dentro de ello buscamos lo que hay en el Escritorio

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

Y los Documentos También

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

Y vemos que la Mayoría de Archivos son ilegibles o están añados

Gráfico, Gráfico circular

Descripción generada automáticamente

FDYN-001 – 005

NIST HACKING CASE

Vemos que la Mayoría de Archivos están perdidos debido a que los Discos Anteriores del 002 al 005 están Borrados u Eliminados

Interfaz de usuario gráfica, Aplicación, Tabla, Excel

Descripción generada automáticamente

Y Analizando lo poco del HDD haciendo una Inspección visual podemos identificar que hay muchos archivos .TIF los cuales usamos el Buscador y los Exportamos los Mismos

Tabla, Excel

Descripción generada automáticamente

Corroboramos que se elimino los Documentos y Programas pero no fueron bien eliminadosdevido a que el escritorio podemos ver

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

Gráfico, Gráfico circular

Descripción generada automáticamente

Esta es la Imagen del HDD

FDYN-001 – E01

NIST HACKING CASE

Esta Imagen es Similar a la 001, es decir NO ha sido Eliminado; y mostramos el S.O. del HDD

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

Documentos, ahí podemos observar Diccionarios y Exploits además de Comandos es como una gui para hacer los Ataques

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

También podemos Analizar las Búsquedas de Internet

Interfaz de usuario gráfica, Aplicación, Tabla, Excel

Descripción generada automáticamente

Además vemos los Programas que se usan en ese HDD

Interfaz de usuario gráfica, Aplicación, Tabla

Descripción generada automáticamente

NOTA: Las Maquinas 006 al 008 Están Muy Dañadas y no tiene un elemento servible y son ilegibles; Además podemos Analizar de que estos Discos pertenecen al mismo Dueño, debido a que todos tiene partes u elementos y Herramientas de Hacking incluyendo Diccionarios, Exploits, además de Manuales de funcionamiento de herramientas web.

FDYN-002 – 001

Imagen de la pantalla de un celular con letras

Descripción generada automáticamente con confianza media

**Descripción:** Esta evidencia corresponde al resultado de un proceso de volcado de memoria RAM de uno de los equipos afectados en el incidente presentado en la red informática de la empresa ***Wayne Enterprises***, específicamente en el equipo identificado como:

***Server01. waynenterprises.local***

***Observaciones:*** Esta evidencia es resultado de una adquisición de evidencias de un incidente informáticos presentado en un equipo que esta encendido (Análisis online y/o Directo).

**Anexos y/ soportes:** Archivo en formato Word, donde se describe de forma detallada el proceso de adquisición del volcado de memorias, con datos detallados del archivos generado, así como las herramientas utilizadas para la generación del archivo y el cálculo de integridad.

**Integrida**d: Se toma cálculo de integridad aplicando un proceso de cálculo de HASH, usando los algoritmos MD5 y SHA.

**HASH MD5:** 38d54952e8b655e8bd6a6ae6aff9b9f7

**HASH SHA:**

a1c5a216f0c6b3e1a63e6d227bbc170f4a9167b2bb3ecdd833cce6c2c419966fca0ed44b14797db02329dadb9abf758758eb8fdaf4a72aaecd1425c72182bed1

FDYN-002 – 002

Texto

Descripción generada automáticamente con confianza media

**Descripción:** Esta evidencia corresponde al resultado de un proceso de extracción física del disco duro de uno de los equipos tipo servidor afectados en el incidente presentado en la red informática de la empresa ***Wayne Enterprises***, específicamente en el equipo identificado como:

***Server01. waynenterprises.local***

***Observaciones:*** Esta evidencia es resultado de una adquisición física, correspondiente a una de las partes de un equipo de cómputo del tipo servidor, el cual hace parte de un incidente informático presentado en un equipo que estaba apagado (Análisis Post-Mortem).

La extracción física del disco duro del servidor, se realiza teniendo en cuenta precauciones, tales como: Guantes especiales contra descargas eléctricas, se filmó en un video el proceso de extracción del disco duro del servidor, además el video contiene en sonido la narración del analista, respecto a la extracción del disco duro.

El disco duro se guarda como evidencia en el laboratorio de la empresa CODSE, con previa autorización por escrito la empresa ***Wayne Enterprises***. Se aclara que el disco duro será sometido a un proceso de réplica de disco duro, para dejar intacta la evidencia original, y trabajar sobre la copia.

**Anexos y/ soportes:** Archivo en formato video mp3, donde se describe de forma detallada el proceso de extracción del disco duro, como parte de recolección y adquisición de posible dispositivos que contengan evidencia, al respecto de la incidencia presentada en la red informática de la empresa ***Wayne Enterprises***.

Archivo tipo documento firmado (compulsado) en notaria por parte la empresa **Wayne Enterprises,** donde autoriza la custodia del disco duro descrito en la evidencia ID FDYN-002 a la empresa de investigación forense CODSE.

**Integrida**d: Se toma cálculo de integridad aplicando un proceso de cálculo de HASH, usando los algoritmos MD5 y SHA.

**HASH MD5:** f8b115f35dcf34a989cdda048e3d6ace

**HASH SHA:**

Administrador:500:98f4165244bc658836077a718ccdf409:b7452fd8928e71f44b650c346c7890db:::

Invitado:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::

|  |
| --- |
| **ID Evidencia:** FDYN-003  **Nombre:** Imagen tipo replica Firewall servidor  **Datos: (Disco duro replica)**  Número de serie: 12XXXXX-FFF-YYY-2889  Marca: Maxtor SAS/SATA de 2 TB  Modelo: v33-8498  Fecha copiado (Replica) disco físico: 26/10/2016  Hora: 20:15 Horas |

**Descripción:** Esta evidencia corresponde al resultado de un proceso de copiado total (Tipo replica-Imagen) del disco duro físico que se extrajo del equipo tipo servidor identificado como ***Server01. waynenterprises.local***, a un disco duro nuevo.

***Observaciones:*** Esta evidencia es resultado de una copia total del disco duro físico, correspondiente a una de las partes de un equipo de cómputo del tipo servidor, el cual hace parte de un incidente informático presentado en un equipo que estaba apagado (Análisis Post-Mortem).

El disco duro utilizado para la réplica, fue descontaminado, y examinado de forma minuciosa por diversos sistemas antivirus.

La copia tipo réplica del disco duro extraído del servidor **server01.waynenterprises.local**, se realizó con Hardware específico para este tipo de labores de copiado, garantizando altamente la integridad física y lógica del disco duro original, mediante labores prioritarias de prevención y protección ante escritura del disco duro original.

**Anexos y/ soportes:** Archivo en formato Word, donde se describe de forma detallada el proceso de copiado tipo réplica del disco duro extraído del servidor server01.waynenterprises.local, a un disco duro nuevo y descontaminado.

**Integrida**d: Se toma cálculo de integridad aplicando un proceso de cálculo de HASH, usando los algoritmos MD5 y SHA. (Tener en cuenta que los valores Hash son iguales para el disco duro original, y el disco duro replica)

**HASH MD5:** f8b115f35dcf34a989cdda048e3d6ace

**HASH SHA:** 3a3d6c1b4a33ba9401225d7dcd49104ddae83c64

**5.2 Análisis de Evidencias:**

Los siguientes son los procedimientos de análisis llevados a la práctica sobre las evidencias recolectadas en los dispositivos y equipos de cómputo durante el proceso de investigación digital y forense, respecto a las incidencias, acciones ilícitas e ilegales, presentadas en los sistemas de información de la empresa **Wayne Enterprises**.

**Evidencia analizada: FDYN-001-- Captura memoria** **RAM**

**Fecha y Hora del Análisis:** 19/05/2015, Hora: 14:20 horas

**Analista:** Robert Bruce Banner Banner

**Procedimiento ejecutado:** Análisis de registros en la memoria RAM, utilizando la herramienta volatility. Para el análisis de los registros del archivo que contiene la memoria RAM, se ejecutó lo siguiente:

* Se dispuso del archivo identificado como: memdumpw7.mem, para copiarlo de forma completa al equipo tipo estación de trabajo del analista Robert Bruce Banner Banner.
* Se calculó de nuevo integridad de HASH sobre el archivo en mención.
* Dentro de la estación de trabajo en mención, la cual está localizada en el laboratorio forense de la empresa CODSE, lab número 2, se tiene instalado el sistema operativo Kali Linux, y la herramienta **voltility**.
* Una vez que se tiene la imagen en el disco duro del analista Robert Bruce Banner Banner, se procede a validar el tipo de archivo que contiene el volcado de memoria, para validar exactamente el sistema operativo del equipo, de donde se ha adquirido el volcado de memoria.
* Luego se ejecuta la herramienta voltility con una opción específica para observar al momento en que se adquirió el volcado de memoria en el equipo analizado (víctima del fraude o ataque), que procesos estaban activos en el sistema.

Análisis:

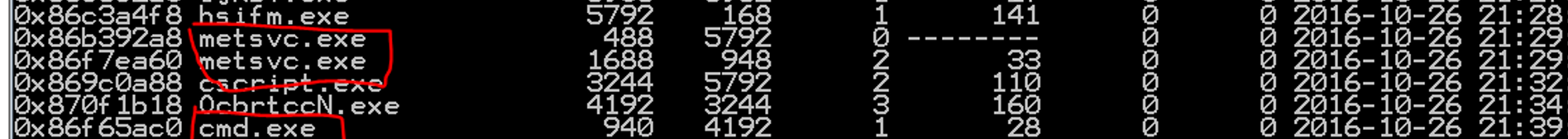
Entre las variables interesantes que suministra la salida de este comando de análisis de memoria con volatility, se encuentran: Identificador del procesos Hilos de conexión, hora en que se inició el procesos, entre otros.

Imagen que contiene Diagrama

Descripción generada automáticamente

En los resultados obtenidos de este comando, se puede observar lo siguiente:

* + Se encuentran procesos cargados en el sistema, típicos de sistemas Windows, tales como: winlogon.exe, lsass.exe, dns.exe, svchost.exe, entre otros, que están asociados a servicios de red del servidor Windows server.
  + Pero también se observar algunos servicios con nombres algo extraños.



* + Importante también observar que los servicios y/o archivos que comúnmente pertenecen a sistemas Windows, tienen una hora promedio 2016-10-26 21:29:51 UTC+0000.
  + Los procesos que difieren a los Normales debido a sus Nombres es el proceso metsvc.exe
  + Llevándole promedio de inicio de unos 16 minutos, respecto a compararlos con otros procesos, como los que s e han mencionado como sospechosos.
  + Los procesos sospechosos también se caracterizan, por no tener muchos hilos de conexión (mínimo 1, máximo 3)
* Luego se ejecuta la herramienta voltility con una opción específica para identificar las conexiones activas de red, las cuales están presentes al momento que se adquirió la muestra de la memoria RAM, mediante el volcado de memoria

Análisis:

Texto

Descripción generada automáticamente

* + La dirección IP del equipo víctima del fraude informático, o que se está analizando es: 192.168.41.159
  + Se evidencia una conexión del equipo victima con la dirección IP 192.168.1.66 por el puerto TCP 443 y el 65000
  + Además se observa que desde la dirección IP 192.168.1.66, hay una conexión al equipo victima por el puerto 65000 TCP
  + Se observa que la dirección IP 192.168.1.66 está conectado al equipo victima por el puerto 443TCP, y por el puerto 5556
* Teniendo presente que cada una de las conexiones tiene un PID, se complementa el análisis, con el proceso de validar que archivos están relacionados con dichas conexiones. Esta información se obtiene mediante la ejecución de la herramienta voltility con una opción específica para identificar - validar que archivos que están relacionados con las conexiones registradas anteriormente.

Análisis:

Texto

Descripción generada automáticamente

* Al ser una conexión activa asociada a un proceso con un nombre extraño, y localizado en la carpeta SYSTEM, se puede clasificar como una actividad, y archivo sospechoso.

Texto

Descripción generada automáticamente

* Analizando la anterior conexión, se puede evidenciar el uso de la herramienta netcat, en modo puerta trasera, dejando abierto el puerto 5556 TCP, con modo y/o opción de entrada para ejecutar la consola de comando en el sistema víctima.

Texto

Descripción generada automáticamente

* Y el proceso cmd , es el resultado de conectarse de parte de un atacante a la victima
* Luego se ejecuta la herramienta voltility con una opción específica para para extraer los archivo(s) relacionados con los procesos sospechoso, que estaban presentes al momento que se adquirió la muestra de la memoria RAM, mediante el volcado de memoria

Análisis:

Texto

Descripción generada automáticamente

* Al momento de cargar el archivo (sospechoso) a la herramienta online virus total, y se analiza, se apreciar que muchos antivirus lo identifican como sospechoso.

Interfaz de usuario gráfica, Aplicación, Teams

Descripción generada automáticamente

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

* Luego se ejecuta la herramienta voltility con una opción específica, donde se pueden observar los identificadores de seguridad, y al final poder deducir si un proceso malicioso ha logrado escalar privilegios, respecto a los registros que estaban presentes al momento en que se adquirió la muestra de la memoria RAM, mediante el volcado de memoria

Análisis:

* Se identifica que el archivo malicioso lsass.exe, ha logrado escalar privilegios en el sistema afectado

Texto

Descripción generada automáticamente

**5.3 Resultados:**

Los siguientes son los resultados de los análisis llevados a la práctica sobre las evidencias recolectadas en los dispositivos y equipos de cómputo durante el proceso de investigación digital y forense, respecto a las incidencias, acciones ilícitas e ilegales, presentadas en los sistemas de información de la empresa **Wayne Enterprises**.

* Según el análisis de la evidencia, se identifica de forma clara que se ha realizado una intrusión no autorizada al servidor identificado como: ***2003Server. waynenterprises.local,*** desde el equipo de la red local, descrito como***: pcmaligno. waynenterprises.local.***
* La conexión (intrusión) no autorizada al servidor ***2003Server, NAS y el Firewall. waynenterprises.local,*** se realiza mediante conexión a puertas traseras persistentes, las cuales fueron creadas con el payload Meterpreter, el cual hace parte del Framework de explotación Metasploit.
* De una forma más concreta, el usuario no autorizado utilizo herramientas automatizadas para la conexión no autorizada a un sistema de información, que para el caso fue al servidor ***Server01. waynenterprises.local.***
* Por medio de las conexiones no autorizadas en mención, las cuales se soportan en puertas traseras (Backdoors) y vulnerabilidades del servidor ***Server01.waynenterprises.local*** , se supone que el usuario no autorizado ha podido controlar el servidor de forma total, y llevarse de este servidor información confidencial, la cual se sospecha se ha vendido a empresas competidoras de Wayne Enterprises.

**6. Conclusiones.**

Las siguientes son las conclusiones del procesos de investigación digital llevada a la práctica respecto a las incidencias, acciones ilícitas e ilegales, realizadas por medio y/o usando los sistemas de información de la empresa **Wayne Enterprises**.

* Las conexiones no autorizadas sobre sistemas informáticos de la empresa **Wayne Enterprises**, se realizaron por personal técnico y equipos de cómputo pertenecientes a la red local.
* La conexión no autorizada sobre sistemas informáticos de la empresa **Wayne Enterprises**, permitieron un control total del servidor ***2003server, waynenterprises.local***, por lo que es evidente la obtención de información sensible contenida en el servidor en mención, parte de usuario atacante.
* La conexión no autorizadas sobre sistemas informáticos de la empresa **Wayne Enterprises**, se lograron con el uso de herramientas informáticas utilizadas para auditorias de seguridad de sistemas informáticos, las cuales pueden obtenerse de forma legal y gratuita en internet.
* Los tiempos de las conexiones sobre el servidor ***Server01.waynenterprises.local***, coinciden con los registros de las grabaciones en video del PC de escritorio descrito como: ***pcmaligno1.waynenterprises.local***, administrado por el usuario **Norman Osborne** al momento de presentarse algunas de las incidencias en la red informática de la empresa **Wayne Enterprises.**

**7. Recomendaciones.**

Las siguientes son las recomendaciones finales del procesos de investigación digital llevado a la práctica respecto a las incidencias, acciones ilícitas e ilegales, realizadas por medio y/o usando los sistemas de información de la empresa **Wayne Enterprises.**

* Llevar esta incidencia, y el respectivo reporte de investigación digital-forense con todas las evidencias y anexos, como una denuncia penal, ante la unidad de delitos informáticos de la Policía Nacional.
* Solicitar logs de conexión a los ISP y demás sistemas de redes sociales, las cuales están relacionadas con los análisis y resultados de evidencias registrados en este informe, ya que dichas evidencias, y su posterior análisis complementario, dependen estrictamente de una orden judicial para la solicitud y extracción de logs de los sistemas de los ISP y sistemas de redes sociales en mención.

**8. Diccionario de datos.**

***Metasploit Framework:*** Es una herramienta para desarrollar y ejecutar exploits contra una máquina remota.

***Payload:*** Un código Payload, es la porción de código en el exploit que tiene como objetivo ejecutar una acción concreta y maliciosa en el sistema víctima.

***Meterpreter***: Meterpreter se define como un Payload avanzado y como una extensión de Metasploit, la cual permite aprovechar al máximo las funcionalidades de Metasploit y aumentar el alcance en lo que respecta a comprometer una maquina víctima.

**9. Anexos y-o Soportes.**

Los siguientes son los documentos anexos, que se mencionan como apoyo a la recolección y/o análisis de las evidencias pertenecientes al proceso de investigación digital llevado a la práctica respecto a las incidencias, acciones ilícitas e ilegales, realizadas por medio y/o usando los sistemas de información de la empresa **Wayne Enterprises.**

* Volcadomemoria.docx
* Video\_extraccion\_HDD\_SERVER.MP3
* Copia\_imagen\_hdd\_server.docx

**Firma:**

**----------------------------------------------------------------**

**ULTRAMAGNU**

**Ingeniero Informático, Especialista en Investigación Forense.**

**Tarjeta profesional numero: 96325-XCCV-28**

**Analista Forense Nivel II**

**Empresa Certified Offensive and Defensive Security Expert (CODSE)**