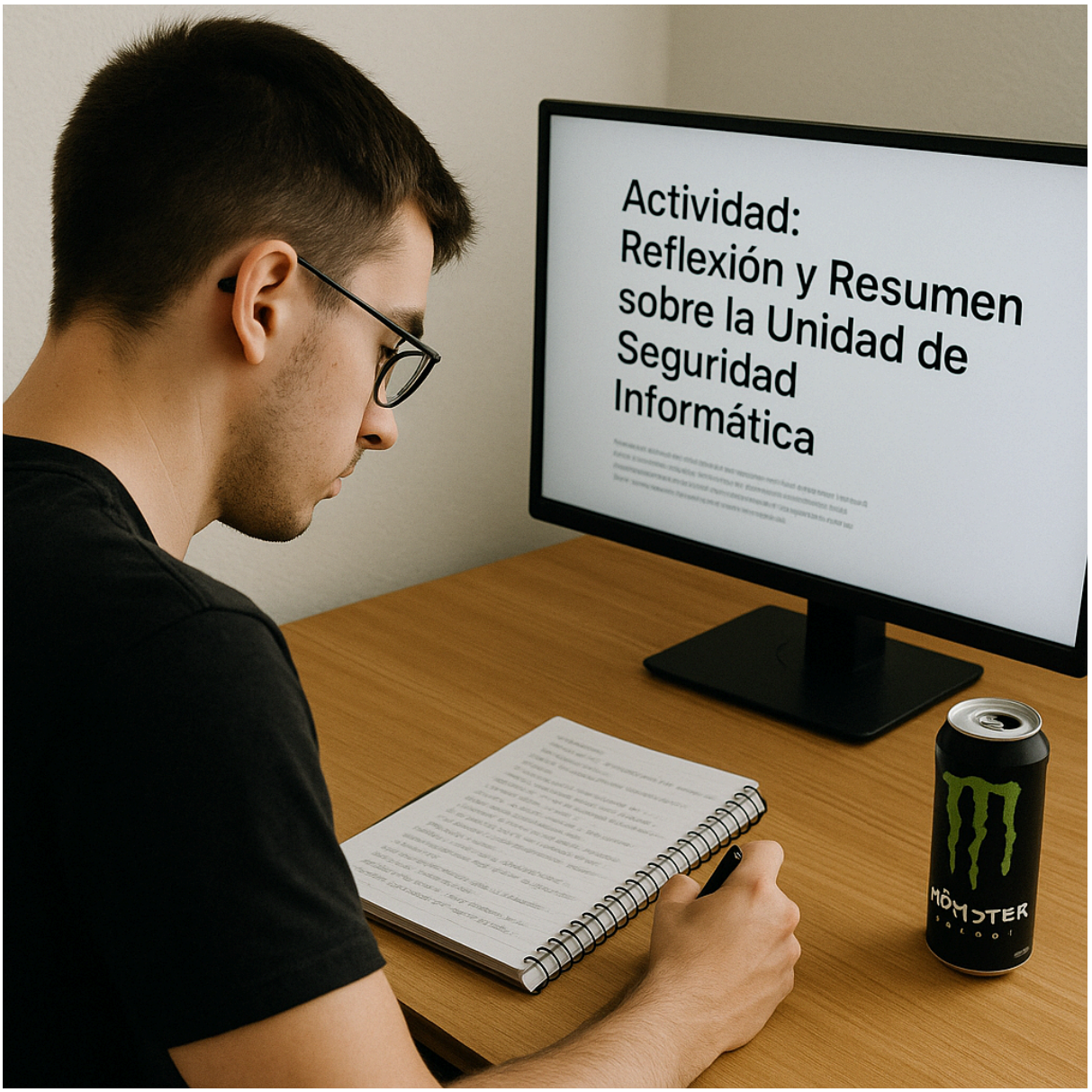
Actividad: Reflexión y Resumen sobre la Unidad de Seguridad Informática



Nicolás Ruiz Ruiz

Incidentes de ciberseguridad

Introducción

Tercera y última actividad de la asignatura de Incidentes de Ciberseguridad. Este podría ser el tema más corto del curso, ya que únicamente hemos visto 4 apartados, “Metodología ante la recolección y almacenamiento de evidencias”, “Análisis e investigación de evidencias”, la “Toma de evidencias" y “MITRE ATT&CK y RE&CT”. Voy a repetir la estructura de los resúmenes anteriores.

¿Qué te han parecido los temas tratados?

Sinceramente, no sé muy bien qué pensar de este temario, me explico, el primer tema de la unidad consistía en desarrollar una guía de cómo actuar en caso que nos llamaran para recolectar evidencias digitales(más adelante detallo más en esto); el segundo, una vez obtenidas estas evidencias, analizarlas en busca de información relevante; y el último, en la toma de evidencias digitales. Es evidente que esta unidad comparte temarios con la de forense, pero con diferentes herramientas, equipos y evidencias.
Voy a detallar mucho más los temas porque con esta opinión parece que no me ha interesado el tema en absoluto, y nada más lejos de la realidad.

Metodología ante la recolección y almacenamiento de evidencias

Este tema consiste en la creación de una metodología propia para los casos de recolección y almacenaje de evidencias. Para ello, tuvimos que analizar varios estándares (ISO, UNE, RFC, etc) y recopilar los puntos más importantes, de otra forma, hemos juntado las plastilinas de todos los colores y para sorpresa de todos, hemos creado un nuevo color. No voy a volver a desarrollar la metodología que hicimos, porque son varias hojas, pero comentaré el punto de los procedimientos, que pienso que es el más interesante, y útil.

Este punto lo dividimos en:

1. Recolección.

   Como su propio nombre indica, consiste en ir a la empresa(digo empresa como estándar, podría ser un colegio, casa, museo, etc.) y recoger de la manera indicada las evidencias. Y no es tan fácil como suena, si lo fuera no tendría un apartado en este punto. Existen muchas formas de recoger las evidencias, pero lo más importante es: **¿El equipo está encendido o apagado?** Si está encendido, debe permanecer encendido hasta llegar al laboratorio, y en caso de que no se pueda, por ejemplo, un pc de sobremesa, se hará la recolección de datos en la propia empresa,

y este equipo no se podrá tocar hasta que termine el proceso. Y si está apagado pues, da un poco igual donde lo hagas, lo único que puedes analizar es el disco.
Bueno, he hablado de recolectar, **¿pero qué recojo?** pues lo que se debe hacer es copiar todos los archivos relevantes siguiendo el orden de volatilidad, o sea, primero RAM y luego disco duro, con estos 2 ya se tiene suficiente, el resto de cosas se pueden encontrar directamente en disco. Otra cosa importante a destacar es que se debe anotar la fecha, hora y hash de la evidencia tomada, así como el autor de dicha recolección.

2. Almacenado.

El almacenado realmente consiste en cómo guardar las evidencias del punto anterior, hasta la llegada al laboratorio de análisis. Resumiendo mucho, los equipos encendidos con conexiones wifi/bluetooth, deben guardarse en bolsas antiestáticas para evitar comunicaciones con el exterior, usar maletines acolchados para los equipos frágiles y por su puesto cajas de seguridad, no candados del chino, cajas grandes de seguridad que solo se puedan abrir con llave, y no con tenazas, del chino también.
Voy a hacer un paréntesis para comentar algo. Es importante mencionar la cadena de custodia, de forma burra, la cadena de custodia es un papel que indica quién tiene X evidencia, además de la fecha y hora de la entrega, y quién se la dió. De esta forma, en caso de modificaciones en las evidencias, podemos ver quién ha podido ser el responsable de esto.
Cerramos el paréntesis y volvemos al transporte. Podemos mover las evidencias de varias formas, pero la única válida es en un vehículo motorizado, ha poder ser una furgoneta, ya que caben más cosas y el “maletero” es más personalizable, pudiendo forrar las paredes con materiales antiestáticos; y por supuesto, ir con el mayor de los cuidados desde la empresa hasta el laboratorio, porque, según el caso, podemos ser objetivos de alguien… malo.
Por último tenemos la llegada al laboratorio, ya estamos a salvo, fuera de peligro y listos para empezar el análisis, pero antes, tenemos que volver a rellenar la cadena de custodia, ya que ahora los “dueños” de las evidencias son otros, y horas diferentes.

3. Análisis.

Este es el apartado más guay… y en el que menos me voy a explayar. Es muy muy denso, pero básicamente, el objetivo del análisis es recrear el equipo a partir de un archivo de disco/RAM en busca de información relevante del caso. Si estás analizando un disco infectado, vas a ver conexiones abiertas, URLs visitadas o archivos maliciosos; si estás analizando un disco en busca de material ilegal, buscarás más en las carpetas, al final es un poco de sentido común, y en caso de no saber muy bien, siempre puedes analizarlo completamente y pasarle el marrón al del informe.

4. Presentación.

Y hablando de informes, aquí tenemos que presentar toda la información que hemos sacado de las evidencias. Si, es tan aburrido como suena, pero es lo que hay, el cliente va a ver esto, no lo que has hecho, piensa que lo que habéis sacado, solo lo entendéis vosotros, los simples mortales no entiende lo que es un “ransomware”, debes explicar qué es y como se ha colado en el dispositivo. Nosotros hicimos un esquema de informe que, cada vez que tenemos que hacer uno, simplemente copiamos, pegamos y rellenamos con los datos nuevos, es bastante cómodo la verdad. Evidentemente, no voy a poner el esquema aquí, pero si puedo poner el índice que usamos siempre:

Estructura del informe

1. Portada: Datos del caso y analista.
2. Introducción: Contexto, objetivos y normativas aplicadas.
3. Descripción de evidencias: Métodos de adquisición, estado y hashes.
4. Metodología de análisis: Herramientas y técnicas empleadas.
5. Resultados: Hallazgos clave, línea de tiempo y actividad sospechosa.
6. Conclusiones y recomendaciones: Impacto del incidente y medidas correctivas.
7. Anexos: Capturas, logs y verificación de integridad.

Si, faltan varios puntos de la metodología, pero esta actividad es un resumen, no un recopilación y debemos cortar muchísimo, igualmente, os dejo aquí el proyecto que hicimos donde se encuentra mucho más desarrollado, además de la presentación. Cosas a comentar, este proyecto ya se hizo en análisis forense, por lo que, realmente, nos centramos en mejorar el proyecto que ya teníamos en base a las correcciones que nos enviaron.

Análisis e investigación de evidencias

Este tema se podría resumir como el punto 3 del tema anterior, nos dan una evidencia, y tenemos que analizarla. Este tema fue más práctico que otra cosa, evidentemente, solo tenemos que buscar información relevante del caso en cuestión. Hicimos 2 prácticas de análisis de evidencias, la primera centrada en analizar información del sistema, donde se nos entregó un volcado completo de un disco y debíamos buscar cosas como el sistema instalado, la versión exacta, etc; y la segunda consistía en analizar los logs del sistema de una máquina que había estado sufriendo ataques, viendo varios intentos de inicio se sesión, uno de ellos con éxito.
Estuvo bastante guay la verdad, siempre hemos estado en la otra parte, la que atacaba, y nunca en el que analiza, como única pega, podría decir que fue demasiado corto, pero tampoco tiene mucho más el tema.

Toma de evidencias

Al igual que el anterior, este tema coincide con el punto 2 de la metodología. Literalmente igual, desde nuestra llegada a la empresa hasta la entrega en el laboratorio. Francamente, he resumido bastante bien el punto de *Almacenado* y volver a hacerlo aquí es absurdo, pero básicamente consiste en llegar, ver los equipos, recoger los dispositivos necesarios, guardarlos debidamente, llevarlos al laboratorio y analizarlas allí; y por supuesto, desarrollar la cadena de custodia. Es literalmente el resumen del resumen.

MITRE ATT&CK y RE&CT

Por último, tenemos las tablas MITRE ATT&CK y RE&CT. Como resumen, ATT&CK es una base de datos de conocimiento que documenta las tácticas y técnicas utilizadas por atacantes reales en entornos del mundo real. Está organizada por fases del ciclo de ataque y cada técnica describe cómo los atacantes alcanzan un objetivo específico. Básicamente, es como un mapa mental del comportamiento del enemigo.
Y por otro lado tenemos RE&CT es un marco complementario a ATT&CK, pero enfocado en las respuestas defensivas. RE&CT te ayuda a decidir *cómo responder bien*. Se trata de una tabla estructurada de contramedidas y controles defensivos que puedes aplicar para mitigar las tácticas y técnicas del ATT&CK. Es útil para analistas defensivos, arquitectos de seguridad y equipos de blue team.
Este tema se dividió en 4 apartados, uno por cada grupo. Al nuestro le tocó el más interesante a mi opinión, aplicar MITRE ATT&CK para analizar un incidente. Analizamos las técnicas utilizadas por los ciberdelincuentes y las técnicas de mitigación y detección. Durante el proceso del análisis, tuvimos que editar nuestra propia tabla, resultando en un proceso bastante cómodo y didáctico.

¿Qué te ha parecido más útil para tu futuro puesto de trabajo en un equipo de seguridad?

Sería un poco trampa elegir el tema de la metodología, ya que abarca los 3 primeros temas, pero siendo objetivos, creo que es el mejor, explica paso a paso cómo tenemos que recolectar, transportar y analizar las evidencias.

¿Conocías todos los puntos tratados en la unidad? ¿Cuáles no?

Como dije antes, esta unidad comparte mucho contenido con forense, por lo que sí, conocía varios puntos de la unidad, para ser más concreto, el único punto que no conocía del todo, eran las tablas MITRE ATT&CK y RE&CT.

¿Alguno te ha llamado especialmente la atención? ¿Por qué?

Si por supuesto, el tema de Análisis de evidencias ya que, como dije antes, tratamos la investigación forense desde otro punto de vista en el que tenemos que investigar qué ha pasado en el sistema.

¿Descartarías algún punto de la unidad? ¿Cuál y por qué?

No descartaría ningún punto de la unidad, lo que sí, se podría dar una vuelta a la metodología, ya que es el primer proyecto que se hace en forense entonces sucede lo que comenté antes, corregimos el que hicimos anteriormente.

¿Has echado en falta algún tema?

Ahora que hemos terminado el temario completo, puedo decir con seguridad que no, no echo en falta ningún tema en concreto, pienso que todos los temas dados en el curso han sido bastante relevantes. Además, había un buen equilibrio entre teoría y práctica, lo cual ayuda bastante a la comprensión.