DATOS DE LA ACTIVIDAD							
No. de Actividad:	**2.8**	**Investigación**	Investigación: Tecnologías de detección de intrusos (IDS) y prevención de intrusiones (IPS)				
Unidad:	2: Configuración de seguridad en firewall, Switches, Routers y Access point						
Carrera:	Tgo. en Desarrollo de Software						
Materia	**SEGURIDAD EN ITI**					Clave	MPF3608DSO
Profesor:	Andrés Figueroa Flores						
Alumno:	Daniel Tejeda Saavedra					Registro:	17300288
Institución:	**Centro de Enseñanza Técnica Industrial plantel Colomos**						
Semestre:	8	Grupo:	D1	Período:	Feb-Jun 2021	Fecha:	09/05/2021
Compet. Genéricas		4.1, 4.5, 5.2, 5.5		Compet. Profesional		CP1-1	

1. Objetivo(s) de la actividad

Identificar los sistemas de detección y prevención de intrusiones en una red.

2. Introducción

Los sistemas de detección y prevención de intrusiones que supervisan de forma activa y pasiva el tráfico en la red para prevenir ataques y tener una mejor respuesta ante amenazas.

3. Instrucciones (Descripción) de la actividad

1. Investigar qué es y cómo se implementa la detección de intrusos (IDS) y la prevención de intrusiones (IPS). (al menos una cuartilla por cada tecnología).
2. Usar el archivo de ejemplo de actividades, completar todos los datos del encabezado identificando si es Actividad, Investigación o Practica, así como las competencias a desarrollar para esta actividad.
3. Subir el archivo terminado, no se te olvide, la reflexión, agregar la bibliografía en formato APA y dar clic para marcar como entregada la actividad.

- **Desarrollo**

Un Sistema de Detección de Intrusos (IDS: *Intrusion Detection System*) es un componente dentro del modelo de seguridad informática de una organización. Consiste en detectar actividades inapropiadas, incorrectas o anómala, desde el exterior o interior de un dispositivo o una infraestructura de red.

El IDS se basa en la hipótesis de que el patrón de comportamiento de un intruso es diferente al de un usuario legítimo, lo que se emplea para su detección por análisis de estadísticas de uso.

Funcionamiento

El funcionamiento de un Sistema de Detección de Intrusos se basa en el análisis pormenorizado del tráfico de red o el uso de los dispositivos. Para la evaluación se compara la situación con firmas de ataques conocidos, o comportamientos sospechosos.

La mayoría de los IDS suelen disponer de una base de datos de “firmas” de ataques conocidos, que le permiten distinguir entre el uso normal de un dispositivo y el uso fraudulento, y/o entre el tráfico normal de la red y el tráfico que puede ser resultado de un ataque o intento del mismo.

En una red de comunicaciones, un IDS no solo analiza qué tipo de tráfico se emplea, sino también revisa su contenido y comportamiento; además, observa si ocurre un escaneo de puertos o la transmisión de paquetes de datos mal formados, entre otros aspectos.

Normalmente un IDS es integrado con un *firewall*, de preferencia en un dispositivo que funcione como puerta de enlace de una red. Esta asociación es muy poderosa, ya que se une la inteligencia del IDS y el poder de bloqueo del *firewall*, en el punto donde forzosamente deben pasar los paquetes y pueden ser bloqueados antes de penetrar en la red.

Un modelo IDS intenta crear patrones de comportamiento de usuarios respecto al uso de programas, archivos y dispositivos, tanto a corto como a mediano y largo plazo, para hacer la detección efectiva; además, utiliza un sistema de reglas predefinidas (“firmas o signaturas”) para la representación de violaciones conocidas.

Detección de Anomalías

La idea central del funcionamiento de un IDS se basa en el hecho de que la actividad intrusiva constituye un conjunto de anomalías (acciones extrañas o sospechosas). Si alguien consigue entrar de forma ilegal a un sistema, no actuará como un usuario comprometido, sino que su comportamiento se alejará del de un usuario normal.

De forma general, la mayoría de las actividades intrusivas resultan de la suma de otras actividades individuales que por sí solas no constituyen un comportamiento intrusivo; así las intrusiones pueden clasificarse en:

- Intrusivas, pero no anómalas: denominados Falsos Negativos (el sistema erróneamente indica ausencia de intrusión). En este caso la actividad es intrusiva pero como no es anómala no es detectada. No son deseables, porque dan una falsa sensación de seguridad del sistema.
- No intrusivas pero anómalas: denominados Falsos Positivos (el sistema erróneamente indica la existencia de intrusión). En este caso la actividad es no intrusiva, pero como es anómala el sistema "decide" que es intrusiva. Deben intentar minimizarse, ya que en caso contrario se ignorarán los avisos del sistema, incluso cuando sean acertados.
- No intrusiva ni anómala: son Negativos Verdaderos, la actividad es no intrusiva y se indica como tal.
- Intrusiva y anómala: se denominan Positivos Verdaderos, la actividad es intrusiva y es detectada.

Los detectores de intrusiones anómalas requieren realizar muchas estimaciones de varias métricas estadísticas, para determinar cuánto se aleja el usuario de lo que se considera comportamiento normal.

Características de un IDS

Cualquier sistema de detección de intrusos, sea cual sea su tipo y base de funcionamiento, debería contar con las siguientes características:

- Debe funcionar continuamente sin supervisión humana. El sistema debe ser lo suficientemente fiable para poder ser ejecutado en segundo plano como parte del dispositivo o la red que está siendo observada.
- Debe ser tolerante a fallos en el sentido de que debe ser capaz de sobrevivir a una caída del sistema.
- Debe ser resistente a perturbaciones, en el sentido en que puede monitorizarse a sí mismo para asegurarse de que no ha sido perturbado.
- Debe imponer mínima sobrecarga sobre el sistema. Un sistema que consume muchos recursos computacionales no debe ser utilizado.
- Debe observar desviaciones sobre el comportamiento estándar.
- Debe ser fácilmente adaptable al sistema operativo ya instalado, pues cada uno tiene un patrón de funcionamiento diferente y el mecanismo de defensa debe adaptarse de manera sencilla a esos patrones.
- Debe hacer frente a los cambios de comportamiento del sistema según se añaden nuevas aplicaciones al mismo.
- Debe ayudar a identificar de dónde provienen los ataques que se sufren, y recoger evidencias que pueden ser usadas para identificar intrusos.
- Deben ser “difíciles de vulnerar” y suministrar a los especialistas de seguridad “cierta tranquilidad”.

Tipos de IDS

Los sistemas de detección de intrusos pueden clasificarse dependiendo del tipo de evento que monitorean y cómo se implementan:

- **IDS basados en Red**: El sistema de detección de intrusiones de red monitorea el tráfico de red en un segmento o dispositivo, y analiza la red y la actividad de los protocolos para identificar actividades sospechosas. Este sistema también es capaz de detectar innumerables tipos de eventos de interés, y por lo general se implementa en una topología de seguridad como frontera entre dos redes, por donde el tráfico es enfilado; en muchos casos, el propio IDS termina por integrarse directamente en el firewall.
- **IDS basados en Host o abonado de la red**: El sistema de detección de intrusiones en el *host* se refiere a un equipo o activo propiamente dicho. En este caso, se considera un host, por ejemplo, al dispositivo personal de un usuario o a un servidor de aplicaciones. La detección de intrusión, en este formato, monitorea las características del dispositivo y los eventos que ocurren con él en busca de actividades sospechosas. Generalmente los IDS basados en host se pueden instalar de manera individual, tanto para equipos corporativos dentro de una red empresarial, como para terminales personales. Entre las principales características que los acompaña, se destaca el tráfico de la red para el dispositivo, los procesos en ejecución, los registros del sistema, así como el acceso y cambio en archivos y aplicaciones.
- **IDS basado en Conocimiento: hace** referencia a una base de datos de perfiles de vulnerabilidades de sistemas ya conocidos para identificar intentos de intrusión activos. En este caso, es de suma importancia que la estructura tenga una política de actualización continua de la base de datos (firmas) para garantizar la continuidad de la seguridad del ambiente, teniendo en cuenta que lo que no se conoce, literalmente, no será protegido.
- **IDS basado en Comportamiento**: analiza el comportamiento del tráfico siguiendo una línea de base o estándar de actividad normal del sistema, para identificar intentos de intrusión. En el caso de que haya desviaciones de este patrón o líneas de base, se pueden tomar algunas acciones, ya sea bloqueando ese tráfico temporalmente, o emitiendo alarmas de operación de red, que permitan que esa anormalidad pueda ser mejor investigada, liberada o permanentemente bloqueada.
- **IDS Activo:** se define un IDS como activo, desde el momento en que se determina que bloqueará automáticamente ataques o actividades sospechosas que sean de su conocimiento, sin necesidad de intervención humana. Aunque potencialmente es un modelo extremadamente interesante, es importante un ajuste de parámetros adecuado a los ambientes protegidos, para minimizar falsos positivos, y que se bloqueen conexiones legítimas que causen trastornos para las organizaciones.
- **IDS Pasivo:** monitorea el tráfico que pasa a través de él, identificando potenciales ataques o anormalidades y, con base en ello, genera alertas para administradores y equipos de seguridad; sin embargo, no interfiere en absolutamente nada en la comunicación. Aunque no actuar directamente en la prevención, sirve como un excelente termómetro de ataques e intentos de acceso no autorizados a la infraestructura de una empresa.

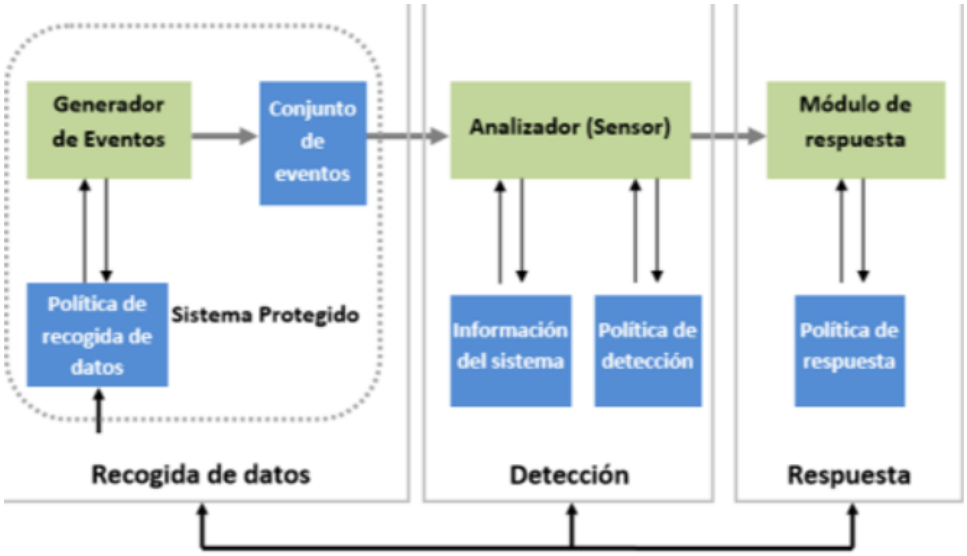
Implementación

Para poner en funcionamiento, un sistema de detección de intrusos se debe tener en cuenta que es posible optar por una solución de hardware, de software, o incluso una combinación de estos. La posibilidad de introducir un elemento hardware es debido al alto procesamiento de información en redes con mucho tráfico; a su vez, los registros de firmas y las bases de datos con los posibles ataques necesitan gran cantidad de almacenamiento.

Primero que nada, es necesario elegir un software IDS tomemos por ejemplo SNORT un sistema IDS de código abierto mas usados.

Para tratar con una amenaza deberemos seguir con los siguientes pasos:

- Prevención
- Simulación
- Monitorización de la intrusión
- Notificación
- Respuesta



Mediante SNORT podemos aplicar una serie de reglas con las cuales podemos configurar la seguridad de la red.

SNORT puede implementar cualquier tipo de regla, las **reglas de SNORT** no están incluidas con el software. Sin embargo, existen diferentes fuentes para encontrar e implementar reglas:

1. **Equipo de Investigación de Vulnerabilidad (VRT)**: Estas son las reglas de Snort "oficiales". Son proporcionados por Sourcefire y son actualizados semanalmente por Sourcefire VRT.
2. **Emerging Threats (ET):** Las reglas de amenazas emergentes son un proyecto comunitario de código abierto. Este conjunto es el conjunto de reglas de Snort más diverso y de movimiento más rápido. Las reglas se actualizan varias veces al día.
3. **Reglas de la comunidad**: Estas reglas son creadas por la comunidad de SNORT. Hay muy pocas reglas y la última versión es de 2007 para Snort 2.4. La mayoría de las amenazas que detectan ya están implementadas en ET o VRT.
4. **Reglas caseras y otras**: Son las reglas, creadas y mantenidas localmente, según las necesidades específicas de la red. También pueden existir otras reglas. Para amenazas específicas y otras amenazas "únicas", los motores de búsqueda pueden proporcionar reglas más específicas, pero es necesario saber qué buscar.

Definir reglas SNORT

Una regla de SNORT puede definirse mediante muchos parámetros. Una regla se compone de dos partes distintas: El encabezado de la regla y las opciones de la regla.
El encabezado de la regla contiene la acción de estas, el protocolo, las direcciones IP de origen y destino y las máscaras de red, y la información de los puertos de origen y destino. La sección de opciones de reglas contiene mensajes de alerta e información sobre qué partes del paquete deben inspeccionarse para determinar si se debe tomar la acción de la regla. Por ejemplo:

```
alert tcp any any -> 10.0.0.0/24 80 \ (content:"|00 00 00 00|"; depth: 8; \
msg:"Error de bytes nulos"; sid:9876)
```

Esta regla activará una alerta si se encuentran cuatro bytes nulos en los primeros ocho bytes de todo el tráfico enviado al puerto 80 a la red 10.0.0.0/24. El ID único de la regla es 9876 y el mensaje de alerta es "Error de bytes nulos". Las reglas son poderosas y hay muchas posibilidades: es posible buscar bytes en una posición específica, dentro del rango de otros bytes, o contar el número de ocurrencias de una coincidencia antes de una alertar. También es posible utilizar Expresiones regulares compatibles con Perl (PCRE) en los datos y limitar la búsqueda a bytes específicos.

Para que una regla active una alerta, todos los elementos contenidos en las opciones de la regla deben ser verdaderos. Estos elementos se comprueban secuencialmente. Si el primero es falso, los demás no se comprobarán. Por tanto, *el orden de los argumentos es muy importante para optimizar las reglas*.

Con la implementación de un IDS se lograrán detectar los ataques mas frecuentes y se logra una notoria mejoría en la protección.

Métricas en las reglas SNORT

Las métricas que deben evaluarse para cada conjunto de reglas incluyen, por ejemplo:

Nivel de amenaza

Las amenazas, por ejemplo, podríamos dividirlas en tres categorías:

- **Comprometidos:** Estos son los incidentes más importantes. Incluyen hosts comprometidos, hosts infectados por virus o malwares, o usuarios que realizan acciones ilegales. Cada incidente debe ser detectado y actuar sobre el mismo.
- **Violaciones de políticas**: Cuando un usuario no cumple con las políticas, este conjunto de reglas activará una alerta. Los ejemplos típicos son las reglas de Peer-to-Peer (P2P) e Internet Relay Chat (IRC), por ejemplo.
- **Ataques dirigidos, exploraciones y otros**: Los ataques potenciales entran en esta categoría, incluso si no tienen éxito. No significan que un host se haya visto comprometido. Los virus y otros malwares entrantes se clasificarán aquí. Proporcionan información sobre la actividad de la red, pero no requieren necesariamente ninguna acción.

Clasificación de las reglas SNORT

Utilizando la clasificación propuesta por Snort, se propone el siguiente esquema de clasificación:

- **Comprometido**: Esta categoría contiene todas las firmas que detectan un exploit exitoso o que indican que un host ha sido comprometido. Los siguientes conjuntos de reglas contienen reglas que se incluyen en esta categoría: *attack-answers.rules, backdoor.rules, ddos.rules, emergen-attack response.rules, emergenvirus.rules, virus.rules*. Esta categoría propuesta solo detecta hosts comprometidos o que ejecutan malware que podrían llevar a un atacante remoto a tomar el control abriendo una puerta trasera o robando contraseñas. Los adwares y otros badwares no están incluidos y se colocaron en otra categoría.
- **Política:** Esta categoría contiene todas las firmas que ayudan a detectar P2P e IRC, que no están permitidas por nuestra organización o que recomiendan ciertos CERTs. Los siguientes conjuntos de reglas contienen reglas que entran en esta categoría: *p2p.rules, emergentes-p2p.rules y local.rules*. El último, local.rules, contiene reglas caseras adicionales para detectar el uso de IRC. Los conjuntos P2P contienen firmas para detectar todo tipo de tráfico, y hay algunas reglas que deben desactivarse antes de que este conjunto dé resultados utilizables.
- **Ataques y otros**: Otros archivos fuente entran en esta gran categoría. Existen otras políticas como mensajería instantánea (IM), información sobre ataques entrantes o conjuntos para detectar hosts que ejecutan programas publicitarios y otros programas maliciosos.

IPS

Los IPS son dispositivos de hardware o software encargados de revisar el tráfico de red con el propósito de detectar y responder a posibles ataques o intrusiones. La respuesta consiste en descartar o modificar los paquetes procedentes del ataque de tal manera que se anule su propósito. Este comportamiento los clasifica como dispositivos proactivos debido a su reacción automática a situaciones anómalas.

Mientras el IDS se limita a detectar y notificar la intrusión al administrador del sistema, y éste se encarga de recibir y responder las alertas; el IPS detecta la intrusión y la detiene de algún modo ya predefinido, comprobando ciertos comportamientos en la red previamente configurados como anómalos. Gracias a este hecho, el nivel de alertas de un IPS es considerablemente menor que el nivel de alertas producido por un IDS. La diferencia principal entre los IDS activos y los IPS es que estos últimos están en capacidad de inutilizar los paquetes involucrados en el ataque modificando su contenido. Una desventaja de los IPS viene por parte de la reacción proactiva ante las intrusiones. Por una parte, se tiene una disminución en el tiempo de reacción ante un ataque, pero también puede provocar efectos inesperados e inconvenientes cuando éste reacciona ante un falso positivo (FP), lo que podría llevar a una denegación de servicio o incluso al aislamiento de la máquina. Por ello, el uso de IPS en sistemas de control industrial ha de ser bien estudiado o en su defecto utilizar un cortafuego que posea inspección profunda de paquetes para mayor seguridad en las comunicaciones.

Las arquitecturas actuales centralizan el funcionamiento del IPS, lo que facilita su operación y administración, pero disminuye la escalabilidad del sistema y convierte al IPS en un punto crítico.

Básicamente, los diferentes tipos de IPS se distinguen por su ubicación. νIPS basados en host (HIPS): Esta aplicación de prevención de intrusiones reside en la dirección IP específica de un solo equipo, permite prevenir posibles ataques en los hosts. νIPS basadas en red (NIPS): Monitorizan la red en busca de tráfico sospechoso. νIPS basado en red Wireless (WIPS): Monitorizan redes inalámbricas, al igual que hacen los NIPS con redes LAN. νIPS basado en Análisis de Comportamiento de Red (NBA): Examina el tráfico de red para identificar amenazas que generan tráfico inusual, como ataques de DoS o malware.

PS basado en red (NIPS) vs IPS basado en host (HIPS) Un HIPS puede manejar el tráfico cifrado y sin cifrar por igual, ya que puede analizar los datos después de que hayan sido descifrados en el host. Por otra parte, un NIPS no utiliza el procesador y la memoria del host, por lo que no impacta en el rendimiento de la máquina. Un NIPS puede detectar eventos dispersos a través de la red y puede reaccionar fácilmente, mientras que con un HIPS se tardaría demasiado tiempo en informar a un motor central y posteriormente informar al resto de los equipos.

La evolución y las categorías de los IPS Es posible distinguir dos generaciones históricas de los IPS: νLos IPS de primera generación, al detectar un ataque proveniente de una dirección IP determinada, descartaban todos los paquetes de esa dirección, estuvieran o no involucrados en el ataque. νLa evolución de los IPS se debe a la capacidad de descartar únicamente los paquetes relacionados con el ataque identificado, permitiendo el tráfico de otros paquetes provenientes de la IP del atacante, siempre y cuando no estuvieran relacionados con el ataque. Se pueden distinguir cinco categorías de IPS dependiendo de su funcionamiento, sus capacidades y su ubicación en la arquitectura de la red.

IPS inline. Estos IPS suponen la evolución de los NIDS basados en firmas y hacen la función de un Bridge a nivel de capa dos, revisando todos los paquetes que circulan por la red en busca de firmas. En caso de detectar alguna anomalía automáticamente es almacenado en un log, o incluso puede permitir el paso de un paquete alterando su contenido para de esta manera frustrar un ataque, sin que el atacante se dé cuenta. Este proceso es realizado mediante Scrubbing5, que consiste en la

detección de errores por medio de verificación checksum o por redundancia con copias de datos. Habitualmente son conocidos como IPS de red o NIPS.

Reflexión

Los sistemas de detección y prevención de intrusiones y los sistemas de procedimiento y administración de eventos e incidentes aportan un grado de estabilidad a los sistemas de control continuamente y una vez que se encuentren de manera correcta configurados y supervisados. La configuración de un sistema de prevención puede involucrar varios inconvenientes sobre un sistema de control en producción, por lo cual tienen que ser de manera correcta valoradas cada una de las repercusiones, así como hacer cada una de las probables pruebas anteriormente, incluyendo las de conservar el sistema solamente en modo detección hasta estar plenamente seguros de que no se bloqueará tráfico crítico para el sistema e ir afinando progresivamente el sistema para que solamente detecte o informe de eventos relevantes.

Referencias

Ernesto. A. (12/03/2019). Sistema de Detección de Intrusos
Recuperado el 05/05/2021 de: https://infotecs.mx/blog/sistema-de-deteccion-de-intrusos.html

Ramiro R. (22/Nov/2020). Reglas SNORT Recuperado e 05/05/2021 de:
https://ciberseguridad.blog/reglas-snort-deteccion-de-intrusos-y-uso-no-autorizado/

(Nov, 2017) Diseño y Configuración de IPS, IDS y SIEM en Sistemas de Control Industrial.
Recuperado el 05/05/2021 de:
https://www.incibe-cert.es/sites/default/files/contenidos/guias/doc/certsi_diseno_configuracion_ips_ids_siem_en_sci.pdf