# Detección de intrusiones de red: estado actual

Alvaro J. Fernández Lago,
S. Informática Complexo Hospitalario Xeral-Cíes de Vigo,
alago@unicies.cesga.es

**Introducción:** En este artículo realizaremos una clasificación general de los sistemas actuales de detección de intrusiones de red ("NIDS", en adelante), señalando a grosso modo sus principales capacidades operativas y defectos de diseño. Finalmente, se ofrecerán conclusiones y consejos sobre la implantación de los NIDS.

Con la expansión progresiva de Internet, la I+D para los NIDS y el mercado de productos disponibles ha experimentado en los últimos años un gran crecimiento [IDC][AberdeenGroup]; la mayor parte correspondiendo a los sistemas de detección de intrusiones a nivel de host, permaneciendo los NIDS en un segundo plano. Según lo anterior, podemos clasificar los IDS según: su fuente de datos; la técnica empleada en el análisis; y su arquitectura. En cuanto a las fuentes de datos; tenemos en el primer caso los registros de auditorías a nivel de host. Las tendencias actuales son: activar mecanismos de traza a nivel del sistema operativo y aplicaciones; registrar cambios en atributos del sistema de ficheros; monitorización de llamadas al sistema y procesos; uso de auditorías C2 [TCSEC] a bajo nivel; etc. En este campo existe una gran cantidad de productos – comerciales y gratuítos – disponibles; pero podemos resumirlos en los siguientes ejemplos: tripwire/swatch/logsurfer/procesado de auditorías C2 [ASAX]/herramientas especiales de gestión de configuración y listas específicas de comprobación de seguridad [DII-COE]; etc. para los sistemas Unix. Para los sistemas Windows: ITA Axent, STAT [Harris], ESM, Aelita; etc. La mayor parte de estos sistemas adolecen de los siguientes problemas de diseño: 1.- Salvo que se emplee cifrado fuerte [SK98], sus registros de auditoría pueden ser falseados 2.- Degradación del rendimiento del equipo si se pretende analizar la auditoría en tiempo real; 3.- El IDS debe ser actualizado frecuentemente para detectar nuevas variantes de intrusiones. Otra opción es utilizar los eventos de red. Aquí los NIDS en uso incluyen: el registro pasivo, almacenamiento y post-procesado de paquetes de red ("en bruto" o con pre-selección de protocolo/identificacion de nodo, puerto, etc.) que entran/salen de la red de la organización; agentes SNMP/RMON; reglas de filtrado en cortafuegos/routers que desencadenan auditorías en el equipamiento local o en una estación de gestión dedicada... Ejemplos: [NFR], [ISS], Cisco netflow/NetRanger/CBAC, Bro [Pax98], CIDER [NSWC98] etc. Los problemas actuales de estos sistemas son: 1.- Pueden ser engañados usando ciertas peculiaridades de los protocolos de red (ataques de "inserción y evasión" [PN98]) (NIDS que no defragmenten paquetes; no hagan "checksums"; no re-ensamblen los "flujos" TCP; no conserven el suficiente estado del "flujo" y consiguentemente puedan ser desincronizados y/o sometidos a ataques de denegación de servicio, etc.). 2.- Incapacidad de sostener capturas a alta velocidad (>100 Mbps); 3.- El uso de switches, que obliga a colocar el NIDS en el mismo segmento de los equipos; 4.- El uso creciente de comunicaciones cifradas (SSL, IPsec, PKIX) 5.- El uso de protocolos encapsulados a varios niveles (MPOA; DCOM/HTTP, CORBA, SMB, RPCs, etc.) añadiendo complejidad al análisis de las trazas. Respecto a la técnica empleada en el análisis, tenemos en primer lugar el "uso incorrecto". Éste busca patrones identificables ó firmas de ataques conocidos en los paquetes de red. Ejemplos: NFR (sistemas basados en libpcap); RealSecure de ISS, CyberCop (NAI), Dragon (NSW) N-gram (NSA), etc. Su problema: No se adaptan fácilmente a nuevos ataques, (como por ejemplo el "firewalking", "portscans" con paquetes ICMP distintos de ECHO, etc, etc.), ya que las firmas de los mismos varían. Otra técnica es la "detección de anomalías" (actividad que no se ajusta a un perfil normal). En estos casos, se establece de forma más o menos estática un patrón común de actividad; y se pasan a registrar las desviaciones sobre el mismo (Anzen Flight Jacket, DPEM [UC Davis], etc.). Sus problemas: 1.- No se adaptan con facilidad a nuevos patrones de uso; 2.-Necesitan gran cantidad de recursos (CPU/Disco/RAM) para mantener sus bases de conocimiento. Otra técnica es el análisis estadístico (SHADOW [NSWC], GrIDS (UC Davis), HayStack, etc.), usando series temporales, clustering, etc. Sus problemas: 1.- Su análisis es insensible a la ordenación de los eventos 2.- La determinación de umbrales de alarma se hace compleja. Otra técnica es la del "aprendizaje", que usa redes neuronales, redes de Petri, etc. para realimentar su base de conocimientos [JAM, etc]. Sus problemas: 1.- Gran cantidad de "falsos positivos" dada su alta sensibilidad; 2.- Dependen de que se les "entrene" adecuadamente; 3.- Escaso rendimiento para análisis en tiempo real. En cuanto a la arquitectura, aparte de la centralizada común, existen: La "distribuída", donde una estación central fusiona y correlaciona eventos provenientes de agentes locales. Ejemplos: OV ECS/NNM (HP), EMERALD (SRI), etc. Problemas: 1.- Correlación de eventos primitiva o poca reducción de los mismos, 2.- Ausencia de un estándar común [IETF CIDF] para la interoperabilidad entre varios productos. También tenemos la arquitectura de "agentes autónomos", cuyo máximo exponente en la actualidad es el AAFID2 [COAST]. Sus problemas: 1.- También están sujetos a la interceptación, salvo que se emplee cifrado y autentificación fuertes (Kerberos5, SASL, IPsec). Conclusiones: Los problemas principales hoy en día con los NIDS son: (A).- Su incapacidad para reducir el gigantesco número de "falsos positivos". (B).- No existen métricas adecuadas para su evaluación (C).- Están sujetos a ataques sofisticados (con herramientas de dominio público) [PN98] (D).- La presión del mercado hace que se

oferten IDS/NIDS de baja calidad de diseño, que quedan rápidamente obsoletos ante (C); (E).- Los IDS/NIDS presentan problemas cuando se pretenden emplear como "evidencia legal" ante ataques (logs falseados, fuentes de tiempo incorrectas, falta de colaboración entre proveedores de redes para trazar ataques, etc.) (F).- Los IDS/NIDS ponen de relieve las preocupaciones por la falta de privacidad (captura de paquetes, perfilado estadístico de los usuarios de la red, etc), agravado este hecho por la falta de legislación; y (G).- Existe la tendencia a emplear los IDS/NIDS en organizaciones que renuncian a emplear medidas de seguridad de host/red y/o implantar una política de seguridad formal (¿Pondríamos una alarma en una casa sin cerraduras?) Así pues, recomendamos la utilización de IDS/NIDS, pero bajo previa y exhaustiva evaluación; y sin olvidar que la inversión en detección de intrusiones no debe sustituir el establecimiento previo de medidas de seguridad adecuadas (de las aplicaciones, sistemas operativos, , routers, módems, etc. etc.)

**Bibliografía:** http://www.radium.ncsc.mil/tpep; http://www.nfr.net; http://www.ietf.org; http://www.cert.org; http://iss.net; http://coast.cs.purdue.edu; http://nswc.navy.mil; http://www.itu.ch; http://www.packetfactory.net; http://spider.dii.osfl.disa.mil/cm/dii41/; http://www.anzen.com/research/ndisbench/fragrouter.html