

Detección de Intrusiones

Redes de Comunicaciones 2

**Alvaro Ortigosa
Eloy Anguiano**

Sistema detector de intrusiones (IDS)

- Alarma contra intrusos de los sistemas informáticos



Factores agravantes

- BYOD...
- Cibercrimen = crimen organizado
- Estados implicados
 - Stuxnet y derivados; NSA; *Titan Rain*, Rusia, etc.
- Ataques internos
- Nueva vida digital
 - Redes sociales, sistema bancario, dispositivos cotidianos
- ...

Estado actual

- No hay forma de detener
 - (impedir entrar a un sistema informático)
- a un adversario con suficiente decisión y recursos
- El problema se convierte en dificultar entrada, y detectar asap que han entrado.
 - Duración intrusión media: 15 meses!!

Detección de Intrusiones

- Origen: auditoría de sistemas
- En un principio no eran por motivos de seguridad. Se **examinan logs**:
 - Para cobrarle a los usuarios por uso de recursos
 - Para saber mejor cómo se usaban los sistemas informáticos

Detección de Intrusiones

- Origen:
 - A principios de los 70' los propietarios de los grandes sistemas
 - En particular el DoD@USA
 - perciben los peligros del robo de información
 - Surge la idea de analizar la información de las actividades de los usuarios
 - (es decir, los logs)
 - en buscar de **comportamiento anómalo**

Detección de Intrusiones

- Proceso de monitorizar las redes y sistemas informáticos para detectar violaciones a la política de seguridad.



Sistema detector de intrusiones

- Tres componentes funcionales
 - Fuente de información que provee un flujo de registros de eventos
 - Un motor de análisis que encuentra síntomas de intrusiones
 - Un componente de respuesta que genera las reacciones basadas en la salida del motor de análisis

Respecto de la auditoría

- La detección de intrusiones es un tipo de auditoría.
- La auditoría tradicional (examen sistemático de registros) está diseñada para ocurrir a intervalos infrecuentes.
- La detección de intrusiones enriquece este proceso, convirtiéndolo en un proceso continuo.

Auditoría de seguridad

- Revisión manual de logs
- Estructurado para permitir a los responsables asegurar que las actividades están de acuerdo con algún conjunto de políticas de seguridad

Auditorías de seguridad

- Si se encontraba alguna incumplimiento de las políticas:
 - Atribución (accountability): determinar quién fue responsable.
 - Evaluación de daños: determinar qué acciones se llevaron a cabo y qué daños provocaron.
 - Reparación de daños: determinar qué pasos se requieren para reparar los datos y restaurar la operación segura del sistema.

Evolución de las auditorías

- Al volverse más rápidos, complejos y numerosos los sistemas informáticos
- El tamaño y complejidad de las auditorías de logs también aumentó.
 - Revisar los datos se volvió más caro primero, y luego simplemente imposible.
- Automatizar el proceso de auditoría fue la solución lógica.

Firewall vs. Antivirus vs. IDS

- Comparten similitudes:
 - Por ejemplo, base de patrones de *mal comportamiento*.
- Difieren en:
 - Qué vigilan.
 - Cómo responden

Diferencias: qué vigilan?

- Firewalls: previenen conexiones o transmisión de paquetes que violen las reglas de la política de seguridad.
- Antivirus: buscan la presencia de ficheros (o con parte de contenido) pre-definidos y la ejecución de comandos “problemáticos”
- IDS: buscan comportamientos anómalos del sistema/red, examinando los medios de comunicación y las llamadas al sistema, ya sea usando base de patrones predefinidos o técnicas de profiling.

Diferencias: cómo reaccionan?

- Firewall: negar conexión o eliminar un paquete
- Antivirus: poner en cuarentena el fichero sospecho y avisar al usuario.
- IDS: notificar al administrador del sistema de la sospecha de una intrusión

Más activo



Menos activo

Firewall vs. Antivirus vs. IDS

- Sin embargo la frontera no está tan clara:
 - Por ejemplo, un buen IDS debería detectar la acción de un virus informático.
- Normalmente tienen solapes de funcionalidad.
- Mayor nivel de seguridad si usamos los tres.
 - Defensa en profundidad.
 - Cada uno tiene sus propias limitaciones.

Conceptos de la D.I.: Amenaza

- (Threat)
- Situación o evento con el potencial de dañar un sistema (propiedades CIA).
- La mayoría de los sistemas de seguridad están orientados a prevenir una amenaza.
- Más comunes: hackers, virus, incendio, inundación, rayos, etc.

Conceptos de la D.I.

- Arquitectura.
- Estrategia de monitorización.
- Tipo de análisis.
- Temporización.

Arquitectura

- La información para auditar debe ser almacenada y procesada fuera del sistema protegido.
 - Evitar que un intruso inhabilite el IDS borrando los registros de auditoría.
 - Evitar que un intruso modifique los resultados del detector de intrusiones para esconder su presencia.
 - Minimizar la pérdida de desempeño asociada con la ejecución del sistema de detección de instrucciones.
- El **host** vigila al **objetivo**.

Estrategias de monitorización

- Clasificación de acuerdo a la **fuentes de información**:
 - Monitores basados en el host.
 - Monitores basados en la red.
 - Monitores basados en aplicaciones
 - Monitores basados en el objetivo

Host-based IDS (HIDS)

- Recogen información de los sistemas internos de un ordenador (normalmente a nivel del S.O.)
 - Logs (audit trails) del S.O y del sistema, por ejemplo.
- Dependen del éxito de los intrusos:
 - Asume que dejarán rastros al intentar adueñarse del equipo.
 - El HIDS intenta detectar esas modificaciones y hacer un informe de sus conclusiones

Network-based IDS (NIDS)

- Se recoge información de paquetes.
- Normalmente usando dispositivos en modo promiscuo.

Otros dos

- Basado en aplicación: recogen información de aplicaciones en ejecución.
 - Por ejemplo logs de eventos y otras fuentes internas a la aplicación.
- Basados en el objetivo: estos monitores generan sus propios datos.
 - Usan funciones hash para controlar la modificación de objetos, y verificar si están de acuerdo a la política de seguridad.
 - En vez de actividades vigilan objetos.

Tipo de análisis

- El motor de análisis toma los datos de las fuentes y los examina buscando síntomas de ataques u otras violaciones a la política.
- La mayoría de los enfoques implican detección de malos usos, detección de anomalías o combinación de ambos.

Detección de malos usos

- Buscan por algo clasificado como “malo”.
 - Filtran flujos de eventos buscando patrones de actividad que coincidan con ataques conocidos u otras violaciones.
 - Utilizan técnicas de pattern-matching.
 - La mayoría de los actuales IDS comerciales utiliza esta técnica.

Detección de anomalías

- Buscan por algo raro o inusual.
- Analizan el flujo de eventos usando técnicas estadísticas para identificar actividades que parecen anormales (poco frecuentes).
- Este enfoque refleja la opinión de que intrusiones son un subconjunto de las actividades anormales.

Combinación de técnicas

- Significativas ventajas:
 - El análisis de anomalías protege contra ataques nuevos o desconocidos.
 - El análisis de malos usos previene que un adversario con mucha paciencia pueda gradualmente convertir un comportamiento raro en algo normal.

Temporización

- Modo batch (basado en intervalos):
 - Los datos se envían al motor de análisis en un fichero, abarcando eventos de un período determinado.
 - Los resultados son obtenidos **después** que la intrusión ha tenido lugar.
 - Modelo apropiado cuando el ancho de banda / capacidad de procesamiento no es suficiente para un análisis en tiempo real.

Temporización (ii)

- En tiempo real:
 - Los datos son enviados al motor de análisis a medida que los eventos ocurren (o con un pequeño retardo) y son procesados inmediatamente.
 - El proceso es suficientemente rápido para permitir que los resultados del análisis **afecten** el progreso o resultado final de cualquier intrusión que detecta.
 - Permite, llegado el caso, **respuesta automática**.

Objetivos

- Atribución (*accountability*):
 - Capacidad de atribuir responsabilidad de una actividad o evento a quien corresponda.
 - Normalmente para pedir compensación/responsabilidades -> ayuda que sea una persona (y no una máquina).
 - Más útil aún sería obtener direcciones físicas u otros enlaces al mundo físico.

Objetivos (ii)

- Respuesta:
 - Una respuesta ocurre cuando el análisis produce un resultado accionable.
 - No limitado a tomar represalias contra el atacante.
 - Ejemplos:
 - Registrar resultados de análisis (posterior informe).
 - Disparar alarmas de una variedad predefinida (mensaje en consola, SMSs, mails, etc).
 - Modificar la configuración del objetivo (x ej. firewall). → **IPS** (prevention)
 - Contra atacar.

Determinación de estrategia

- La estrategia óptima dependerá de factores como:
 - Nivel de criticidad o sensibilidad del sistema protegido.
 - La naturaleza del sistema (x ej, complejidad del hardware y plataformas de software).
 - La naturaleza de la política de seguridad de la organización.
 - El nivel de amenaza en el entorno donde el sistema es operado.

Ejemplos de IDS

- Snort
 - Pertenece a la categoría de NIDS.