

T5. Proceso de notificación y gestión de intentos de intrusión



Apartados del BOE (1/2)

- * Establecimiento de las responsabilidades en el proceso de notificación y gestión de intentos de intrusión o infecciones
- * Categorización de los incidentes derivados de intentos de intrusión o infecciones en función de su impacto potencial
- * Criterios para la determinación de las evidencias objetivas en las que se soportara la gestión del incidente
- * Establecimiento del proceso de detección y registro de incidentes derivados de intentos de intrusión o infecciones
- * Guía para la clasificación y análisis inicial del intento de intrusión o infección, contemplando el impacto previsible del mismo

Apartados del BOE (2/2)

- * Establecimiento del nivel de intervención requerido en función del impacto previsible
- * Guía para la investigación y diagnóstico del incidente de intento de intrusión o infecciones
- * Establecimiento del proceso de resolución y recuperación de los sistemas tras un incidente derivado de un intento de intrusión o infección
- * Proceso para la comunicación del incidente a terceros, si procede
- * Establecimiento del proceso de cierre del incidente y los registros necesarios para documentar el histórico del incidente

Factores de detección

- * Los elementos que intervienen en el análisis de la detección de intrusiones son de diversa naturaleza:
 - * Factor humano
 - * Eventos externos
 - * Preámbulos de intrusiones





* **Factor humano**

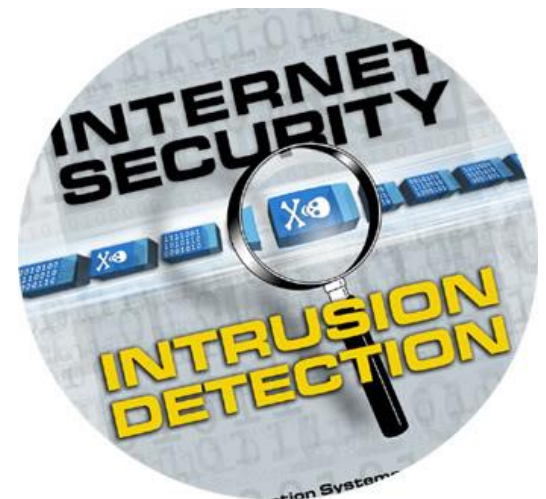
- * Esta es la fuente de información de intrusiones más común y tradicional, pero no quiere decir que sea la mejor, por ejemplo: mientras que el Snort detecta miles de intrusiones, un humano solo podría llegar al 2%

* **Eventos externos**

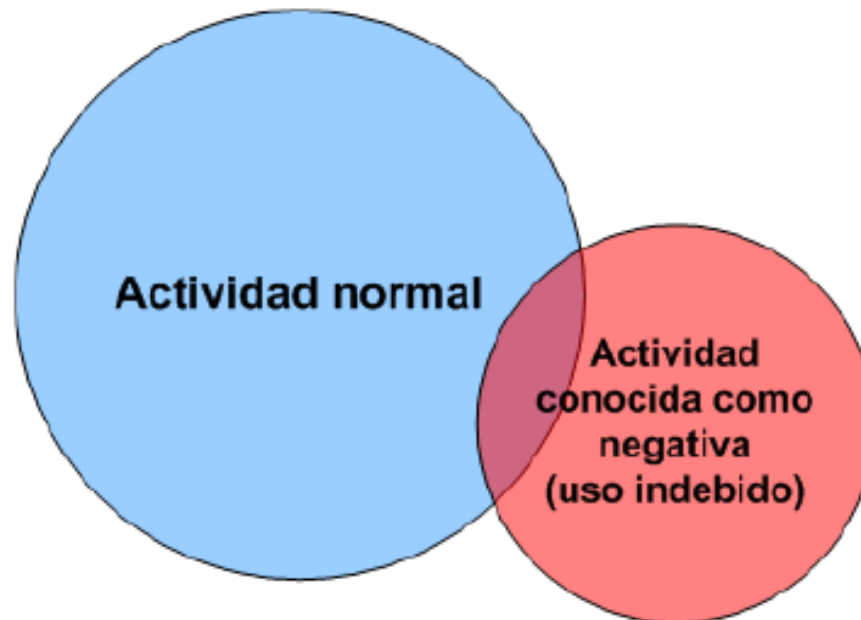
- * Cualquier evento externo al sistema puede aportar información sustancial al análisis:
 - * La contratación o despido de empleados clave en la gestión de seguridad
 - * un inusual crecimiento de informes de anomalías de un determinado sistema
 - * los resultados de baterías de pruebas de vulnerabilidades contra sistemas, etc

* Preámbulos de intrusiones

- * Se puede averiguar si un sistema va a ser atacado si presenta ciertas evidencias de intrusiones.
- * Algunas de estos síntomas pueden ser la instalación de un troyano, la adicción de nuevas cuentas de usuario no autorizados al sistema, etc



Modelos de detección de intrusiones



Toda la actividad del sistema

Actividades de un sistema: usos indebidos y anomalías

Tipos de respuesta

- * Respuestas activas
- * Respuestas pasivas





* **Respuestas activas**

- * Estas respuestas afectan al progreso del ataque, pueden ser llevadas a cabo de forma automática por el sistema, o mediante intervención humana
- * Estas acciones pueden ser de diversa naturaleza, no obstante, la mayoría se pueden clasificar en 3 categorías principales
 1. **Ejecutar acciones contra el intruso**
 2. **Corregir el entorno**
 3. **Recopilar más información**

1. Ejecutar acciones contra el intruso

- * La **más famosa** de las respuestas activas, es la de tomar acciones contra el intruso.
- * La forma más directa en **identificar el origen de ataque**, e **impedirle el acceso al sistema**, por ejemplo, desactivando una conexión de red, o bloqueando la máquina comprometida
- * Sin embargo tomar decisiones tan agresivas **no es siempre buena solución**, hay situaciones que esto podría causar serios problemas:



- * Problemas (1/3):

- * Los **ataques** recibidos a menudo son realizados, **no desde la propia máquina del intruso**, sino desde una **víctima controlada** por aquel.
- * El intruso puede haber utilizado a su víctima mediante algún **programa de control remoto**, o como resultado de un **fallo de seguridad** que le permitiera entrar.
- * Si se bloquea o incluso devuelve el ataque en esta situación, se estaría **perjudicando a alguien inocente**




- * Problemas (2/3)


- * En muchas ocasiones, los atacantes utilizan técnicas de **ocultación de su dirección IP (spoofing)**
- * En este tipo de ataques, las **direcciones IP** de origen **no tienen nada que ver con el atacante.**
- * Incluso pueden no **existir**, hecho beneficioso en casos de ataque de denegación de servicio, en los que el servidor pierde demasiado tiempo esperando la respuesta de direcciones IP que no responden nunca



- * Problemas (3/3)

- * Por otra parte, responder de forma automática a intrusiones puede provocar **penalizaciones legales**
- * Si se devuelve el ataque a una **entidad inocente**, puede efectuar una **demanda por daños y perjuicios**
- * Además, en algunas organizaciones, tomar este tipo de decisiones sin la autorización adecuada puede ser razón de despido

- 
- * Se pueden realizar **acciones** contra **intrusos menos drásticas**
 - * Terminando la sesión TCP problemática
 - * Bloquear durante un intervalo de tiempo el origen de las intrusiones
 - * Enviando un correo electrónico al administrados
 - * Etc.

- 
- * Hay que tener en cuenta que ejecutar **una respuesta definitiva**, de forma **automática**, es algo **delicado**.
 - * Ejp:
 - * Si en un determinado entorno se **bloquean permanentemente las direcciones IP** que intentan **demasiadas conexiones** con el servidor, y un intruso se percata de ello, puede elaborar un **ataque** que consista en realizar **sucesivos intentos de conexión con direcciones falseadas**, pertenecientes a los **clientes** más importantes
 - * De esta forma, el propio detector de intrusiones estaría **bloqueando a sus propios clientes**, ayudando a un **ataque DoS**

2. Corregir el entorno

- * Consiste en efectuar las **acciones** pertinentes para **restaurar el sistema y corregir los posibles problemas de seguridad existentes**.
- * En la mayoría de las ocasiones, esta **respuesta activa suele ser la acción más acertada**
- * Aquellos sistemas que cuentan con métodos de **auto-curación**, son capaces de identificar el problema y proporcionar los métodos adecuados para corregirlos





* **Recopilar más información**

- * Esta opción es utilizada para cumplir los **requisitos necesarios** para **poder tomar acciones legales** contra posibles **criminales**.
- * Normalmente se aplica en sistemas que proporcionan **servicios críticos**
- * Para ello se utilizan **máquinas** o redes **que imitan comportamientos y servicios reales**, para engañar a los intrusos, **servidores decoy** (trampa), **fishbowl** (peceras) o **honeypots** (tarros de miel)

* **Respuestas pasivas**

- * Son aquellas respuestas que consisten en el envío de información al responsable correspondiente, dejando recaer en él la toma de decisiones.
- * Por muy afinados que sean los mecanismos de respuesta automática, hay ocasiones en que un sistema no tiene la responsabilidad suficiente para tomar una decisión.
- * Alarmas por pantalla, correo electrónico, sms, etc



Observaciones sobre las respuestas

- * Aspectos de seguridad
- * Falsas alarmas
- * Almacenamiento de registros



Aspectos de seguridad

* Comunicación oculta

- * Una de las cuestiones que los IDS tienen presente, es la de **no ser reconocidos por atacantes**. Cuando el sistema está siendo comprometido, no conviene que el intruso se percate de que está siendo monitorizado.
- * Por esta razón, se utilizan técnicas que permitan al detector de intrusiones **registrar todo lo sucedido y comunicar las incidencias a los responsables**, todo ello **sin ser interceptado**.
- * En la mayoría de las ocasiones se suele utilizar canales de comunicación **cifrados**.



* Redundancia

- * Otra de las soluciones recomendadas, es el uso de la redundancia en las comunicaciones.
- * Es decir, en **situaciones de alarmas críticas**, conviene utilizar **más de una vía de comunicación** para transmitir la **misma notificación**
- * Se puede enviar por un canal cifrado y otra a través de mensajes de gestión de red, así se **reducen las probabilidades** de que los **mensajes sean bloqueados**



* Protección de registros

- * Una vez comunicadas las alarmas hay que **almacenarlas de forma segura**, protegiéndolas ante **alteraciones o eliminaciones**.
- * Esto es especialmente importante cuando se pretende **utilizar el material obtenido para asuntos legales**.
- * Una de las soluciones practicadas es el almacenamiento de los registros en **medios de una sola escritura**, como un **CD-ROM** o incluso una impresora de **papel** continuo



Falsas alarmas

- * Uno de los problemas asociados a los mecanismos de respuesta de los IDS, es el de las falsas alarmas, son de 2 tipos:
 - * **Falsos positivos** → posibles intrusiones cuando en realidad no los hay
 - * **Falsos negativos** → no notifican intrusiones cuando realmente han tenido lugar



Almacenamiento de registros

- * Casi todos los IDS tienen **métodos especiales** para conservar los **registros generados** a través de sus mecanismos de **respuesta pasiva**
- * Buena parte de ellos contempla la posibilidad de almacenarlos en **BBDD**, esto **simplifica** en gran medida su **análisis** posterior.
- * Además permite a los responsables de seguridad entregar **informes detallados** de la actividad del sistema a los encargados de la gestión ejecutiva



Adopción de políticas de respuesta

- * La correcta **gestión de la seguridad de una organización** conlleva el **cumplimiento** de una serie de **procedimientos**, que definan las **acciones** a tomar en caso de **problemas**.
- * Las actividades contempladas por las políticas de seguridad en caso de intrusiones o violaciones de seguridad, están divididas en 4 categorías:
 - * **Intermedia o crítica**
 - * **Oportuna**
 - * **Largo plazo local**
 - * **Largo plazo global**





* **Intermedia o crítica**

- * Alguna de las acciones a realizar justo después de percibir un ataque o intrusión:
 - * Procedimientos de manejo de incidencias
 - * Contención de los daños
 - * Notificación a la autoridades legales y otras organizaciones
 - * Restaurar el servicio en los sistemas afectados



* Oportuna

- * El tiempo en que se lleva a cabo puede variar entre unas horas y varios días, dependiendo de la organización y el grado de importancia
 - * Investigar manualmente patrones inusuales del sistema
 - * Investigar y aislar las causas del problema
 - * Corregir estos problemas cuando sea posible, aplicando parches o corrigiendo la configuración del sistema
 - * Notificar los detalles del incidente a los responsables adecuados
 - * Mejorar las firmas o patrones de detección del IDS
 - * Tomar acciones legales contra el intruso



* Largo plazo – local

- * Son menos críticas que las dos anteriores. No obstante, no deben dejar de realizarse, ya que desempeñan un papel imprescindible en la seguridad del sistema. Se llevan a cabo de forma periódica, durante la administración de un sistema
 - * Compilar estadísticas y realizar análisis de las tendencias de uso y comportamiento
 - * Seguir la pista de patrones de forma continua



* Largo plazo – global

- * Estas acciones corresponden a actividades no críticas, pero no deben ser ignoradas. El impacto de estas acciones no está limitado a la organización
- * Algunos aspectos de la seguridad del sistema no pueden ser resueltos de forma local, acudir a otras entidades puede hacer que la organización sea partícipe de una solución más completa:
 - * Notificar a los vendedores de los posibles problemas de seguridad encontrados en sus productos
 - * Acudir a entidades legisladoras y al gobierno para solicitar mejores medidas legales contra violaciones de seguridad de sistemas
 - * Enviar estadísticas sobre incidentes de seguridad a autoridades legales u otras organizaciones que mantengan este tipo de estadísticas