Tarea online IC06.

Título de la tarea: Detección Multipunto de Incidentes.

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

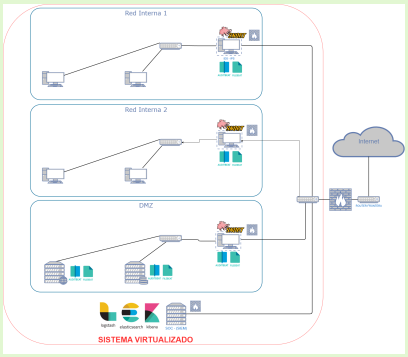
1.- Prototipo de un SOC.
- 1.1.- Prevención de Intrusiones.
- 1.2.- Snort - El IDS/IPS de Código Abierto.
- 1.3.- Instalación y Configuración de Snort.
- 1.4.- Inicio, Arranque y Parada de Snort.
- 1.5.- Ficheros de Configuración Básica de Snort.
- 1.6.- Fichero de Registro de Alertas de Snort.
- 1.7.- Torre de Protocolos ISO-OSI.
- 1.8.- Detección de Tráfico ICMP con Snort.
  - 1.8.1.- Posición del Protocolo ICMP en la Torre de Comunicaciones.
  - 1.8.2.- Construcción de Reglas para Snort.
  - 1.8.3.- Ejemplo de Regla Snort.
  - 1.8.4.- Configuración de Snort para Detección de Tráfico ICMP.
  - 1.8.5.- Práctica de Detección.
- 1.9.- Detección de Tráfico SSH con Snort.
  - 1.9.1.- Posición del Protocolo SSH en la Torre de Comunicaciones.
  - 1.9.2.- Detalle de la regla específica para detección SSH.
  - 1.9.3.- Detección de Tráfico TCP/SSH.

2.- Bibliografía.

1.- Descripción de la tarea.

La Detección Multipunto de Incidentes

En la Unidad 6 hemos estudiado cómo instalar y configurar el IDS Snort, situándolo en la misma máquina en la que estará el SIEM que procesará su información una vez filtrada y almacenada.



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

Sin embargo, aunque esta configuración es habitual en los laboratorios, no es la corriente en las instalaciones reales. En cualquier entorno productivo 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 (Unidad 7).

En esta tarea abordaremos el registro de logs en los diferentes agentes IDS en tiempo real utilizando la aplicación SNORT.

¿Qué te pedimos que hagas?

Para el desarrollo de la práctica nos centraremos en la red DMZ, en concreto sobre el SNORT situado en dicha zona y una de las máquinas, la cual, tiene instalado los servicios SSH, HTTP y MySQL. Esta última máquina se proporciona en esta tarea (WebServer).

- **Apartado 1: Configurar las máquinas virtuales para que tengan comunicación completa.**

  Deberás efectuar las siguientes tareas:

  - Crear la máquina IDS (Snort) con dos interfaces de red y configurarla para que permita la comunicación completa entre ambas interfaces. Una tomará el rol de adaptador puente con la red externa y la otra interfaz sería la puerta de enlace predeterminada de la red DMZ. Se debe mostrar el fichero de configuración de las interfaces de red. *Se recomienda el uso de Ubuntu SERVER o DEBIAN.*
  - Configurar la máquina IDS para que las máquinas de la red interna DMZ (WebServer) se puedan comunicar correctamente con el exterior. Se debe

conseguir acceso a internet y a la red externa.
- Crear una máquina virtual que se denomine SOC, la cual esté conectada a la red externa (adaptador puente). Esta máquina debe tener comunicación con el WebServer. La máquina SOC debe tener interfaz gráfica, por lo que se recomienda la instalación de Ubuntu Desktop.

- **Apartado 2: Configuración del IDS para registrar el tráfico de red. (SNORT)**

  Deberás efectuar las siguientes tareas:

  - Instalar y configurar SNORT en el IDS para poder escuchar y guardar todo el tráfico de la red DMZ.
  - Configurar las reglas de detección de Snort, cada una de ellas debe recoger un mensaje indicando el tipo de conexión que se establece y un identificador único. Las alertas a generar son:
    - Ping (Request) desde la red interna (DMZ) hacia el exterior. Se debe registrar únicamente el Request de la interna y no la respuesta de la externa.
    - Ping (Request) desde el exterior hacia la DMZ. Se debe registrar únicamente el Request de la externa y no la respuesta de la DMZ.
    - Intentos de las conexiones SSH hacia WebServer. Solamente registra el primer paquete de sincronización de este intento de conexión.
    - Intentos de las conexiones HTTP hacia WebServer. Solamente registra el primer paquete de sincronización de este intento de conexión.
    - Intentos de las conexiones a phpMyAdmin hacia WebServer. La ruta hacia la base de datos es *http://ip-de-WebServer/phpmyadmin*.

- **Apartado 3: Pruebas de las alertas generadas.**

  Deberás efectuar las siguientes tareas:

  - Realizar las pruebas pertinentes donde se demuestren las diferentes alertas generadas en el apartado 2.
  - Para cada una de estas alertas se debe recoger pantallazo con las acciones realizadas y un volcado final del archivo de log resultante tras todas las pruebas.

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, auxiliares y recomendaciones

Recursos necesarios

- Ordenador personal con un mínimo de 8 Gigabytes de memoria RAM, Sistema Operativo Windows 10/11 o alternativo y Navegador Web.
- Hipervisor de virtualización: Virtualbox o alternativo.

Recursos auxiliares:

- Apuntes sobre el firewall. Conceptos básicos teóricos.
- IPTABLES: Firewall de red por sofware.
- Habilitar IPTABLES como servicio. Habilitar tráfico que atraviesa el equipo (forwarding).

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_IC06_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 sexta unidad del MP de IC, debería nombrar esta tarea como...

sanchez_manas_begona_IC06_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: Configura las dos interfaces de red del IDS	0.5 puntos (obligatoria)
Apartado 1.b: Habilita correctamente el tráfico que atraviesa el IDS (Forwarding) y crea en iptable la regla de NAT que habilita el tráfico saliente.	1 punto (obligatoria)
Apartado 1.c: Configura la interfaz de red del SOC con una dirección estática y configura en el SOC la ruta estática para conectarse a la DMZ.	0.5 puntos (obligatoria)
Apartado 2.a: Describe en detalle la configuración a efectuar en dos o más máquinas para habilitar la tranmisión de información de logging entre ellas, en tiempo real.	0.5 puntos (obligatoria)
Apartado 2.b: Realiza las reglas SNORT para: ping interno, ping externo, conexiones SSH, conexiones HTTP y conexiones a la base de datos (phpMyadmin).	5 puntos (obligatoria)
Apartado 3.a: Realiza pruebas para demostrar el funcionamiento de las diferentes alertas.	2 puntos (opcional)

Apartado 3.b: Vuelca el fichero de log resultante tras probar las alertas.	0.5 puntos (opcional)

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.