Tarea online IC03.

Título de la tarea: Investigación de incidentes de ciberseguridad.

Curso de Especialización y módulo: Ciberseguridad en Entornos de las Tecnologías de la Información - Incidentes de Ciberseguridad.

¿Qué contenidos o resultados de aprendizaje trabajaremos?

Resultados de aprendizaje

- **RA3.** Investiga incidentes de ciberseguridad analizando los riesgos implicados y definiendo las posibles medidas a adoptar.

Contenidos

1.- Recopilación de Evidencias.
- 1.1.- Principios durante la recolección de evidencias.
  - 1.1.1.- Orden de volatilidad.
  - 1.1.2.- Acciones que deben evitarse.
  - 1.1.3.- Consideraciones sobre la privacidad.
- 1.2.- Procedimiento de recolección.
  - 1.2.1.- Transparencia.
  - 1.2.2.- Pasos.
- 1.3.- El procedimiento de almacenamiento.
  - 1.3.1.- Cadena de custodia.
  - 1.3.2.- Dónde y cómo almacenar las evidencias.
- 1.4.- Herramientas necesarias.
- 1.5.- Conclusiones de la Recopilación.

2.- Análisis de Evidencias.
3.- Investigación del Incidente.
4.- Intercambio de Información del Incidente con Proveedores u Organismos Competentes.
5.- Medidas de Contención de Incidentes.
6.- Bibliografía.

1.- Descripción de la tarea.

Las Técnicas de Investigación de Incidentes

Como hemos estudiado en la Unidad 3, las técnicas de investigación de incidentes están asociadas al momento en el que se efectúa la investigación del incidente, a saber:

INCIBE. *Investigación Incidentes Ciberseguridad* (CC0)

- **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.

¿Qué te pedimos que hagas?

- **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.**

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.

  - 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?

- **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:

WorkPC.ova

Credenciales de acceso: usuario: Worker. Clave: Unp4wn4ble
Máquina preparada para instalar en VirtualBox.

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?

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

- 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.

- 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”).

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.

- 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.

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

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.

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

2.- Información de interés.

Recursos necesarios y recomendaciones

Recursos necesarios

Se trata de un ejercicio práctico, por lo que hará falta:

- Un ordenador personal con Sistema Operativo Windows y Microsoft Office.
- Software de virtualización (VirtualBox) para máquina virtual Windows proporcionada.
- Software de verificación de hashes.
- Software de análisis de imágenes.

Recomendaciones

- Antes de abordar la tarea:
  - lee con detenimiento la unidad, consulta los enlaces para saber más, examina el material proporcionado por el profesor y aclara las dudas que te surjan con él.
  - Realiza el examen online de la unidad, y consulta nuevamente las dudas que te surjan. Solo cuando lo tengas todo claro, debes abordar la realización de la tarea.
- No olvides elaborar el documento explicativo.

Indicaciones de entrega

Una vez realizada la tarea, el envío se realizará a través de la plataforma. El archivo se nombrará siguiendo las siguientes pautas:

Apellido1_Apellido2_Nombre_IC03_Tarea

Asegúrate que el nombre no contenga la letra ñ, tildes ni caracteres especiales extraños. Así por ejemplo la alumna Begoña Sánchez Mañas para la tercera unidad del MP de IC, debería nombrar esta tarea como...

sanchez_manas_begona_IC03_Tarea

3.- Evaluación de la tarea.

Criterios de evaluación implicados

Criterios de evaluación RA3

- **a) Se han recopilado y almacenado de forma segura evidencias de incidentes de ciberseguridad que afectan a la organización.**
- **b) Se ha realizado un análisis de evidencias.**
- **c) Se ha realizado la investigación de incidentes de ciberseguridad.**
- d) Se ha intercambiado información de incidentes, con proveedores y/o organismos competentes que podrían hacer aportaciones al respecto.
- e) Se han iniciado las primeras medidas de contención de los incidentes para limitar los posibles daños causados.

¿Cómo valoramos y puntuamos tu tarea?

Rúbrica de la tarea	
Apartado 1: a) Identifica un posible tipo de incidente clasificándolo de forma correcta según la taxonomía de ciberincidentes de seguridad y justifica la respuesta.	0,5 puntos (obligatorio)
Apartado 1: b) Justifica de forma correcta si el software descargado puede ser un malware y describe cómo se puede comprobar la integridad del software.	0,5 puntos (obligatorio)
Apartado 2: a) Justifica de forma correcta si se puede obtener información de la memoria RAM y cachés.	0,5 puntos (obligatorio)
Apartado 2: b) Detecta posibles conexiones de red sospechosas de ser provocadas por un malware y justifica esta conclusión.	0,5 puntos (obligatorio)
Apartado 2: c) Localiza el servicio sospechoso y en el registro de Windows algunos registros relacionados que lo activan.	1 punto (obligatorio)
Apartado 2: d) Localiza el proceso sospechoso que puede abrir una puerta trasera en el equipo.	0,5 puntos (obligatorio)
Apartado 2: d) Localiza el fichero ejecutable que puede abrir una puerta trasera en el equipo.	0,5 puntos (obligatorio)

Apartado 2: d) Localiza la entrada del registro que lanza el proceso con el inicio del sistema.	0,5 puntos (obligatorio)
Apartado 2: d) Localiza la regla de firewall que permite la conexión desde el exterior.	0,5 puntos (obligatorio)
Apartado 3: a) Comprueba la integridad del fichero descargado explicando el método usado.	0,5 puntos (obligatorio)
Apartado 3: b) Localiza el fichero que contiene errores en sus datos de cabecera indicando el error localizado.	0,5 puntos (obligatorio)
Apartado 3: b) Corrige los errores del fichero y muestra el fichero de forma correcta indicando cómo lo ha reparado.	0,5 puntos (obligatorio)
Apartado 3: c) Encuentra el fichero ofuscado entre los archivos del pen de datos explicando cómo lo ha localizado.	1 punto (obligatorio)
Apartado 3: c) Muestra el contenido del fichero indicando cómo ha conseguido obtener la información.	0,5 puntos (obligatorio)
Apartado 4: a) Explica dos aspectos que han fallado en la seguridad de la empresa.	1 punto (obligatorio)
Apartado 4: b) Explica dos salvaguardas para reducir los riesgos de sufrir el mismo incidente de seguridad acontecido.	1 punto (obligatorio)