Tarea online IC07.

Título de la tarea: Monitorización Multipunto en SIEM.

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

- **RA2**. Analiza incidentes de ciberseguridad utilizando herramientas, mecanismos de detección y alertas de seguridad.

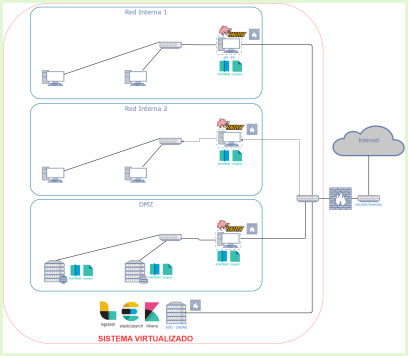
Contenidos

1.- Escenario de Trabajo SIEM.
- 1.1.- Premisas para la Práctica SIEM.
- 1.2.- Instalación de OpenJDK.
- 1.3.- Instalación de Elasticsearch.
  - 1.3.1.- Descarga y Edición del Fichero de Configuración.
  - 1.3.2.- Limitación del Uso de la Memoria RAM.
  - 1.3.3.- Arranque y Chequeo de Status.
  - 1.3.4.- Uso de Nmap para Comprobar Acceso a Elasticsearch.
- 1.4.- Instalación de Logstash.
  - 1.4.1.- Descarga, Instalación y Limitación del Uso de la RAM.
  - 1.4.2.- Edición del Fichero de Configuración, Arranque y Comprobación del Status.
  - 1.4.3.- Revisión del Log de Arranque y Parada de la Aplicación.
- 1.5.- Instalación de Kibana.
  - 1.5.1.- Descarga de Node.js.
  - 1.5.2.- Procedimiento de Instalación.
  - 1.5.3.- Configuración de Kibana.
  - 1.5.4.- Sustitución de Node.js por su versión correcta.
  - 1.5.5.- Edición de un Fichero de Servicio y Arranque.
- 1.6.- Configuración SIEM.
  - 1.6.1.- Arranque del SIEM.
  - 1.6.2.- Pipelines en Logstash.
- 1.7.- Visualización SIEM.
  - 1.7.1.- Arranque de Kibana desde el Navegador.
  - 1.7.2.- Configuración de Kibana.
  - 1.7.3.- Manejo de Kibana.
  - 1.7.4.- Creación de un Histograma.

1.- Descripción de la tarea.

La Monitorización Multipunto en el SIEM

En la Unidad 7 hemos estudiado cómo instalar y configurar un SIEM ELK completo, situándolo en la misma red que los diferentes agentes IDS que detectarán las intrusiones y enviarán la información de registros de SNORT a traves de Filebeat.



José Antonio Santos *Esquema Maqueta Tareas 6 y 7* (CC0)

La estrucura creada en la Tarea 6, es la presente en cualquier entorno productivo en la que suele haber una sonda Snort en cada una de las máquinas perimetrales, comprometidas, vulnerables, etc., cuya información de logging se ha de redirigir hacia una única máquina en la que estará instalado el SIEM (Elastic Stack).

Pues bien, continuando con el trabajo iniciado en la Tarea 6 asociada a la Unidad 6, en esta tarea abordaremos la lectura y tratamiento del log que centraliza la información de todas las sondas Snort, filtrando su contenido, almacenándolo en la base de datos y preparando un conjunto de visualizaciones que recogeremos en un Tablero de Monitorización Multipunto.

¿Qué te pedimos que hagas?

- **Apartado 1: Instalación y configuración de Elasticsearch.**

  Deberás efectuar las siguientes tareas:

  - a) Detallar la configuración a efectuar en Elasticsearch.
  - b) Prueba de funcionamiento de Elasticsearch.

- **Apartado 2: Instalación y configuración de Kibana.**

  Deberás efectuar las siguientes tareas:

- a) Detallar la configuración a efectuar en Kibana.
- b) Prueba de acceso al menú principal de Kibana.

- **Apartado 3: Instalación y configuración de Filebeat.**

  Deberás efectuar las siguientes tareas:

  - a) Detallar la configuración a efectuar en el agente IDS para enviar los registros de Snort a Logstash.
  - b) Mostrar una prueba de funcionamiento de Filebeat mostrando los registros por consola.

- **Apartado 4: Instalación y configuración de Logstash.**

  Deberás efectuar las siguientes tareas:

  - a) Detallar la configuración a efectuar en Logstash para recibir los logs de Filebeat y reenviarlos a Elasticsearch.
  - b) Mostrar una prueba de funcionamiento en la que se puede visualizar la información del índice de logstash en Kibana.

- **Apartado 5: Creación de un filtro en Logstash.**

  Deberás efectuar las siguientes tareas:

  - a) Detallar la configuración a efectuar en Logstash para crear un Pipeline que filtre la información creando campos para los diferentes valores del mensaje de log creado en Snort.
  - b) Mostrar el índice que se crea con la información de sus diferentes campos.

- **Apartado 6: Tablero de Monitorización Multipunto.**

  Deberás efectuar las siguientes tareas:

  - a) Detallar la creación de dos contadores, uno para todos los PINGs desde la red interna y otro para los de la red externa.
  - b) Detallar la creación de dos histogramas, uno para los intentos de inicio de sesión por SSH y otro para los accesos a PHPMyadmin.
  - a) Detallar la creación de un nuevo tablero (dashboard) en Kibana que contenga los contadores y los histogramas creados anteriormente.

NOTA IMPORTANTE

Cuando sea necesario entregar capturas de pantalla para reflejar las acciones realizadas, dichas capturas deberán tener como fondo de pantalla la plataforma con tu usuario mostrando claramente la foto de tu perfil, pues esta es una condición imprescindible para que dicha información se tenga en cuenta en el momento de la corrección. Además, estas capturas de pantalla tendrán resolución suficiente como para que resulten legibles los comandos, las respuestas y los volcados de información pertinentes.

2.- Información de interés.

Recursos necesarios y recomendaciones

Recursos necesarios

- Ordenador personal con un mínimo de 8 Gigabytes de memoria RAM. Recomendables 16 GB.
- Sistema Operativo Windows 10/11. Se pueden usar sistemas alternativos.
- Navegador Web.
- Hipervisor de Virtualización. Preferiblemente Virtualbox.

Recursos adicionales

- Conceptos teóricos sobre el Elastic Stack.
- Guía de instalación del Elastic Stack.

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. Sólo 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_IC07_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 séptima unidad del MP de IC, debería nombrar esta tarea como...

sanchez_manas_begona_IC07_Tarea

3.- Evaluación de la tarea.

Criterios de evaluación implicados

Criterios de evaluación RA2

- a) Se ha clasificado y definido la taxonomía de incidentes de ciberseguridad que pueden afectar a la organización.
- **b) Se han establecido controles, herramientas y mecanismos de monitorización, identificación, detección y alerta de incidentes.**
- c) Se han establecido controles y mecanismos de detección e identificación de incidentes de seguridad física.
- d) Se han establecido controles, herramientas y mecanismos de monitorización, identificación, detección y alerta de incidentes a través de la investigación en fuentes abiertas (OSINT: Open Source Intelligence).
- e) Se ha realizado una clasificación, valoración, documentación y seguimiento de los incidentes detectados dentro de la organización.

¿Cómo valoramos y puntuamos tu tarea?

Rúbrica de la tarea	
Apartado 1: a) Detallar la configuración a efectuar en Elasticsearch.	1 puntos (obligatoria)
Apartado 1: b) Prueba de funcionamiento de Elasticsearch.	0,25 puntos (obligatoria)
Apartado 2: a) Detallar la configuración a efectuar en Kibana.	1 puntos (obligatoria)
Apartado 2: b) Prueba de acceso al menú principal de Kibana.	0,25 puntos (obligatoria)
Apartado 3: a) Detallar la configuración a efectuar en el agente IDS para enviar los registros de Snort a Logstash.	1 puntos (obligatoria)
Apartado 3: b) Mostrar una prueba de funcionamiento de Filebeat mostrando los registros por consola.	0,25 puntos (obligatoria)
Apartado 4: a) Detallar la configuración a efectuar en Logstash para recibir los logs de Filebeat y reenviarlos a Elasticsearch.	1 puntos (obligatoria)
Apartado 4: b) Mostrar una prueba de funcionamiento en la que se puede visualizar la información del índice de logstash en Kibana.	0,25 puntos (obligatoria)

Apartado 5: a) Detallar la configuración a efectuar en Logstash para crear un Pipeline que filtre la información creando campos para los diferentes valores del mensaje de log creado en Snort.	0,8 puntos (obligatoria)
Apartado 5: b) Mostrar el índice que se crea con la información de sus diferentes campos.	0,2 puntos (obligatoria)
Apartado 6: a) Detallar la creación de dos contadores, uno para todos los PINGs desde la red interna y otro para los de la red externa.	1,5 puntos (obligatoria)
Apartado 6: b) Detallar la creación de dos histogramas, uno para los intentos de inicio de sesión por SSH y otro para los accesos a PHPMyadmin.	1,5 puntos (obligatoria)
Apartado 6: c) Detallar la creación de un nuevo tablero (dashboard) en Kibana que contenga los contadores y los histogramas creados anteriormente.	1 puntos (obligatoria)

NOTA IMPORTANTE

Cuando sea necesario entregar capturas de pantalla para reflejar las acciones realizadas, dichas capturas deberán tener como fondo de pantalla la plataforma con tu usuario mostrando claramente la foto de tu perfil, pues esta es una condición imprescindible para que dicha información se tenga en cuenta en el momento de la corrección. Además, estas capturas de pantalla tendrán resolución suficiente como para que resulten legibles los comandos, las respuestas y los volcados de información pertinentes.