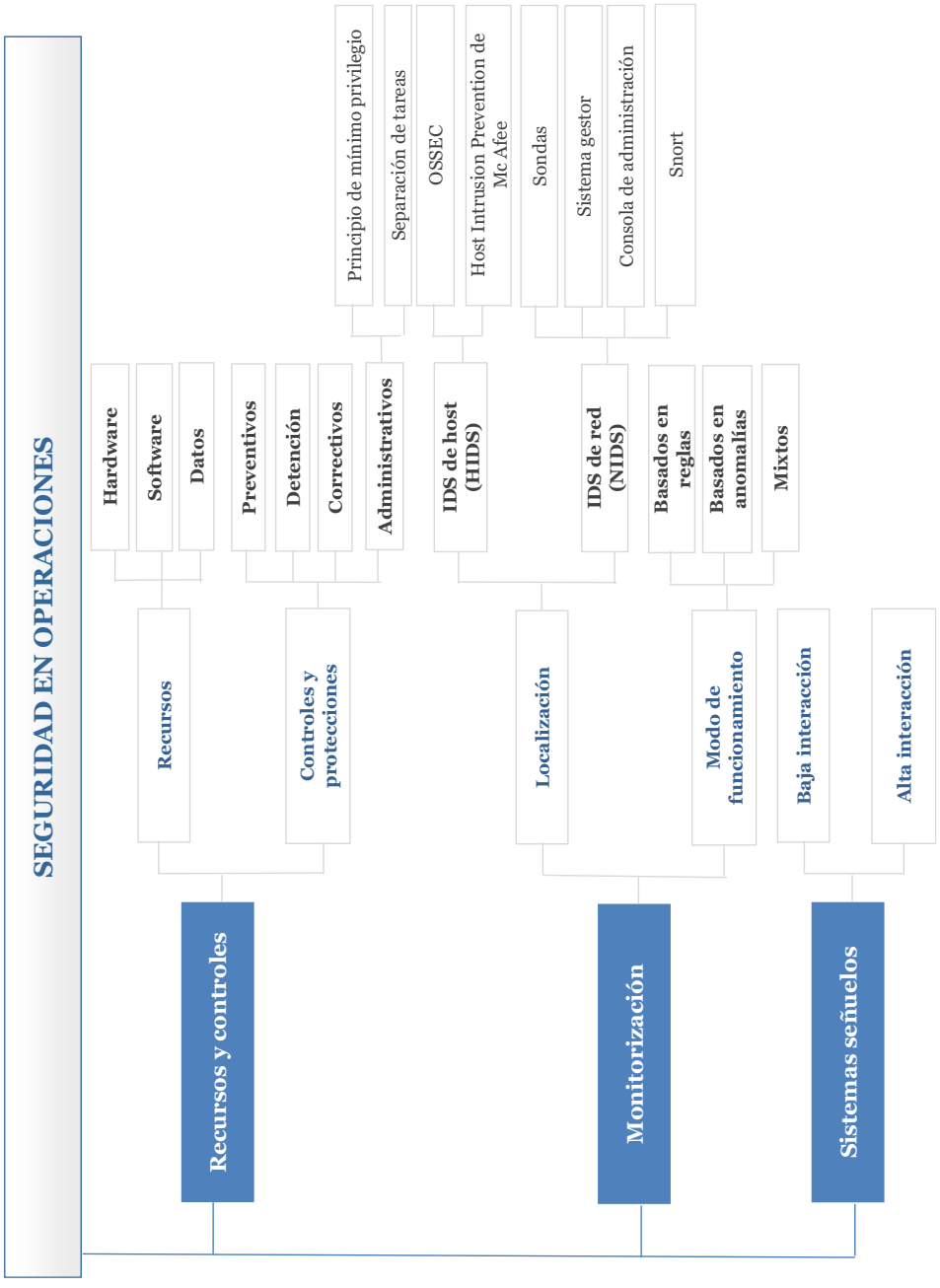
Técnicas de protección de sistemas

TEMA 7

Esquema


SEGURIDAD EN OPERACIONES
Recursos y controles
Monitorización
Sistemas señuelos
Recursos
Controles y protecciones
Localización
Modo de funcionamiento
Baja interacción
Alta interacción
Hardware
Software
Datos
Preventivos
Detención
Correctivos
Administrativos
IDS de host (HIDS)
IDS de red (NIDS)
Basados en reglas
Basados en anomalías
Mixtos
Principio de mínimo privilegio
Separación de tareas
OSSEC
Host Intrusion Prevention de Mc Afee
Sondas
Sistema gestor
Consola de administración
Snort

Ideas clave

7.1. ¿Cómo estudiar este tema?

El estudio de este tema se realiza a través de los contenidos desarrollados en las **Ideas clave** expuestas a continuación.

La ***Seguridad en Operaciones*** dentro de las Tecnologías de la Información hereda la experiencia adquirida en el campo militar y la aplica a la protección de redes, sistemas de ordenadores y aplicaciones informáticas. El objetivo principal de esta práctica es **garantizar que los usuarios, aplicaciones y servidores tienen los privilegios correctos de acceso a los recursos y supervisar su implementación a través de monitorización y auditoría**.

Este tema presentará una introducción a dicho proceso. Para ello, comenzaremos **indentificando los recursos que deben ser protegidos y los privilegios que deben restringirse**. Se discutirán los diferentes mecanismos de control y protección que pueden llevarse a cabo sobre los sistemas de información. A continuación, se hará especial hincapié en las técnicas de monitorización, cuyo principal exponente son los sistemas de detección de intrusos (IDS).

¿Por qué necesitamos un IDS? La visión más práctica que se le puede dar a un profesional del sector es que los cortafuegos no son infalibles, que confiar únicamente en un cortafuegos es arriesgado (en el mejor de los casos), protegen contra ataques que no detectan los cortafuegos, nos protege frente a fallos de otros sistemas de seguridad (no confiar solo en un sistema de seguridad) y proporcionan automatización y facilitan la gestión de la seguridad, así compo avisar al gestor de alarmas.

La mayoría de los softwares de IDS proporcionan un conjunto de reglas que conviertan este sistema de detección de intrusos en un un sistema de prevención, y esto es un IPS. Estas reglas podrán detectar comportamientos anómalos y cortar el acceso como método de prevención.

¿Si aún así nuestro sistema ha sido vulnerado?, aceptémoslo, nuestras reglas del firewall o ACL (Access Control List) no han sido lo suficientemente efectivas. Pero no podemos tirar la toalla, podemos implementar un sistema señuelo o honeypot, que no es más (ni menos) que un host deliberadamente inseguro dentro de nuestra red, para poder atraer a ese visitante no deseado de nuestro sistema. Trataremos de aprender de él lo máximo posible.

7.2. Seguridad en Operaciones

La ***Seguridad en Operaciones*** **(OPSEC)** es un proceso que identifica qué acciones o procesos de un sistema pueden relevar información sobre el mismo a un posible atacante y si la información obtenida por los atacantes puede ser interpretada de un modo útil en contra de los intereses del sistema; para luego establecer las medidas oportunas que eliminen dichas amenazas.

El origen de la seguridad en operaciones es de carácter militar y se remonta a la Guerra de Vietnam. El ejército de los Estados Unidos observó que a pesar de no contar con espías entre sus filas y de aplicar un estricto protocolo de seguridad que restringía el acceso a la información confidencial, el enemigo tenía constancia de las intenciones aliadas antes de que éstas llevasen a cabo sus operaciones militares.

Ante estos hechos, se llegó a la conclusión de que no era suficiente con proteger la información confidencial, sino que, además, debían analizarse las operaciones militares, identificar las acciones que relevaban información sobre las intenciones aliadas al enemigo y tomar las oportunas contramedidas.

Con el tiempo, este proceso se fue perfeccionando y salieron a la luz los indicadores, más allá de los protegidos por los programas de seguridad tradicionales, que relevaban información al enemigo sobre los planes de las tropas aliadas: información no clasificada, eventos, constancia de comunicaciones, indicios de movimientos de tropas, características físicas, etc.

El **proceso OPSEC** se compone de las siguientes **fases**:

1. Identificación de la información crítica La información crítica, también conocida como indicadores, es información sobre las intenciones, capacidades o limitaciones de un sistema que un atacante podría utilizar para conseguir una ventaja militar, política, diplomática, económica o tecnológica.
2. Análisis de Amenazas Identificación de adversarios potenciales y de sus capacidades e intenciones de recolectar, analizar y aprovechar información crítica para favorecer sus intereses.
3. Análisis de Vulnerabilidades Análisis de las operaciones propias para identificar cuáles de ellas representan una vulnerabilidad, esto es; revelan información crítica a un adversario.
4. Evaluación de riesgos Medida del impacto que produciría la obtención y la utilización por parte de un adversario de información crítica.
5. Aplicación de contramedidas En base a las cuatro fases anteriores, se deben establecer contramedidas para las vulnerabilidades que representen un riesgo para el sistema.

7.3. Recursos y Controles

El primer paso que debe llevarse a cabo para analizar la ***Seguridad en Operaciones*** de un sistema es la identificación de los recursos que deben ser protegidos y descripción de los controles que pueden implementarse de cara a restringir los privilegios de acceso a estos recursos.

Recursos

A continuación se enumeran los **recursos** que componen un sistema dedicado a las tecnologías de la información:

Hardware
– Dispositivos de comunicaciones: routers, switches, módems – Medios de almacenamiento: cintas, CD-ROMs y discos – Sistemas de procesamiento: servidores – Dispositivos personales: PC's de sobremesa, PDAs, teléfonos – Otros dispositivos (impresoras, etc.)
Software
– Código fuente y librerías de las aplicaciones desarrolladas – Software utilizado, tanto comercial como de desarrollo propio – Aplicaciones de seguridad: cortafuegos, sistemas de detección de intrusos (IDS), dispositivos biométricos, infraestructura de clave pública (PKI) – Sistemas operativos y utilidades del sistema
Datos
– Directorios del sistema operativo – Archivos de contraseñas – Archivos de usuario – Backups – Registro del sistema (logs) y rastros de auditoría – Documentación

Controles y Protecciones

Los **controles** y las **protecciones** son los métodos utilizados para prevenir que los usuarios hagan uso de más privilegios de los que le han sido asignados. Los controles pueden clasificarse en base a **varios criterios**.

Desde un **punto de vista temporal**, podemos clasificarlos en:

- **Controles Preventivos:** su objetivo es la reducción de la cantidad y el impacto de los errores no intencionados que se producen en el sistema y prevenir el acceso de intrusos al mismo.
- **Controles de Detención:** se utilizan para la detención de errores una vez que estos se han producido.
- **Controles Correctivos:** ayudan a reducir el impacto producido por la ocurrencia de un error en el sistema a través de procesos de recuperación.

Nos centraremos en este punto, sin embargo, en una clasificación **basada en la naturaleza de los controles**; diferenciándose los siguientes:

- **Controles Administrativos**
- **Controles Hardware**
- **Controles Software**
- **Controles de Medios de Almacenamiento**
- **Controles de Acceso Físico**

Controles Administrativos

Los controles administrativos se centran en definir los privilegios que cada usuario tiene sobre los recursos del sistema. Esta definición está basada en el **principio de mínimo privilegio** y la **separación y rotación de tareas del personal**, estando ambos conceptos íntimamente relacionados.

El ***principio de mínimo privilegio*** consiste en dotar a los usuarios del sistema de los mínimos privilegios necesarios para que puedan llevar a cabo su tarea dentro del sistema. Por su parte, **la separación y rotación de tareas** se centra en la división de las responsabilidades de los usuarios, de modo que ningún usuario tengo un control total sobre el sistema, y en la rotación de las mismas, para limitar el tiempo durante el cual un posible usuario malicioso puede corromper los recursos a los que tiene acceso dentro del sistema.

A continuación se detallan las **principales tareas de los controles administrativos**:

- **Definición de los usuarios que tienen acceso físico a los recursos, principalmente los que no son de uso personal:** servidores, dispositivos de red, dispositivos de comunicaciones, bases de datos, cintas de backup, etc.
- **Quién puede hacer uso de los recursos.** Asignación de credenciales a los usuarios que controlen el acceso a los mismos.
- **Definición de los privilegios que tiene cada usuario sobre cada recurso:** simple uso, instalación, configuración, modificación, capacidad de dotar de acceso al recurso a otros usuarios o control total.
- **Definición de los permisos que tiene cada usuario.** Una vez han accedido a los recursos, que operaciones pueden llevar a cabo: lectura, escritura, ejecución.

Controles Hardware

Los **controles hardware** se encargan de proteger los recursos hardware del sistema. Destacan:

- **Mantenimiento de Hardware:** el hardware del sistema debe ser supervisado temporalmente para garantizar su buen estado y su correcto funcionamiento.
- **Cuentas de acceso para mantenimiento:** la mayoría de los sistemas traen habilitadas cuentas de mantenimiento que llevan asignadas contraseñas por defecto. Estas cuentas deben ser deshabilitadas hasta que sea necesario su uso o deben modificarse las contraseñas que permiten hacer uso de ellas.
- **Control de puertos:** algunos dispositivos cuentan con puertos que permiten acceso directo al hardware con propósitos de diagnóstico. Debe controlarse que estos puertos solo pueden ser utilizados por el personal autorizado.
- **Controles físicos:** el acceso físico a los recursos debe controlarse situando los recursos de uso no personal (servidores, dispositivos de red, dispositivos de comunicaciones, bases de datos, cintas de backup, etc.) en salas convenientemente cerradas y mediante la utilización de alarmas.

Controles Software

Su papel es el de **controlar las aplicaciones utilizadas dentro del sistema**. Los **mecanismos de control software** más importantes son los siguientes:

- **Administración de software antivírico:** todas los dispositivos del sistema deben contar con un programa antivirus actualizado que realice inspecciones periódicas de los programas presentes en el mismo y bloquee la posible inserción de virus o gusanos.
- **Comprobación de Software:** tanto las nuevas aplicaciones como las actualizaciones de las utilidades ya instaladas deben pasar un proceso de comprobación antes de su puesta en operación dentro del sistema para evitar cualquier tipo de error, como posibles incompatibilidades, con el software ya presente.
- **Utilidades de Administración:** en todos los sistemas existen programas dedicados a fines administrativos y cuyo uso malicioso puede comprometer la integridad de los mismos. Es por ello que el acceso a estos comandos privilegiados debe estar restringido a los operadores y administradores del sistema.

- **Almacenamiento seguro:** debe evitarse la modificación no autorizada del software y de las copias de seguridad del sistema mediante la combinación de controles de acceso lógico y físico.
- **Controles de Backup:** periódicamente deben llevarse a cabo copias de seguridad de los datos personales de los usuarios y del sistema. Estas copias deben estar almacenadas de un modo seguro y además, debe comprarse su validez de cara a una posible restauración.

Controles de Medios de Almacenamiento

Los **controles sobre los medios de almacenamiento** pueden dividirse en dos áreas: **controles de seguridad** y **controles de viabilidad**.

Los **controles de seguridad** previenen la pérdida o exposición de información sensible a agentes no autorizados. Destacan tres mecanismos:

- Registro del uso de los medios por parte de los usuarios (Logging).
- Control de acceso físico a los medios.
- Destrucción apropiada de los medios de almacenamiento.

Por su parte, los **controles de viabilidad** pretenden proteger los medios de almacenamiento durante su uso, almacenaje y transporte. Los métodos utilizados son los siguientes:

- Etiquetado de los medios para su fácil identificación.
- Trato adecuado de los medios durante su transporte y utilización.
- Almacenamiento de los medios en condiciones ambientales que eviten su degradación.

Controles de Acceso Físico

Una parte muy importante de la seguridad en operaciones es el **control del acceso físico a los recursos**, tanto hardware como software. Debe prestarse especial atención al personal que debe tener contacto físico con los mismos para poder desempeñar su trabajo diario, como por ejemplo:

- Personal técnico de la empresa.
- Servicio de limpieza.

- Técnicos del sistema de ventilación y aire acondicionado.

7.4. Monitorización

El **objetivo** principal de la monitorización y auditoría es la **identificación y la resolución de problemas**.

La monitorización comprende los mecanismos, utilidades y técnicas que permiten la identificación de eventos de seguridad cuyo impacto puede perturbar el correcto funcionamiento de un sistema, informando al administrador del sistema sobre los hechos acaecidos.

Su necesidad surge, como hemos ido viendo a lo largo de la asignatura, de que el panorama de la seguridad informática ha cambiado enormemente en los últimos años. Una de las consecuencias más visibles ha sido el **incremento en el número de incidentes de seguridad**, número que no para de crecer.

En esta nueva situación se hace imprescindible contar con sistemas de protección más avanzados que un simple cortafuegos. Estos, que han demostrado su innegable utilidad durante muchos años, carecen de habilidades para proteger por ejemplo, aplicaciones Web.

Estos nuevos sistemas de protección se conocen con el nombre de **sistemas de detección de intrusión**, cuyo objetivo básico es detectar posibles ataques a nuestros sistemas y alertar sobre ellos.

Situación actual

Las razones que justifican este aumento en el número de ataques son muy diversas, y no existe un consenso unánime en ellas. Pero una de las más importantes es, sin duda, una que ya hemos analizado en otros temas y que está relacionada con la **profesionalización de los responsables**.

Atrás quedaron los tiempos en los que los verdaderos *hackers* atacaban sistemas con el mero propósito de demostrar sus habilidades. De unos años a esta parte, los atacantes se han dado cuenta de que pueden ganar mucho dinero con estas actividades y se han convertido en verdaderos delincuentes, ayudados sin duda, por la entrada en escena de mafias organizadas.

Para las mafias, Internet es un lugar ideal para «ampliar» sus negocios tradicionales y ofrece estupendas posibilidades para el blanqueo de dinero, por ejemplo. Para entrar en este nuevo mundo con buen pie, las mafias reclutan a *hackers* expertos (sobre todo jóvenes de Europa del Este y del sudeste asiático) para montar para ellos ataques de *phishing* o escribir troyanos bancarios específicos. Hasta tal punto ha llegado la organización del negocio, que pueden encontrarse fácilmente kits de *phishing*, con todas las funcionalidades necesarias, al módico precio de 600€.

Y todo esto es posible debido a que la inmensa mayoría de sistemas (sistemas operativos, aplicaciones, elementos de red) sufren vulnerabilidades. De hecho, algunos expertos, como el influyente Steve Bellovin, creen que los sistemas de computación nunca serán absolutamente seguros. Sirvan algunos datos, como el tiempo medio que un sistema vulnerable expuesto en Internet tardará en ser comprometido:

***Windows* vulnerable**	Menos de 3 horas
***Linux* vulnerable**	Aproximadamente 3 meses

Dejando al margen el debate sobre qué sistema operativo es más seguro (debate que, otra parte, parece algo artificial: cualquier SO puede ser perfectamente seguro si se administra correctamente), lo cierto es que todos sufren el problema de la necesidad de la aplicación periódica de parches.

7.5. Sistemas de detección de intrusión

Historia

El concepto de detección de intrusión fue introducido en el artículo que James Anderson escribió en 1980 para el NIST, llamado *Computer Security Threat Monitoring and Surveillance*, donde se mencionaron por primera vez los conceptos de detección de mal uso y eventos específicos provocados por los usuarios.

Ya en 1983, Dorothy Denning, comenzó a trabajar en un proyecto del gobierno norteamericano que pretendía desarrollar un sistema de detección de intrusión. Su objetivo era analizar registros de actividad provenientes de grandes *mainframes* de la administración y crear perfiles de usuarios en base a sus comportamientos. Un año después, el primer modelo para detección de intrusión, basado en el uso de sistemas expertos, estaba listo.

Pero no sería hasta 1990 cuando aparecieron los IDS de red, introducidos por Todd Heberlein de la Universidad de California con su *Network Security Monitor* (NSM). Estos sistemas provocaron un interés renovado en el campo de la detección de intrusión y consiguió que las inversiones en ese mercado aumentaran significativamente. Tanto que los primeros sistemas comerciales no tardarían en llegar, en 1997, con el primer IDS comercial de la compañía ISS, denominado *RealSecure*.

El campo creció de forma tan espectacular en tan poco tiempo que, para el año 2000, todas las grandes compañías de seguridad tenían una solución IDS. El siguiente gráfico ilustra los hitos más importantes en el desarrollo de esta tecnología:

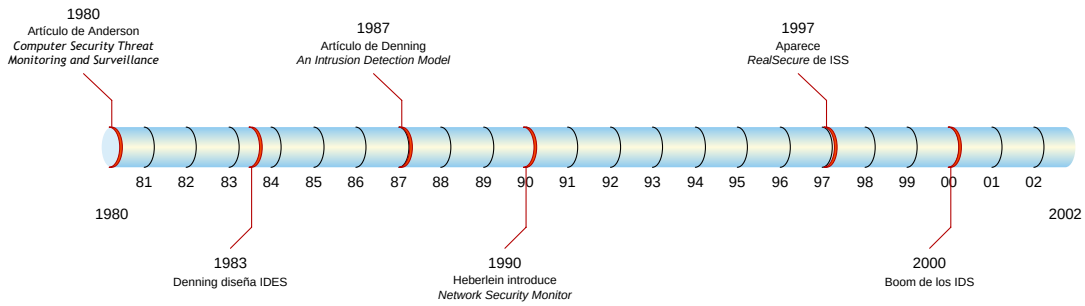


Figura 1. Evolución histórica de los sistemas IDS

Definiciones

Hasta ahora no nos hemos preguntado qué se entiende exactamente por una **intrusión**. Consideramos una intrusión como «la secuencia de acciones realizadas por un atacante que resulta en el compromiso de un sistema». Por tanto, la **detección de intrusión** es el proceso de identificación y respuesta a intentos de ataques. Como proceso que es, involucra *tecnología*, *personas* y *herramientas*.

En otras palabras, un sistema de detección de intrusión son los ojos de nuestra arquitectura de seguridad, que nos permite saber qué esta pasando, dentro y fuera de nuestras redes. Su funcionamiento es sencillo: el IDS monitoriza continuamente una serie de parámetros y características de los sistemas vigilados. Cuando se detecta un intento de ataque se genera una **alerta**, que debería ser revisada de inmediato por un operador humano.

Estas alertas pueden clasificarse en **dos grandes categorías**:

- **Falso positivo:** se produce cuando un IDS genera una alerta falsa sobre un ataque que no se ha producido. La elevada tasa de falsos positivos es uno de los grandes inconvenientes de los IDS.
- **Falso negativo:** se produce cuando un IDS no detecta un ataque y no genera la alerta correspondiente. Es un muy peligroso, porque un único falso negativo puede provocar que una intrusión no sea detectada.

Clasificación

Los **sistemas de detección de intrusión** pueden clasificarse en cuatro grandes tipos agrupados, a su vez, en **dos categorías**, **según su localización y modo de funcionamiento**.

Según el primer criterio, **su localización**, los sistemas IDS pueden catalogarse en:

- **IDS de *host*:** funcionan a nivel de máquina, monitorizando parámetros del sistema operativo y de algunas aplicaciones.
- **IDS de red:** se sitúan en la red, capturando y monitorizando su tráfico.

Y utilizando el segundo, su **modo de funcionamiento**, encontramos:

- **IDS basado en reglas:** buscan patrones, tanto en el tráfico como el comportamiento del usuario, para identificar los posibles ataques.
- **IDS basado en anomalías:** generan un modelo del «comportamiento normal» del sistema y buscan desviaciones del mismo.

Esta clasificación puede observarse gráficamente en el siguiente esquema:

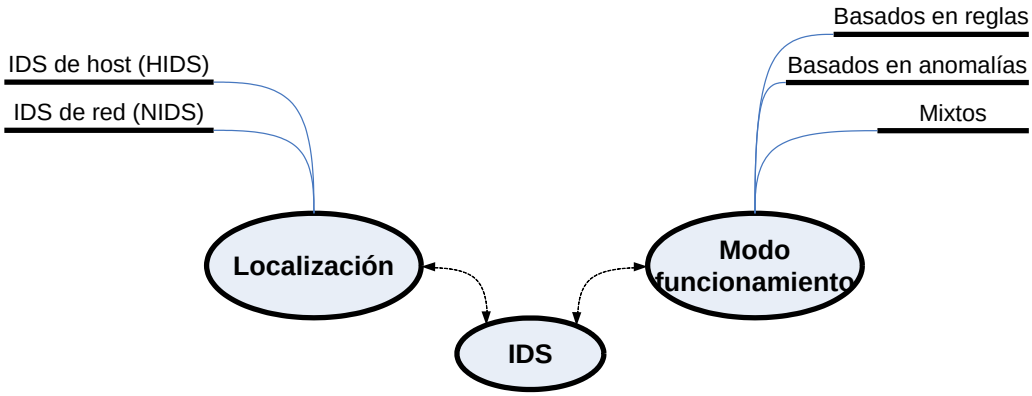


Figura 2. Tipos de IDS

Es los siguiente apartados analizaremos en detalle cada uno de estos **tipos de IDS**.

7.6. IDS de *host*

Este tipo de IDS se instala, en **forma de un *agente***, en cada máquina que debe vigilada y monitorizan, detectan y responden a la actividad del usuario y del sistema, examinando parámetros del sistema operativo y del comportamiento del usuario como:

- **Uso de CPU y memoria.**
- **Monitorización de *logs*.**
- **Intentos fallidos de *login*.**
- **Monitorización del sistema de ficheros.**

Por su modo de funcionamiento, los IDS de *host* (HIDS) son más adecuados para combatir las amenazas internas, como las provenientes de desempleados deshonestos que, de hecho, constituye la fuente de ataques más numerosa y peligrosa.

Otra ventaja de los HIDS es que son mucho más baratos que el resto de tipos de IDS. A grandes rasgos, podemos encontrar licencias de HIDS por unos 50€ por máquina, mientras que un IDS de red puede alcanzar sin problemas los 8.000€. Por supuesto hay que tener en cuenta el número total de máquinas donde hay que instalar el agente del HIDS. Por último, existen ataques difíciles de detectar para un NIDS y que, por el contrario, pueden ser fácilmente capturados por un HIDS.

Por supuesto, estos esquemas también tienen una serie de inconvenientes. La primera de ella es que suponen una solución que puede ser costosa de administrar en determinados entornos. Por ejemplo, la política de detección debe ajustarse para evitar una alta tasa de falsos positivos, lo que puede suponer un problema en grandes organizaciones, con sistemas muy heterogéneos y un alto número de máquinas. Por otro lado, los HIDS utilizan recursos del sistema, como CPU y memoria RAM.

Despliegue de un HIDS

Uno de los aspectos más importantes a considerar en el despliegue y puesta en marcha de un IDS en general y de un HIDS en particular, es el lugar donde ubicar los agentes. Claramente, lo ideal sería situar uno de ellos en cada máquina de la organización, pero existen una serie de problemas con esa solución:

- Los costes podrían llegar a ser prohibitivos en una organización de tamaño medio/alto (con una estimación de 50-500€ por máquina).
- La tasa de falsos positivos puede ser muy alta en máquinas que se reconfiguran frecuentemente.

En cualquier caso, a pesar de estos problemas, los agentes deberían ser instalados, al menos, en las siguientes máquinas de la infraestructura de una organización típica:

- Servidores de «negocio» (perimetrales e internos).
- Cortafuegos.
- Servidores Web, DNS y de correo.

Ejemplos de HIDS

A continuación, veremos algunos **ejemplos de HIDS comerciales y libres**. Los primeros se enfocan básicamente en plataformas *Windows* y los segundos en *UNIX*, pero hay algunas excepciones. Una lista básica podría ser la siguiente:

- Soluciones sencillas (y baratas) para *UNIX*:
  - *OSSEC*
  - *TCPWrappers*
  - *Syslog*
  - *Swatch*
  - *Tripwire*

- Soluciones comerciales para *Windows*:
  - *OSSEC*
  - *BlackICE* de ISS
  - *Host Intrusion Prevention* de McAfee
  - *Sentinel* de Enterasys

7.7. IDS de red

Los **IDS** de red, a diferencia de los HIDS, funcionan **capturando y analizando todo el tráfico de un segmento de red**, **en busca de actividad maliciosa**.

Una ventaja clara de esta aproximación es que el número necesario de **sondas**, el elemento que captura y analiza el tráfico, es mucho menor que el de agentes. Sin embargo, los NIDS tradicionales han tenido problemas para trabajar en:

- Entornos conmutados.
- Entornos con comunicaciones cifradas.
- Redes de alta velocidad (redes Gigabit o de más de 100 Mbps). Aunque desde hace poco tiempo, existen ya algunos IDS capaces de trabajar en redes a estas velocidades.

Estructura de un NIDS

Un IDS de red se compone de, básicamente, los siguientes elementos:

- **Sondas:** elementos recolectores del sistema. Capturan el tráfico y realizan un primer paso de procesado. Después, envían los eventos o alertas generados al sistema gestor.

- **Sistema gestor:** encargado de almacenar y gestionar los eventos recibidos. Se compone, a su vez, de:
  - Base de datos, donde se almacenan los eventos.
  - Sistema de correlación de eventos (opcional).

- **Consola de administración:** clasifica y muestra los eventos recibidos. Normalmente esta consola cuenta con un interfaz gráfico (GUI), que permite gestionar los eventos, viendo sus detalles, archivarlos, descartarlos, etc…

Esquemáticamente, la estructura puede ser similar a la siguiente:

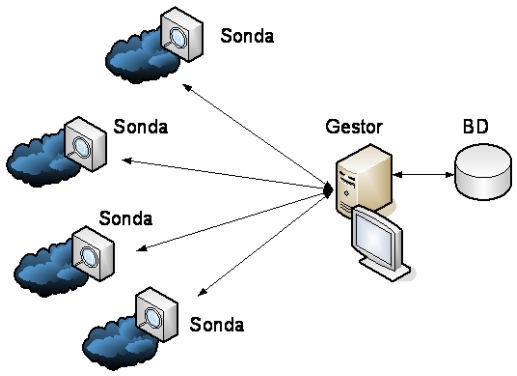


Figura 3. Estructura típica de un NIDS

Implantación de un NIDS

La **implantación de un NIDS** es un proceso complejo y delicado que implica, entre otros, los siguientes pasos:

1. Elección del producto más adecuado (comercial o libre).
2. Elección del tipo de sondas, que analizaremos en el siguiente punto.
3. Elección del número y ubicación de las mismas.
4. Ajuste de la política de cada sonda, para reducir el número de falsos positivos.

Un error en cualquiera de estos pasos puede resultar muy caro, en todos los sentidos y no solo en el económico, también en el tiempo que habría que utilizar en revertir los cambios de una mala elección.

Tipos de sondas

Las sondas, o elementos recolectores, pueden implantarse en distintas plataformas, de más especializadas a menos:

- ***Hardware dedicado:*** muchos IDS comerciales utilizan esta fórmula.
  - **Ventajas:** en teoría, pueden alcanzar mayores tasas de captura.
  - **Inconvenientes:** son cajas negras, de las que se desconoce su funcionamiento. En general, son mucho más caras.

- ***Un simple PC:*** con sus tarjetas de red en modo promiscuo.
  - **Ventajas:** reduce costes y facilita el mantenimiento.
  - **Inconvenientes:** en teoría, podrían ser menos fiables.

En principio, no existe ninguna ventaja definitiva de un enfoque sobre el otro. Las razones para decidirse por uno u otro suelen más de tipo económico: muchos IDS comerciales sólo se venden en forma de hardware dedicado, de forma que no es posible utilizar PC's baratos. Por el contrario, todos los IDS libres (como Snort) permiten su instalación en estas plataformas, lo que añadido a que no tienen ningún tipo de licencia por uso, abarata enormemente sus costes.

Ubicación de las sondas

Otro gran problema que hay que resolver como parte del proceso de implantación de una infraestructura de detección de intrusión es **decidir el número y ubicación de cada sonda**. Esta es una decisión muy importante, pues determina qué tráfico podrá monitorizarse y cuál no.

En principio, en entornos conmutados sería necesaria una sonda por cada segmento de red. Esto puede disparar los costes, así que para agregar el tráfico y poder utilizar una única sonda para enlizar tráfico de varios segmentos existen **dos soluciones básicas**:

Veamos cada una de estas alternativas con detalle.

1. Puertos de spanning

Hoy en día, casi cualquier switch tienen un puerto de *span* (o de agregación), por el que se recibe todo el tráfico que pasa por el mismo. De esta forma, si se conecta la sonda a ese puerto, ésta es capaz de capturar y analizar todo el tráfico.

Sin embargo, existen algunos **problemas** achacables a este enfoque:

- Si el tráfico es muy alto, el switch puede tener problemas de rendimiento y empezar a descartar paquetes.
- Algunos switches sólo permiten un puerto de span por VLAN, lo que puede dificultar la captura en entornos en los que existen múltiples VLAN's, lo que es muy común.

La gran ventaja de esta solución radica, claramente, en que es la más barata, ya que no necesita, en principio, la compra de ningún hardware adicional ni el rediseño o reconfiguración de la estructura existente de la red.

2. TAPs

La siguiente solución posible es el uso de *taps*. Un **tap** es un **dispositivo hardware** que **se coloca en mitad de un cable de datos** y **envía una copia del tráfico que pasa a través de él a uno o más puntos**.

Su gran ventaja es que, a diferencia de los puertos de span, no tienen problemas de rendimiento, siendo capaces de gestionar cualquier tasa de tráfico. Por esta misma razón, se debe elegir su ubicación con cuidado, pues pueden sobrecargar fácilmente las sondas, enviándoles más tráfico del que éstas pueden gestionar. Tampoco necesitan configuración, más allá de su introducción física en la red.

La siguiente figura muestra el aspecto de un TAP comercial para una red Ethernet de hasta 100Mbps:

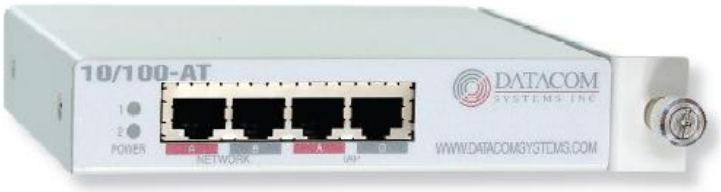


Figura 4. TAP comercial.

Capacidad de proceso de las sondas

Otro aspecto importante a tener en cuenta es que **las sondas tienen una capacidad de procesamiento limitada**. La cantidad exacta depende del tipo de sonda (hardware dedicado o no, recursos de memoria RAM y CPU, etc…), pero un cifra estimativa puede ser alrededor de unos 80 Mbps a plena carga.

Esto obliga a repartir el tráfico entre las distintas sondas en base a **varios criterios**:

- La carga de la red determinará el número mínimo de sondas. Es decir, si los picos de nuestra red en horas punta pueden llegar a los 100 Mbps, necesitaremos, como mínimo, dos sondas.
- Distintas zonas de la red tendrán distintos tipos de tráfico, de forma que no debe utilizarse una única sonda para todos ellos, pues esto impediría poder ajustar las políticas de cada sonda de forma individual.

7.8. IDS basados en firmas

La otra gran categoría de IDS utiliza el modo de funcionamiento para llevar a cabo la clasificación. Según este criterio, los IDS basados en firmas funcionan buscando patrones previamente definidos en aquellos parámetros que monitorizan, como el tráfico de red para los NIDS o el sistema de ficheros, por ejemplo, para los HIDS.

Como ya hemos visto, cuando se detecta una concordancia, se dispara la regla y se genera una alerta. Esta alerta se envía a una consola central, donde un operador humano debería analizarla y actuar en consecuencia.

Para un HIDS una firma podría ser algo como:

```
IF número_intentos_login_último_minuto >= 10
        AND mismo_usuario THEN ALERT
("Ataque de fuerza bruta contra cuenta de usuario")
```

Por otro lado, para un NIDS:

```
IF misma_dir_IP_origen AND diferentes_puerto_destino
AND num_conexiones >= 10 THEN ALERT
("Escaneo de puertos")
```

Aunque, como suele ocurrir, en el mundo real las firmas no son tan sencillas. Por ejemplo, esta es una firma de Snort para detectar un tipo de ataque concreto contra dispositivos Cisco:

```
alert tcp any any -> $HOME_NET 23 (msg: "BLEEDING-EDGE EXPLOIT Cisco Telnet Buffer Overflow"; flow: to_server, established; content:"|3f 3f 3f 3f 3f 3f 3f 3f 3f 3f 3f 3f 3f 3f 3f 3f 61 7e 20 25 25 25 25 25 58 58|"; threshold: type limit, track by_src, count 1, seconds 120; reference: url,www.cisco.com/warp/public/707/cisco-sn-20040326-exploits.shtml; classtype: attempted-dos; sid: 2000005; rev:4; )
```

Implantación

Todos los IDS basados en firmas necesitan de una configuración inicial cuidadosa. Esta configuración consiste, principalmente, en el **refinado de la base de reglas**, **necesario para adaptar el conjunto de reglas por defecto del IDS al tipo de tráfico más habitual de la red que se pretende monitorizar**.

Si no se lleva a cabo este paso, tendremos un sistema prácticamente inservible, que generará multitud de falsos positivos, lo que provocaría un efecto «que viene el lobo». Es decir, ante la avalancha de falsos positivos, los operadores pronto dejarían de prestar la atención debida, lo que facilitaría mucho que un ataque real se perdiera entre la gran cantidad de alertas.

Este refinado se basa en el hecho de que cuanto más general sea una regla, más posibilidades tendrá de detectar un ataque en particular. Aunque también, más posibilidades de que cualquier otro paquete, que no tenga nada que ver, concuerde con sus criterios y provoque un falso positivo.

Por otro lado, si hacemos la regla demasiado específica, podemos generar un falso negativo, al no comprobar alguna característica importante del tráfico malicioso. Se trata, por tanto, de encontrar un equilibrio entre ambos criterios, que adapten la base reglas a nuestro tráfico sin provocar nunca falsos negativos.

Un ejemplo real: Snort

Vamos ahora a analizar un ejemplo real de IDS ampliamente utilizado, **Snort**. Se trata, sin duda, del **mejor IDS libre y uno de los mejores de todo el mercado**, que tiene poco que envidiar a sus contrapartidas comerciales. Donde no puede competir con ellos es en su interfaz gráfica, capacidad de generar informes o alertas, donde claramente en muy inferior.

Por lo demás, se trata de un IDS muy extendido, fiable y con una extensísima documentación. Ha sido desarrollado y utilizado por la comunidad de software libre, muy activa, lo que proporciona bases de reglas exactas y rápidamente actualizadas.

Otra ventaja importante es que la base de reglas se almacena en ficheros de texto plano, lo que proporciona un control total sobre los mismos. Este aspecto, que puede parecer muy obvio, no lo es tanto: muchos IDS comerciales son «cajas negras». Es decir, no se conoce ni se tiene control sobre su base de reglas y, por tanto, no se puede reducir la tasa de falsos positivos manualmente.

Ventajas e inconvenientes de los IDS basados en firmas

Las **ventajas** principales de este tipo de IDS que **son conceptualmente sencillos y flexibles**. Esto último permite escribir nuevas firmas rápidamente cuando se descubren nuevos ataques. Esta opción, como hemos visto, no está disponible en muchos IDS comerciales, con los que se debe esperar a que el fabricante genere y distribuya la firma correspondiente a la nueva amenaza.

En cuanto a los **inconvenientes**, sin duda el más importante es que este tipo de IDS **no detecta nuevos ataques que no hayan sido definidos previamente en su base de reglas**. Por tanto, necesitan de un continuo ajuste de la misma que, si no se realiza con regularidad, provoca que:

- La tasa de falsos positivos se incremente con el tiempo.

- El sistema pierda toda su eficacia, pues se vuelve incapaz de detectar las amenazas más recientes que son, claramente, las que más se utilizan por los atacantes y, por tanto, las más peligrosas.

IDS basados en anomalías

Por último, la otra gran categoría de IDS son los basados en anomalías. Estos funcionan generando un modelo del comportamiento «normal» o habitual del sistema o del usuario. Después, monitoriza la actividad del sistema o de la red, clasificándola como **normal** o **anómala** según el siguiente criterio: todo lo que no sea normal, es anómalo. El punto clave es que esta clasificación se lleva a cabo utilizando **heurísticas**, en vez de patrones o firmas.

Hasta el momento para generar estas heurísticas se han utilizado todo tipo de **técnicas de inteligencia artificial**, como:

- Redes neuronales.
- Sistemas clasificadores difusos.
- Mapas autoorganizados o de Kohonen.

La realidad es que este tipo de IDS no han funcionado hasta el momento como se espera de ellos, a pesar de todos los esfuerzos realizados, motivados por su gran ventaja: que podrían detectar un tipo de ataque desconocido (siempre que sea suficientemente «anómalo»).

Así pues, **los IDS basados en anomalías son la eterna promesa del campo de la detección de intrusión**, porque:

- Reducirían la tasa de falsos positivos.
- Detectarían ataques desconocidos.

Pero lo cierto es que después de cientos de artículos en la literatura sobre el tema, el campo de investigación, totalmente abierto, sigue casi en el mismo punto.

7.9. Sistemas señuelos

"¿Cómo podemos defendernos de un atacante, cuando no sabemos quién es ni cómo actúa?"

Para responder a esta pregunta se introdujo el concepto de **sistema señuelo**, o ***honeypot***, que en pocas palabras es, una trampa:

- *A nivel de máquina:* corren servicios reales en una máquina «sacrificada» o se simulan estos servicios en un entorno controlado.
- *A nivel de red:* se simulan máquinas y redes completas, servidores que no existen para hacer creer a un atacante que ha encontrado una organización vulnerable.

Los **honeypots** pretenden, por tanto, **aprender de los atacantes**. Por ejemplo, imaginad esta situación:

- Un grupo hacker ha descubierto una nueva vulnerabilidad en el servicio IMAP, que corre en el puerto 143 TCP.
- El cortafuegos de cualquier organización debería detener las conexiones entrantes a ese puerto.
- Pero entonces, el ataque no podrá ser llevado a cabo y no tendremos ningún detalle sobre el mismo.
- Si colocamos un *honeypot* en la red, podremos obtener información sobre qué están tratando de hacer los atacantes.

Tipos de honeypots

Los tipos de honeypots **se clasifican en función de lo real que sea la simulación que llevan a cabo**. De esta forma, se agrupa en honeypots de:

	Baja interacción		Alta interacción
Ventajas	- Simulan servicios, aplicaciones y sistemas operativos - Suponen un riesgo bajo y son fáciles de implantar y mantener	Ventajas	- Servicios, aplicaciones y SO's reales - Capturan mucha información
Inconvenientes	- Son fácilmente detectables por atacantes con experiencia - Capturan una cantidad de información limitada	Inconvenientes	- Suponen un alto riesgo (pueden ser utilizadas como plataformas para nuevos ataques) y son difíciles de mantener

Implantación

Se establece una red muy controlada, donde cada paquete que entra o sale es monitorizado, capturado y analizado. Existen, por ejemplo, buenas herramientas libres para esta tarea, como:

Sebek → Para sistemas de alta interacción

Honeyd → Para sistemas de baja interacción

Por otro lado, los *honeypots* son una tecnología relativamente compleja y no son adecuados si no se tiene interés real en mantenerlos en buenas condiciones. Esto implica:

- **Estudiar la información recolectada:** este puede ser un paso que necesite de mucho tiempo y esfuerzos.
- **Compartir los análisis con la comunidad de seguridad:** solo de esta forma se puede avisar de forma temprana de nuevas amenazas.

¡Cuidado! Un *honeypot* descuidado es la mejor forma de tener problemas, ya que con seguridad, será utilizado como plataforma para otros ataques.

Lo + recomendado

No dejes de leer…

Honeypots: Tracking Hackers

Un honeypots se usa para observar y aprender sobre los *hackers*. El interés práctico y comercial en estas nuevas formas de defensa de *hackers* se hace imprescindible.

Accede al documento a través del aula virtual o desde la siguiente dirección web:
http://www.diva-portal.org/smash/get/diva2:327476/fulltext01

Instalación y configuración de Snort

En la página Web indicada más abajo, podrás encontrar un entretenido documento en el quese resumen los pasos más importantes para la instalación, configuración y primesos pasos de puesta en marcha de *Snort*, así como un pequeño tutorial sobre cómo escribir reglas para el mismo.

Accede al documento a través del aula virtual o desde la siguiente dirección web:
https://seguridadinformaticaufps.wikispaces.com/file/view/1150214.pdf

No dejes de ver...

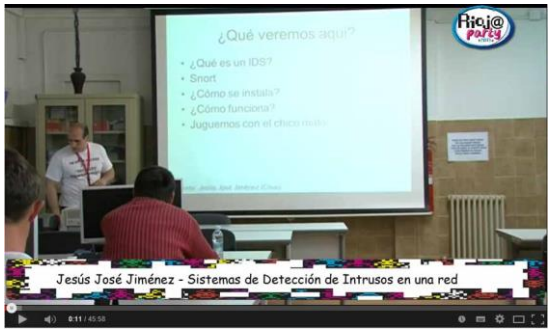
IDS/IPS con KALI LINUX

En este vídeo se explicá cómo instalar y configurar un sistema de detección y prevención de intrusiones.

Accede al vídeo a través del aula virtual o desde la siguiente dirección web:
https://www.youtube.com/watch?v=rzbIX5sYcVQ

CPEU1 - AlienVault. Fuente de seguridad abierta

Hasta ahora en la asignatura hemos visto multitud de herramientas, como *sistemas de detección de intrusión*, *sniffers de red*, *honeypots* y muchos otros. Cada uno genera su alerta, por lo que han surgido elementos que unifican estas alertas y las muestran en un único lugar. En esta presentación de la Campus Party (2010) se introducen este tipo de sistemas, denominados sistemas de correlación de eventos.



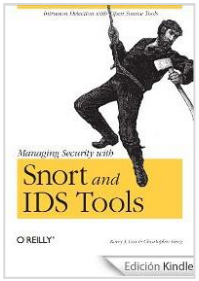
Accede al vídeo a través del aula virtual o desde la siguiente dirección web:
https://www.youtube.com/watch?v=WC4fg1lDjIg

+ Información

A fondo

Managing Security with Snort & IDS Tools

Cox, K.J. & O'Reilly, C.G. (2004). *Managing Security with Snort & IDS. Tools*. Paperback. ISBN-13: 978-0596006617. ASIN: B0043EWV0Q.



Este libro describe la que es, sin duda, la más conocida herramienta IDS, *Snort*. Es un libro realmente bien escrito, con multitud de ejemplos prácticos, por lo que resulta muy útil para comenzar desde cero en el área. Se muestran además, otras herramientas auxiliares, por lo que el objetivo del libro es montar un kit completo de detección de intrusión.

Enlaces relacionados

El proyecto *Honeynet*

Este proyecto es una interesante iniciativa que aglutina buena parte del conocimiento existente alrededor de los honeypots. En su página Web podrás encontrar todo tipo de información, pero no te pierdas el siguiente enlace, en el que se recoge una serie de estadísticas sobre los ataques más frecuentes en el año en curso.

Accede a la web a través del aula virtual o desde la siguiente dirección:
https://www.honeynet.org/node/1183

Bibliografía

Kruegel, C.; Valeur, F. & Vigna, G. (2005) *Intrusion Detection and Correlation: Challenges and Solutions*. Springer. ISBN: 0-387-23398-9.

Test

1. Existen dos grandes controles administrativos, que son básicos, además, en seguridad informática. ¿Puedes identificarlos?

A. Sistemas de detección de intrusión y sistemas señuelos
B. Registros del sistema y *logs*
C. Principio de mínimo privilegio y separación y rotación de tareas del personal
D. Documentación y etiquetado de los medios de almacenamiento

2. Verificar el currículum vitae de un posible empleado de una empresa, para comprobar, por ejemplo, que no tiene antecedentes penales si va a tratar con información confidencial, sería una medida de control:

A. Preventiva
B. Detección
C. Correctiva
D. Administrativa

3. Un componente esencial de un sistema de detección de intrusión son las alertas. En ocasiones, se producen fallos, denominados falsos positivos y negativos. ¿En qué consiste cada uno de ellos, FP y FN, respectivamente?

A. FP: alerta que se dispara que no se corresponde a un ataque real, FN: la alerta no se dispara ante un ataque real
B. FP: la alerta no se dispara ante un ataque real, FN: alerta que se dispara que no se corresponde a un ataque real
C. FP: alerta que se dispara pero corresponde a un ataque real, FN: la alerta no se dispara ante un ataque real
D. FP: alerta que se dispara que no se corresponde a un ataque real, FN: la alerta se dispara pero el ataque no es real

4. Tienes cuatro servidores en tu red, ¿Cuántas sondas instalarías?

A. Uno en cada servidor
B. Uno, en un único servidor
C. Uno en cada servidor y otro en la red
D. Ninguno

5. *OSSEC y Snort* son dos de las alternativas de código abierto más conocidas de:

A. HIDS y NIDS, respectivamente
B. NIDS y HIDS, respectivamente
C. Los dos son NIDS
D. Los dos son HIDS

6. Las sondas de un IDS de red sirven básicamente para:

A. Recolectar el tráfico y enviarlo al sistema gestor, que se encarga de analizarlo
B. Recolectar y analizar el tráfico, generar alertas y enviar éstas al sistema gestor
C. Almacenan y gestionan las alertas recibidas
D. Clasifican y muestran los eventos recibidos, normalmente desde un interfaz gráfico

7. En entornos conmutados, cada sonda de un NIDS sólo podría analizar el tráfico del segmento en el que está ubicada. Sin embargo, imagina que tu presupuesto es limitado y debes utilizar menos sondas que segmentos. ¿Qué alternativas puedes utilizar para agregar el tráfico de red?

A. Hardware dedicado
B. Únicamente TAPs, pues los puertos de spanning no serían adecuados para este supuesto
C. TAPs y puertos de spanning en los switches
D. Únicamente puertos de spanning, puesto que los TAPs no serían adecuados en este supuesto

8. Un IDS basado en firmas funciona:

A. Buscando patrones predefinidos, pero únicamente en el tráfico de red
B. Buscando patrones predefinidos, pero pueden aplicarse tanto a HIDS como NIDS
C. Buscando patrones, pero dispone de cierta capacidad para detectar nuevos ataques que no hayan sido previamente definidos
D. Generan un modelo del comportamiento normal de la red y buscan patrones que se alejen del mismo

9. Un sistema señuelo o *honeypot*:

A. Es un tipo de IDS de red

B. Es un tipo de IDS de host

C. Es un sistema simulado trampa, con el fin de aprender las técnicas utilizadas por los atacantes

D. Es un escáner de vulnerabilidades

10. Una de las consecuencias más comunes de un IDS basado en firmas cuya base de reglas no es regularmente ajustada es que:

A. Pierden eficacia con el tiempo, ya que se reduce su capacidad de reducir las amenazas más recientes

B. Pierden eficacia con el tiempo, ya que su tasa de falsos negativas tiende a aumentar significativamente

C. Pierden eficacia con el tiempo, ya que su tasa de falsos positivos tiende a aumentar significativamente

D. Las respuestas A y C son correctas