Examen monitorizacion

Edición 5

*Obligatorio

Correo *

e202010663@upc.edu.pe

Nom i cognoms

Ernesto Guarda Higginson

En el ámbito de la seguridad informática, los logs deben tener una característica fundamental. ¿Cuál es?

- (●) Relevancia
- ( ) Dualidad
- ( ) Trazabilidad
- ( ) Correlación

Borrar selección

¿En qué consiste la administración de registros (log management)?

- ○ Archivado centralizado de mensajes de registro
- ◉ Tratamiento de grandes volúmenes de mensajes de registro generados por sistemas y dispositivos
- ○ Creación de reglas para la clasificación de los mensajes de registro
- ○ Correlación de los mensajes de registro

Borrar selección

¿Cuáles son los elementos clave de la administración y guardado de registros?

- ◉ Volumen de logs, heterogeneidad de formato y la arquitectura de las redes y sistemas
- ○ Volumen de logs, clasificación y correlación de los mismos
- ○ Clasificación de logs, correlación y análisis de los mismos
- ○ Volumen de registros y correlación de los mismos

Borrar selección

¿Cómo se llaman los ficheros locales en los que se registran los sucesos que ocurren en el sistema operativo?

- ○ Ficheros de sucesos
- ○ Registros de sucesos
- ○ Registro
- ◉ Ficheros de log

Borrar selección

¿Cómo se llama el servicio de Windows que permite registrar, consultar y suscribirse a eventos?

- ○ RegistryService
- ○ EventService
- ○ LogService
- ◉ EventLog

Borrar selección

En qué sistema operativo podemos tener rsyslog?

- ○ Windows 10
- ◉ Linux y sus variantes
- ○ Windows 2022 Server
- ○ Windows 8

Borrar selección

¿Qué programa permite guardar filtros de eventos útiles como vistas personalizadas para usarlas en el futuro?

- ◉ Event Viewer
- ○ Management Console
- ○ Task Scheduler
- ○ WEvtUtil

Borrar selección

Dado este comando: eventcreate /t error /id 100 /l application /d"Create event in application log"

- ○ Da error ya que el ID tiene que ser menor que 100
- ○ No funciona, falta la prioridad
- ◉ Creará un evento ficticio con el texto "Create event in application log"
- ○ El parametro application es incorrecto

Borrar selección

¿Qué comando se usaría para mostrar las últimas diez líneas de un fichero?

- ◉ tail -f file.log
- ○ tail -f 10 file.log
- ○ tail -n 10 file.log
- ○ tail -n +11 file.log

Borrar selección

¿Cómo se puede garantizar la entrega de mensajes syslog?

- ○ Enviando los mensajes por duplicado
- ◉ Usando el protocolo TCP
- ○ Utilizando un listener para recoger los mensajes
- ○ No se puede

Borrar selección

¿Qué IDS son muy efectivos para detectar amenazas previas conocidas?

- ○ Los IDS basados en red
- ○ Los IDS basados en host
- ◉ Los IDS basados en firmas
- ○ Los IDS basados en anomalías

Borrar selección

¿Qué comando de Snort se utilizará para ver el payload de los paquetes que pasan por la interfaz eth0?

- ○ snort -v -i eth0
- ○ snort -v -p -i eth0
- ◉ snort -v -d -i eth0
- ○ Cualquiera de los anteriores

Borrar selección

¿Cuál de las siguientes reglas de Snort es incorrecta?

- ○ alert tcp $EXTERNAL_NET any → $HOME_NET any (msg:"A"; sid:100;)
- ◉ alert tcp $HOME_NET any ← $EXTERNAL_NET any (msg:"A"; sid:101;)
- ○ alert tcp $EXTERNAL_NET any → $HOME_NET 80 (msg:"A"; sid:102;)
- ○ alert tcp $EXTERNAL_NET 80 → $HOME_NET 80 (msg:"A"; sid:103;)

Borrar selección

¿Qué acción en una regla de Snort permite alertar y activar otra regla dinámica almismo tiempo?

- ○ alert
- ○ dynamic
- ○ log
- ◉ activate

Borrar selección

En una regla de detección de contenido de Snort, ¿cuál de las siguientesafirmaciones es falsa?

- ○ offset indica la posición del paquete donde empezar a buscar el patrón
- ◉ distance indica la posición dónde se ha encontrado el patrón
- ○ depth indica la posición del paquete hasta la cual se buscará el patrón
- ○ Ninguna de las anteriores

Borrar selección

¿En qué consiste el proceso de decodificación en OSSEC?

- ◉ Extracción de la información genérica de los logs (p.ej. el nombre de host)
- ○ Identificación de la información clave de los logs (p.ej. la dirección IP)
- ○ Comprobación de las firmas leyendo un fichero XML
- ○ Escribir módulos del programa

Borrar selección

Puede OSSEC monitorizar la integridad del sistema de ficheros?

- ○ Si, pero debe configurarse
- ◉ Si, viene activado por defecto
- ○ No, esto solo puede realizarse con Splunk
- ○ No, pero Wazuh si puede

Borrar selección

¿Cuál de las siguientes herramientas NO está incluída en OSSIM?

- ○ OSSEC
- ○ Snort
- ○ Nagios
- ◉ Wazuh

Borrar selección

La transformación de un mensaje de registro en campos comunes que luego serán almacenados en una base de datos para poder ser consultados se llama ...

- ◉ Correlación
- ○ Normalización
- ○ Decodificación
- ○ Análisis
- ○ Option 5

Borrar selección

¿Cuál de las siguientes afirmaciones sobre Splunk Free no es correcta?

- ○ No permite generar informes en PDF
- ○ No permite monitorizar en tiempo real
- ○ No permite indexar más de 500MB/día
- ◉ No tiene integración con SSO

Borrar selección

Enviar Borrar formulario