

Sistemas de Detección de Intrusiones

Diego González Gómez

Julio, 2003

Índice de contenidos

- Definiciones
- Historia
- Clasificaciones
- Modelo de funcionamiento
- Casos especiales
- Aspectos legales
- Ventajas e inconvenientes
- Futuro
- Conclusiones

Definiciones

Definiciones

- **Intrusión:**
 - Conjunto de acciones que intentan comprometer la integridad, confidencialidad o disponibilidad de un recurso (Anderson, 1980).

- **Sistema de Detección de Intrusiones:**
 - Elemento que detecta, identifica y responde a actividades no autorizadas o anormales (Denning, 1987).

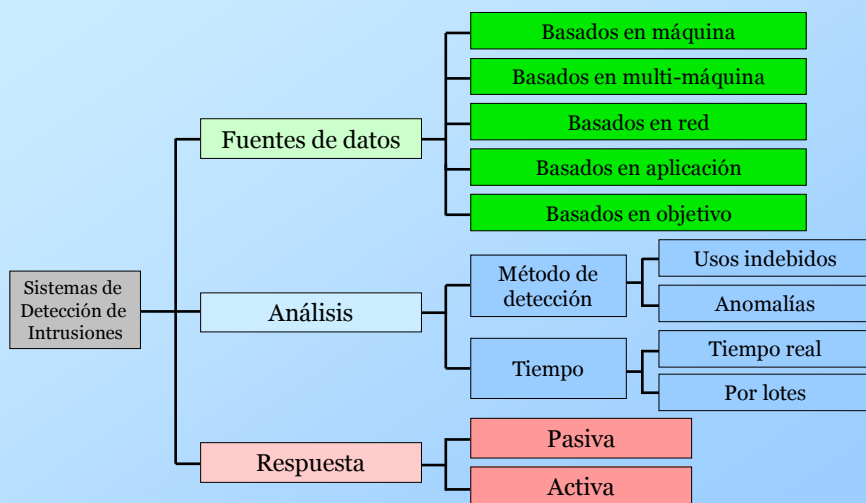
Historia

Historia

- **Años 50:**
 - La Bell Telephone System desarrolla el EDP (Procesamiento Electrónico de Datos) para realizar auditorías mediante ordenadores.
- **Años 70:**
 - El Departamento de Defensa de EEUU crea la Iniciativa de Seguridad, que define los requisitos de seguridad de los Sistemas de Confianza.
- **Años 80:**
 - James P. Anderson elabora el primer documento en que se habla sobre la detección de intrusiones.
 - Dorothy Denning y Peter Newmann desarrollan el IDES (Sistema Experto de Detección de Intrusiones).
 - Numerosas iniciativas en materia de detección de intrusiones: Haystack, MIDAS, NADIR, NSM, Wisdom and Sense, etc.
- **Años 90:**
 - Detección de intrusiones de red y primeros productos comerciales.

Clasificaciones

Clasificaciones

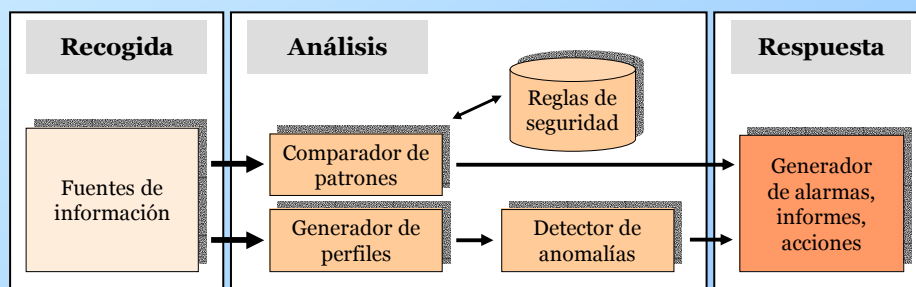


Modelo de funcionamiento

Modelo de funcionamiento General

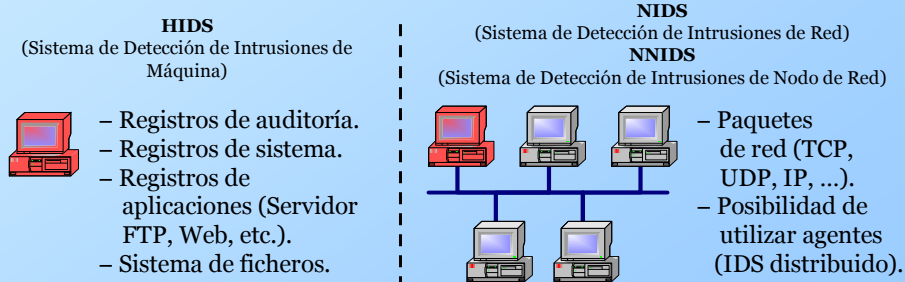
■ Tres fases:

- **Recogida de datos:** Registros de auditoría, de sistema, de aplicación, de sistema de ficheros, paquetes de red, etc.
- **Análisis:** de usos indebidos, de anomalías.
- **Respuesta:** pasiva, activa.

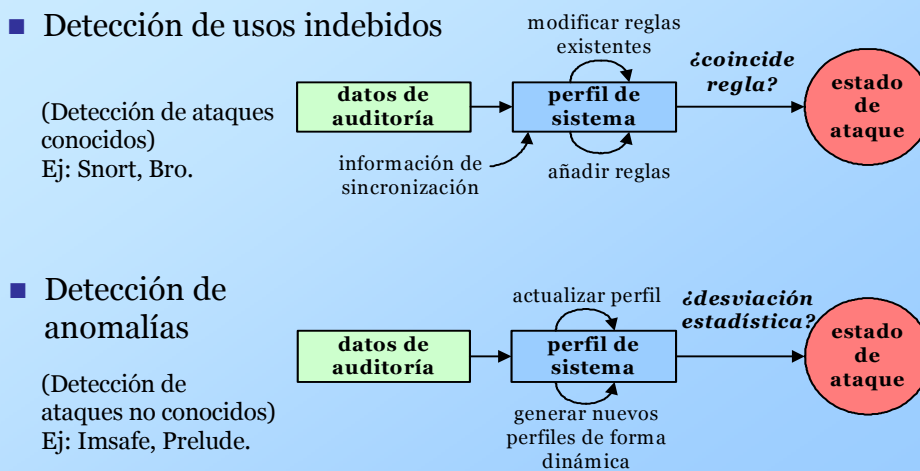


Modelo de funcionamiento Recogida de datos

- Basado en máquina, multi-máquina.
 - Basado en aplicación.
 - Basado en objetivo.
 - Basado en red.
- } Ej: Imsafe, GFI
LANguard S.E.L.M.,
Tripwire, Prelude.
- } Ej: Snort, Bro, Prelude.



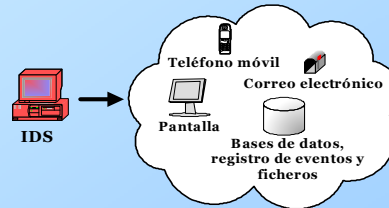
Modelo de funcionamiento Análisis



Modelo de funcionamiento Respuesta

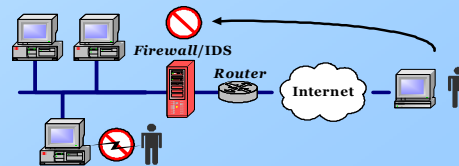
■ Respuesta pasiva

- Generación de eventos.
- Envío de alertas (correo electrónico, mensaje a móvil, etc.)



■ Respuesta activa

- Cierre de la sesión de usuario.
- Bloqueo de la conexión del intruso.



Casos especiales

Casos especiales

- Escáner de vulnerabilidades
 - Realizan comprobaciones de seguridad o ataques contra sistemas para encontrar fallos. Ej: SAINT, NÉSSUS, CIS (Cerberus Internet Scanner).
- *Honeypot* (Sistema trampa), *Honeynet* (Red Trampa)
 - Recursos cuyo valor reside en el uso no autorizado o ilícito de los mismos. Ej: Honeyd, BackOfficer Friendly, Specter.
- *Padded Cell* (Célula de aislamiento)
 - Sistema en que se redirige el tráfico no deseado a una “zona aislada”. Ej: Bait and Switch.

Casos especiales (2)

- Comprobadores de integridad
 - Herramientas que aplican algoritmos de cifrado, como funciones resumen, sobre ficheros para detectar cambios en los mismos. Ej: Tripwire.
- IPS (Sistemas de Prevención de Intrusiones)
 - Resultado de la combinación de IDS + cortafuegos.
 - Identifican el curso de un ataque y lo bloquean *antes* de que suceda. Ej: IntruShield, Hogwash, Radware, Storm watch.

Aspectos legales

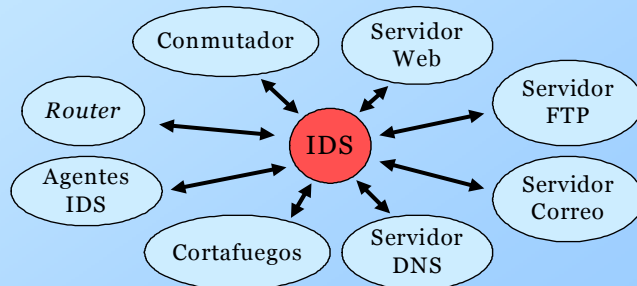
Aspectos legales

- **Europa:**
 - "Convenio sobre la Ciberdelincuencia" (21 de noviembre de 2001).
 - Define los delitos informáticos y elementos relacionados con éstos.
- **España:**
 - Código Penal español de 1995 (Ley Orgánica 10/1995, del 23 de Noviembre).
 - *Hacking* directo, mero acceso no consentido: El intruso sólo accede al sistema y sale, demostrando el fallo de seguridad del mismo, sin ánimo delictivo en esta conducta. Actualmente no castigado por el Código penal español.
 - *Hacking* indirecto: Acceso no consentido a un sistema o informática para cometer un delito. El acceso queda subsumido en el delito finalmente cometido (descubrir secretos de empresa, interceptar comunicaciones, producir daños, etc.).

Futuro

Futuro

- Mejoras
 - Falsos positivos
 - Estandarización (IDWG, CIDF)
 - Encriptación
 - Nuevos protocolos (IPv6, etc.)
 - Escalabilidad
 - Detección de anomalías
- Correlación, composición



Conclusiones

Conclusiones

- Tecnología en pleno desarrollo y evolución.
- Numerosos productos y trabajos.
- Prometedores resultados en experimentos con detección de anomalías, pero pocas soluciones aún de este tipo.
- Falta de acuerdos en cuanto a estándares.

Referencias y recursos

Referencias y recursos

- Productos
 - GFI LANguard S.E.L.M.
 - <http://www.gfi.com/lanselm/>
 - Imsafe
 - <http://imsafe.sf.net>
 - Prelude
 - <http://www.prelude-ids.org>
 - Snort
 - <http://www.snort.org>
 - Tripwire
 - <http://www.tripwiresecurity.com>
 - Nessus
 - <http://www.nessus.org>
- Portales de seguridad, vulnerabilidades, información sobre IDS
 - SANS Institute
 - <http://www.sans.org/rr/>
 - <http://www.sans.org/resources/idfaq/>
 - SecurityFocus
 - <http://www.securityfocus.com/ids>

Referencias y recursos (2)

- Normativa legal y entidades oficiales
 - Guardia Civil - Grupo de Delitos Telemáticos
 - <http://www.guardiacivil.org/ootelematicos/>
 - C.N.P. - Brigada de Investigación tecnológica
 - <http://www.mir.es/policia/bit/>
- Documentos
 - Bace, Rebecca, Peter Mell. ICSA Labs. *An Introduction to Intrusion Detection And Assessment*.
 - http://www.infidel.net/Articles/ICSA_Whitepaper.pdf
 - Ptacek, Thomas H. and T. N. *Insertions, Evasion, and Denial of Service: Eluding Network Intrusion Detection*. Enero, 1998.
 - <http://www.securityfocus.com/data/library/ids.ps>
 - Bace, Rebecca. *NIST Special Publication on Intrusion Detection Systems*. 1999.
 - <http://csrc.nist.gov/publications/nistpubs/800-31/sp800-31.pdf>
 - González, Diego. *Sistemas de Detección de Intrusiones*. Julio, 2003.
 - http://www.dgonzalez.net/secinf/ids/IDS_v1.o.pdf

Preguntas