UNIVERSIDAD CATÓLICA DE CÓRDOBA
JESUITAS

INTRUSION DETECTION SYSTEMS

MATERIA: Seguridad Informática
PROFESOR: Mariano Aliaga
ALUMNAS: Londero, Camila Soledad - Vargas, Maria Micaela

Conceptos básicos

- **Intrusión**: Conjunto de acciones que intentan comprometer la integridad, confidencialidad o disponibilidad de un recurso. Podemos decir que se trata de una violación de las políticas de seguridad del sistema. Los intrusos pueden utilizar fallos en la arquitectura de los sistemas y el conocimiento interno del sistema operativo para superar el proceso normal de autentificación.

  Tipos de intrusos:
  - Suplantador: Es un individuo que no está autorizado a usar el sistema y penetra los controles de acceso para obtener provecho de la cuenta de un usuario legítimo. Es un usuario externo.
  - Usuario fraudulento: Es un usuario legítimo que accede a recursos para los que el acceso no está autorizado o hace mal uso de sus privilegios. Es un usuario interno.
  - Usuario clandestino: Es un individuo que toma el control de supervisión del sistema y lo usa para evadir los controles de auditoría y de acceso o para suprimir información de auditoría. Es un usuario interno o externo.

- **Detección de intrusos:** Análisis automático de parámetros que modelan la actividad de un entorno con el propósito de detectar e identificar intrusiones.
- **Falso positivo:** Consiste en la detección de datos o paquetes como una amenaza o intrusión cuando en realidad no se trata de un intento de ataque sobre la red.
- **Falso negativo:** Consiste en los paquetes o datos que son amenazas para una red pero el sistema de seguridad no detecta dichas amenazas.
- **Firewall:** es un elemento de hardware o software que se utiliza en una red de computadoras para controlar las comunicaciones, permitiéndolas o prohibiéndolas según las políticas de red que haya definido la organización responsable de la red.
- **Firmas / Bases de datos de firmas:** Las bases de datos de antivirus se llaman históricamente *firmas*, tanto en el uso común como en el escrito. Las firmas de virus son una secuencia continua de *bytes* comunes en cierta muestra de *malware*, lo que significa que se contiene dentro de este o del archivo infectado y no en archivos no afectados.
- **Log:** Un log es un registro que deja un sistema informático. Por ejemplo: accesos de usuarios, actividades de borrado y cambios realizados en el sistema.Con esta información podemos ver claramente las actividades que se han realizado en nuestros sistemas y, por lo tanto, con un pequeño análisis podríamos detectar situaciones extrañas y anómalas

¿Qué son los IDS?

El sistema de detección de intrusiones es una aplicación usada para detectar accesos no autorizados a un ordenador o a una red, es decir, son sistemas que monitorizan el tráfico entrante y lo cotejan con una base de datos actualizada de firmas de ataque conocidas. Ante cualquier actividad sospechosa, emiten una alerta a los administradores del sistema quienes han de tomar las medidas oportunas.Los IDS no sólo analizan el tráfico de la red, sino que también analizan su comportamiento y su contenido. Estos accesos pueden ser ataques esporádicos realizados por por usuarios malintencionados o repetidos cada cierto tiempo, lanzados con herramientas automáticas. Estos sistemas sólo detectan los accesos sospechosos emitiendo alertas anticipatorias de posibles intrusiones, pero no tratan de mitigar la intrusión. Su actuación es REACTIVA.

Ventajas y Desventajas

Ventajas:

- Ver lo que está sucediendo en la red en tiempo real en base a la información recopilada.
- Reconocer modificación en los documentos
- Automatizar los patrones de búsqueda en los paquetes de datos enviados a través de la red.

Desventajas:

- Estas herramientas no están diseñadas para prevenir o detener los ataques que detectan.
- Son vulnerables a ataques DDos que pueden provocar inoperatividad.
- Pueden ocurrir falsos positivos (cuando detecta datos o paquetes como una amenaza o intrusión y se lanza una alarma pero no se trata de algún intento de ataque) o falsos negativos (paquetes o datos que son amenazas para una red pero el sistema de seguridad no detecta dichas amenazas).

Funcionamiento:

El funcionamiento de estas herramientas se caracterizan por un sistema de gestión central que recibe las informaciones necesarias tanto desde el software basado en la red como desde el software basado en el host. Hay tres componentes básicos involucrados en el proceso de reconocimiento.

Monitoreo de datos

El monitor de datos tiene la tarea de recoger y hacer un primer filtro a los datos necesarios para filtrar intrusos. Se trata de la auditoría de datos, que incluye archivos log de sistemas informáticos y aplicaciones de seguridad como, por ejemplo, la capacidad de la CPU, el número de conexiones de red activas o la cantidad de intentos de inicio de sesión. Además, en los sistemas híbridos de detección de intrusos, el monitor de datos también evalúa los datos de las conexiones TCP/IP, tales como direcciones de origen y destino y otras propiedades de los paquetes de datos enviados y recibidos, que obtiene gracias al sensor IDS basado en la red.

Análisis

El monitor de datos envía el flujo de datos recogidos y previamente filtrados al llamado analyzer (analizador). Este debe editar y evaluar la información obtenida en tiempo real, de lo contrario no sería posible evitar los ataques a tiempo. Los métodos utilizados por el analizador para evaluar los datos son:

- **Por patrón:** En caso de usos indebidos del sistema (misuse detection), el analizador intenta detectar patrones de ataque conocidos, denominados firmas (signature), en los datos obtenidos. Estos se almacenan en una base de datos independiente que es actualizada periódicamente. Allí, cada entrada recibe, además, información sobre la gravedad del ataque. La desventaja de este método es que mientras que los patrones de ataque conocidos pueden ser claramente identificados y evaluados, aquellos que no hayan sido incluidos en la base de datos serán imperceptibles para este mecanismo de detección.
- **Heurística:** La detección de anomalías (anomaly detection) se basa en un principio diferente: este método de análisis supone que el acceso no autorizado causa un comportamiento anormal en el sistema y, por lo tanto, se diferencia de los valores previamente establecidos. Así, el analizador se puede configurar de tal manera que encienda una alarma cuando la capacidad de la CPU o el tráfico a la página web sobrepase un cierto número (enfoque estático). Como alternativa, este también puede incluir la secuencia temporal de los eventos en la evaluación (enfoque lógico). La detección de anomalías puede ayudar a detectar ataques nuevos y desconocidos, sin embargo, este activo método de reconocimiento también alerta en caso de que el sistema se encuentre en un estado inusual que no haya sido generado por un intruso.

Informe de resultados

En la etapa final, el Intrusion Detection System informa al administrador de la red si encontró un ataque o un comportamiento sospechoso del sistema. Dependiendo del potencial de riesgo, existen diferentes posibilidades de notificarlo. Así, por ejemplo, un sistema que necesita defenderse enviaría

- un correo electrónico que explique la naturaleza del ataque,
- una alarma local como una ventana emergente que active la consola de seguridad,
- o un mensaje de alerta a un dispositivo móvil.

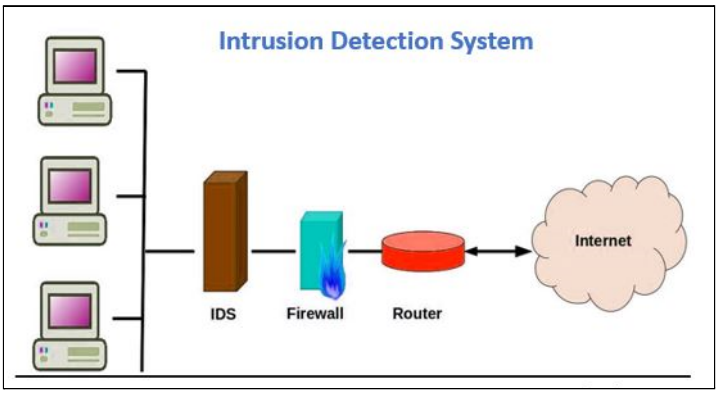
El grado de riesgo obtenido en la detección de anomalías se deriva del grado de desviación del valor estándar, mientras que el procedimiento de identificación de usos indebidos en el sistema, como se mencionó anteriormente, obtiene un nivel de clasificación dentro de la base de datos de patrones.

Normalmente esta herramienta se integra con un firewall. El detector de intrusos es incapaz de detener los ataques por sí solo, excepto los que trabajan conjuntamente en un dispositivo de puerta de enlace con funcionalidad de firewall, convirtiéndose en una herramienta muy poderosa ya que se une la inteligencia del IDS y el poder de bloqueo del

firewall, al ser el punto donde forzosamente deben pasar los paquetes y pueden ser bloqueados antes de penetrar en la red.

Los IDS suelen disponer de una base de datos de “firmas” de ataques conocidos.

Dichas firmas permiten al IDS distinguir entre el uso normal del PC 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.



Algunas de las técnicas específicas que usan los IDS en sistemas informáticos son:
Almacenamiento de paquetes bajo sospecha de ataque: cuando se sospecha de alguna intrusión, el IDS va a tomar la medida de guardar un registro detallado con todos los paquetes de información que ocasionaron una señal de alerta y que fueron capturados por el protocolo de detección.
Verificación de la configuración de dispositivos externos: en donde al momento de detectar una intrusión o sospechar de su existencia, el IDS procede a solicitar una reconfiguración de los dispositivos externos que tiene la misión de bloquearla, como por ejemplo, el firewall. Esto se realiza mediante el envío de una señal de alerta.
Envío de una señal de alerta: Los IDS cuentan con la función de notificar visualmente al usuario, así como también a los administradores del sistema sobre la presencia de una posible intrusión.
Alerta mediante correo electrónico: algunos IDS cuentan con la capacidad de remitir un correo electrónico de alerta a uno o más usuarios en donde se informa la posible intrusión.
Registro de la intrusión en una base de datos: Toda detección de una posible intrusión debe ser registrada, para así llevar un control detallado del incidente. Precisamente, el IDS se encarga de cumplir con este requerimiento, por lo que remite un informe a una base de datos centralizada.
Dicho informe debe contener la fecha específica del ataque, el protocolo utilizado, así como las direcciones IP del intruso y del destinatario.

Características de un IDS

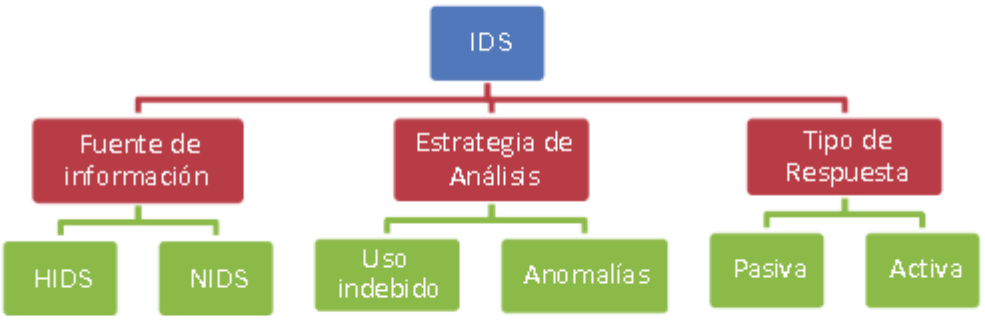
Un IDS debe poseer las siguientes características:

- ❏ Ligero: Debe imponer mínima sobrecarga sobre el sistema.
- ❏ Adaptable: Debe ser fácilmente adaptable al sistema operativo ya instalado, pues cada sistema operativo tiene un patrón de funcionamiento diferente y el mecanismo de defensa debe adaptarse de manera sencilla a esos patrones. También debe

hacer frente a los cambios de comportamiento del sistema según se añaden nuevas aplicaciones al mismo

- ❏ Confiable: Debe funcionar continuamente sin supervisión humana y por lo tanto lo suficientemente fiable para poder ser ejecutado en segundo plano como parte del dispositivo o red que está siendo observada. También deben ser difíciles de vulnerar y suministrar “tranquilidad” a los especialistas de seguridad.
- ❏ Robusto: debe ser tolerante a fallos en el sentido de que debe ser capaz de sobrevivir una caída del sistema y además resistir perturbaciones, en donde deberá monitorizarse a sí mismo para asegurarse que no ha sido perturbado.
- ❏ Distinguir lo que es un ataque de lo que es compartir un recurso del sistema.
- ❏ Debe ayudar a identificar de dónde provienen los ataques que se sufren, y recoger evidencias que pueden ser usadas para identificar intrusos.

Clasificación de IDS



Según tipo de respuesta:

- **Pasivos:** realiza el sencillo trabajo de detección y alerta. Simplemente alerta al administrador de cualquier tipo de amenaza y bloquea la actividad en cuestión como medida preventiva. Solo notifican mediante algún mecanismo (alerta, log, etc) pero no actúa sobre el ataque o el atacante.
- **Activos:** detecta actividad malintencionada, alerta al administrador de las amenazas y también responde a esas amenazas. Genera algún tipo de respuesta sobre el sistema atacante o fuente de ataque como cerrar la conexión, reprogramar el firewall o enviar algún tipo de respuesta predefinida.

Según estrategia de análisis:

- **Uso indebido:** son los IDS que cuentan con el conocimiento a priori de las secuencias y actividades que conforman el ataque. Por lo tanto, para detectar intrusiones dentro de la información recopilada de la fuente, se realiza una comparación de la misma con los patrones de ataques previamente almacenados y, en caso de encontrar similitud, se genera una alarma. Con este método se logra detectar intentos de explotación de vulnerabilidades típicos, de los cuales ya existe información.

Utilizar este tipo de IDS tiene varias ventajas entre las cuales podemos nombrar la amplia seguridad que ofrece al detectar una intrusión puesto que clasificar una actividad como intrusiva significa que correspondió con un patrón (de la base de datos) que fue reconocido con anterioridad como un ataque y de esta forma tenemos menos falsos positivos. La desventaja principal de este tipo de detección radica en su incapacidad para detectar nuevos ataques y en la necesidad de mantener constantemente actualizada su base de patrones. Estas debilidades son de vital importancia en la actualidad, donde los ataques son cada vez más originales y cada vez más frecuentes. Debido a esto, las investigaciones recientes de detección de uso indebido se centran en lograr patrones más genéricos que permitan que los sistemas de este tipo no puedan ser burlados con mutaciones de ataques conocidos

- **Detección de anomalías**: tienen un conocimiento complementario a los de uso indebido, es decir, que parten del conocimiento de lo normal y toda actividad que se aleje de este comportamiento es considerada una intrusión.Este tipo de detección evita el proceso de actualización de una base de datos de patrones de intrusión y brinda la posibilidad de detectar ataques nuevos de los cuales no se tenga información alguna. Sin embargo, este tipo tiene algunas desventajas como generar falsos positivos ya que el comportamiento normal de los usuarios es extremadamente difícil de modelar por lo variable que puede llegar a ser y por lo tanto un comportamiento inusual no tiene necesariamente que ser ilícito. Otra debilidad es que necesitan un largo periodo de “entrenamiento”, previo a su uso, para poder identificar los comportamientos normales de los usuarios y sistemas dentro de la red.

Según el Origen de Datos:

- **HIDS (IDS basados en host):** Son diseñados para monitorear, detectar y responder a los datos generados por un usuario o un sistema en un host. Estos sistemas ayudan a las organizaciones a monitorear los procesos y aplicaciones que se ejecutan en dispositivos como servidores y estaciones de trabajo. HIDS rastrea los cambios realizados en la configuración del registro y la configuración crítica del sistema, archivos de registro y contenido, alertando sobre cualquier actividad no autorizada o anómala.
  Las tecnologías HIDS son de naturaleza 'pasiva', lo que significa que su propósito es identificar la actividad sospechosa, no prevenirla.

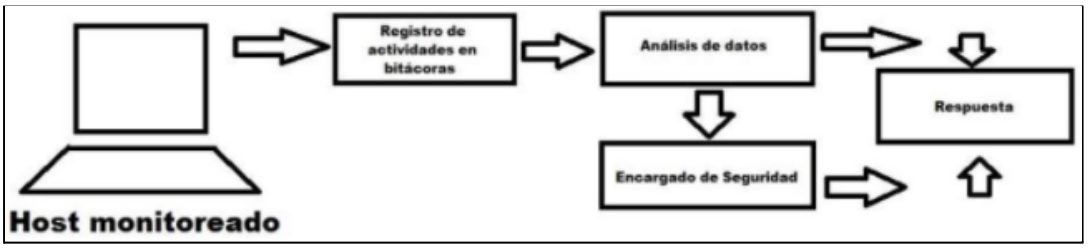
  Para detectar amenazas, los sistemas de detección de intrusos basados en host requieren la instalación de sensores conocidos como 'agentes HIDS' en activos monitoreables.

  Un sistema HIDS utiliza una combinación de métodos de detección basados en firmas y basados en anomalías para identificar una amplia gama de amenazas, que incluyen:
  - Intentos de acceso e inicio de sesión no autorizados
  - Escalada de privilegios
  - Modificación de archivos de configuración, datos y binarios de la aplicación
  - Instalación de aplicaciones no deseadas
  - Procesos deshonestos

- Servicios críticos que se han detenido o no se han podido ejecutar

Ventajas:
- Detectan mejor los ataques desde dentro del equipo.
- Asocian usuarios y programas con sus efectos en el sistema.
- Informan sobre el estado del blanco atacado.
- Protegen el host donde residen.

Desventajas:
- Lento en comparación con el NIDS.
- Tardan en actuar (registros de actividad y cambios en el sistema).
- Dificultad de implantación.
- No son seguros si se ha atacado con éxito.
- Si cae el host no se genera ninguna alerta.

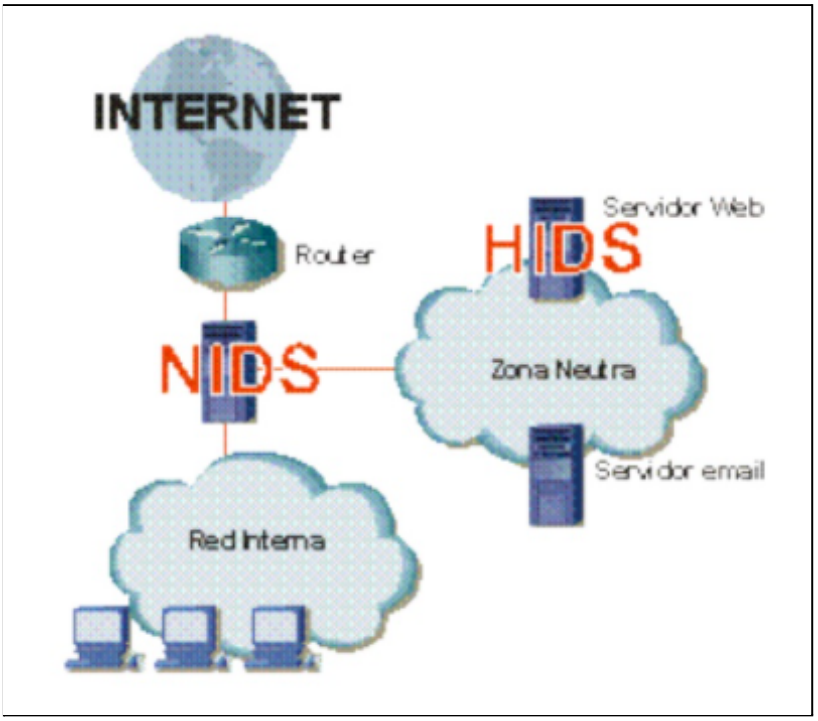


- **NIDS (IDS basados en red):** Son diseñados para analizar el tráfico de la red completa examinando los paquetes individualmente, detectando paquetes armados maliciosamente y diseñados para no ser detectados por los firewalls, encontrar cual es el programa al que se está accediendo y producir alertas cuando el atacante intenta explotar algún fallo de este programa. Es un dispositivo de red configurado en modo promiscuo. Analizan el tráfico de red, en tiempo real y no solo trabajan a nivel TCP/IP sino también a nivel de aplicación.

  Componentes:
  - Sensores(agentes): Buscan el tráfico sospechoso.
  - Consola: Recibe las alarmas de los sensores y reacciona dependiendo de la alarma.

  Ventajas:
  - Se instala en un segmento de red, detecta ataques en todos los equipos conectados.
  - Independiente de la plataforma de los equipos.
  - Capaces de detectar manipulación de cabeceras IP, negación de servicio.
  - Invisibles a los atacantes.

  Desventajas:
  - Ineficientes con texto cifrado.
  - Malos en redes de alta velocidad.
  - La congestión provocará la pérdida de paquetes.
  - No se determina si el ataque tuvo éxito o no.



Acciones a tomar ante una intrusión

Una vez que nuestro IDS detecta una intrusión, hay dos tipos de respuestas:

- **Respuestas Activas:** Estas respuestas se pueden dividir en dos clases

  - Aquellos que ejercen control sobre el sistema atacado y modifican el sistema para mitigar los efectos del ataque.Las actuaciones dependen del tipo de ataque en concreto, pero en general, deberemos de asegurarnos de que:

    - *Contengamos el ataque*, por ejemplo, aislando los dispositivos infectados.
    - *Eliminamos las posibles causas,* para asegurarnos de que el ataque no se vuelva a reproducir.
    - Determinamos el alcance del ataque, teniendo en cuenta tanto los equipos y dispositivos, como la posible información que haya sido sustraída.
    - *Aseguramos la continuidad del servicio*, para limitar lo más posible las consecuencias sobre nuestro negocio.

  - Aquellos que ejercen control sobre el sistema atacante y se convierten en atacantes intentando remover la plataforma de operación del atacante. (No es legal ni defendible frente a una corte).

- **Respuestas Pasivas:** Estas responden con una notificación a la autoridad necesaria, y no intentan mitigar el daño hecho o buscar dañar al atacante.

Para poder responder con eficacia el punto inicial es la planificacion y organizacion, por lo que debemos:

- **Planear:** Crear un plan simple, claro y preciso que determine de forma clara quién hace qué, cómo y cuándo. Este plan debe permitir reaccionar de forma rápida y precisa ante un ataque.
- **Crear un equipo de respuesta a incidentes:** Se debe crear un equipo con roles detallados y responsabilidades claras. Se recomienda que el equipo no esté formado únicamente por técnicos, sino que hay que mezclar equipo técnico y no técnico. Es importante que participen otros departamentos como Marketing, RRPP, legal, RRHH y alta dirección, todos deben estar presentes ante una crisis. Hay que tomar decisiones que pueden tener impactos económicos, legales y de daños de imagen.
- **Clasificar incidentes:** Es muy importante clasificar incidentes, establecer criticidades, vectores de ataque e impactos. Esto permite tener un histórico de incidentes que nos permite aprender para futuras ocasiones. Todo esto tiene el objetivo de proteger el negocio, por tanto, debemos entender qué prioridades tiene el negocio, saber qué es lo principal porque quizá tengamos que proteger los activos críticos y quizá sacrificar lo menos críticos.
- **Priorizar el negocio:** Se debe entender las prioridades del negocio y alinear el plan a sus necesidades.

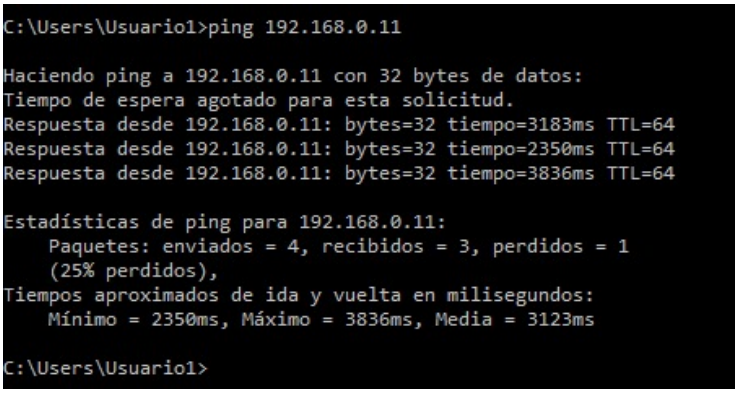
Ejemplos de IDs

1. **Snort:** es una IDS libre y gratuito. Es el más conocido de los IDs ya que su principal ventaja es la capacidad para realizar análisis de tráfico en tiempo real y registro de paquetes en redes. Snort es muy utilizado para detectar worms, exploits, exploración de puertos y otras amenazas maliciosas..
2. **Suricata:** es de código abierto, rápido y robusto. El motor de Suricata es capaz de detectar intrusos en tiempo real, prevenir intrusiones en línea y monitorear la seguridad de red. Captura el tráfico que pasa en un flujo antes de la decodificación. A diferencia de Snort, configura los flujos separados después de capturar y especifica cómo se separa el flujo entre los procesadores.
3. **OSSEC:** Este IDS realiza tareas como análisis de registro, comprobación de integridad, supervisión del registro de Windows, detección de rootkits, alertas basadas en el tiempo y respuesta activa. El sistema OSSEC está equipado con una arquitectura centralizada y multiplataforma que permite que los administradores supervisan de forma precisa varios sistemas .
4. **Security Onion:** Es una distribución Linux que está orientada a la detección de amenazas, monitorización de seguridad y gestión de los logs.Una de las características más destacadas de Security Onion, es que cuenta con múltiples herramientas incluidas por defecto. Incluye TheHive, Playbook, Fleet, Osquery, CyberChef, Elasticsearch, Logstash, Kibana, Suricata, Zeek, Wazuh y muchas otras herramientas de seguridad.

UNIVERSIDAD CATÓLICA DE CÓRDOBA
JESUITAS

PARTE PRÁCTICA
Usando SNORT
Instalamos snort y definimos una regla de mensaje que nos debería mostrar al realizar un ping en el Ip.

Realizamos un ping a la ip desde otro dispositivo.



En la consola de snort nos notificará sobre los intentos de intrusión.

UNIVERSIDAD CATÓLICA DE CÓRDOBA
JESUITAS

Bibliografía:

https://www.incibe.es/protege-tu-empresa/blog/son-y-sirven-los-siem-ids-e-ips
https://es.slideshare.net/katkt8/expo-ids
https://www.tecsens.com/proteger-mi-empresa-de-intrusiones/
https://dementium2.com/administrador-neto/sistemas-de-deteccion-de-intrusiones-explicados-12/
https://uss.com.ar/preguntas-frecuentes/sistema-de-deteccion-de-intrusos/
http://www.cybsec.com/upload/ESPE_IDS_vs_IPS.pdf
https://www.rediris.es/cert/doc/unixsec/node26.html#SECTION07680000000000000000
https://infotecs.mx/blog/sistema-de-deteccion-de-intrusos.html
https://www.researchgate.net/publication/277872813_Estudio_de_viabilidad_de_un_modelo_de_deteccion_de_intrusos_de_red#pf6
http://www.cryptomex.org/SlidesSeguridad/IDS.pdf
https://www.ibm.com/ar-es/services/business-continuity/cyber-attack
https://blog.mdcloud.es/ataque-cibernetico-consecuencias-como-actuar-y-como-protegerse/
https://www.cic.es/preparacion-respuesta-ataques-ciberneticos/