Identificación y análisis de la tecnología de detección y prevención de intrusiones

Por Javier y Gloria Areitio

Prof. Dr. Javier Areitio Bertolín – E. Mail: jareitio@eside.deusto.es
Catedrático de la Facultad de Ingeniería. ESIDE. Director del Grupo de Investigación Redes y Sistemas. Universidad de Deusto.
Prof. Dra. Gloria Areitio Bertolín – E. Mail: gloria.areitio@ehu.es
Laboratorio de Informática Aplicada. Universidad del País Vasco (UPV / EHU)

En el presente artículo se examina y analiza la tecnología de detección y prevención de intrusiones como componente clave de las medidas de protección en las redes y sistemas de computación (servidores, puestos de trabajo fijos y móviles, palm, PDAs, etc.). Se analizan los cortafuegos, los IDS, sus funciones, dimensions, métodos y arquitectura, sus limitaciones, sus capacidades, opciones de despliegue, motivos para utilizar la tecnología de detección de intrusiones, etc. Por último se examinan los motivos para utilizar esta tecnología.

La seguridad de un sistema de información abarca todas las dimensiones existentes a proteger: informática, telecomunicaciones, infraestructura-física, personal, organización-administración, información (datos, conocimientos, etc.), etc. Deberían estar muy claras las funciones (ó roles) y las responsabilidades de los usuarios, responsables de seguridad, administradores, etc. Un programa ó plan director de seguridad de la información debería incluir todos los aspectos de sensibilidad de la información corporativa, incluidos la confidencialidad, integridad y disponibilidad-accesibilidad.

Un programa-plan de concienciación en seguridad debería implantarse a todo el personal sobre los posibles riesgos y exposiciones y sus responsabilidades como sujetos de interacción y custodia de la información corporativa. La seguridad de un sistema de información se debe gestionar y administrar; la gestión es un proceso para el que no existen algoritmos mientras que donde existan algoritmos estará presente la administración.

Cortafuegos. Clasificación. IDS.

Los cortafuegos a veces implantados en routers sirven para controlar todo el tráfico entre una red protegida (ó intranet o red corporativa) y una red abierta no segura como Internet. Existen diversos tipos de cortafuegos (ó firewall):

Cortafuegos de filtrado de paquetes ó filtros de paquetes, controlan el tráfico de paquetes IP/TCP. Actúan de acuerdo a una política de seguridad en base a la información de la cabecera. No guardan el estado interno. La información accesible es: direcciones IP origen y destino, puertos TCP/UDP origen y destino, campo de opciones, bits ACK/SYN/FIN, campo tipo de protocolo (ICMP, TCP, etc.), etc.

Las ventajas de este tipo de cortafuegos son: fáciles y baratos de implementar, transparentes a los niveles superiores de protocolos, previenen algunos tipos de ataques "IP spoofing" y de router.

Los principales inconvenientes son: utilizan posiblemente direcciones IP y números de puerto falsos, el filtrado no es muy al detalle (por ejemplo, de acuerdo a los usuarios), especificación de las tabla de filtrado proclives al error (tablas grandes no leíbles, necesidad de herramientas).

Con un cortafuegos de filtrado de paquete si se bloquean segmentos TCP entrantes con el bit ACK a cero se impide que clientes externos realicen conexiones TCP con clientes internos, pero permite que clientes internos se conecten con el exterior. Así mismo, con un cortafuegos de filtrado de paquetes al bloquear datagramas entrantes y salientes con el campo protocolo igual a 17 y con el puerto origen o destino igual a 23 se bloquean todas las conexiones telnet y flujos UDP entrantes y salientes.

Iptables, es el nombre de la herramienta de línea de comandos con la cual los administradores de Linux crean reglas para el filtrado de paquetes y módulos NAT. Se utiliza para configurar, mantener e inspeccionar las reglas de cortafuegos IP del kernel de Linux; estas reglas se pueden dividir en cuatro categorías diferentes: la cadena de entrada IP, la cadena de salida IP, la cadena de reenvío IP y las cadenas definidas por el usuario. Se pueden definir varias tablas, que pueden contener cadenas nativas o definidas por el usuario, cada cadena es una lista de reglas que identifican a una serie de paquetes de red. Cada regla de la cadena especifica la acción a realizar con dicho paquete, la cual puede ser un salto a otra cadena definida por el usuario en la misma tabla. Una regla de cortafuegos especifica criterios para un paquete y un objetivo, si el paquete no concuerda se examina la siguiente regla de la cadena, si concuerda la siguiente regla se especifica por el valor del objetivo, que puede ser el nombre de una cadena definida por el usuario o

Figura 1. Ventajas e inconvenientes de los IDS de detección de anomalías y de detección de uso indebido.

IDS DE DETECCION DE ANOMALIAS

VENTAJAS

- DETECTA COMPORTAMIENTO ANOMALO Y POR TANTO TIENE LA CAPACIDAD DE DETECTAR SINTOMAS DE ATAQUES SIN EL CONOCIMIENTO ESPECIFICO DE LOS DETALLES.
- PUEDE PRODUCIR INFORMACION QUE PUEDE A SU VEZ UTILIZARSE PARA DEFINIR FIRMAS DE ATAQUE PARA IDS DE DETECCION DE USOS INDEBIDOS.

INCONVENIENTES

- PRODUCE UN GRAN NUMERO DE FALSAS ALARMAS (FALSOS POSITIVOS, SEÑALA QUE SI CUENDO ES QUE NO – FALSOS NEGATIVOS, SEÑALA QUE NO CUANDO ES QUE SI) .
- A MENUDO REQUIERE EXTENSOS "CONJUNTOS DE ENTRENAMIENTO" DE REGISTROS DE EVENTOS DEL SISTEMA PARA PODER CARACTERIZAR LOS PATRONES DE COMPORTAMIENTO NORMAL.

IDS DE DETECCION DE USOS INDEBIDOS

VENTAJAS

- MUY EFECTIVO PARA DETECTAR ATAQUES SIN GENERAR UN NUMERO ABRUMADOR DE FALSAS ALARMAS.
- PUEDE RAPIDA Y FIABLEMENTE DIAGNOSTICAR ELUSO DE UNA HERRAMIENTA O TECNICA DE ATAQUE ESPECIFICA.
- PERMITE A LOS ADMINISTRADORES DEL SISTEMA SEGUIR LA PISTA DE LOS PROBLEMAS DE SEGURIDAD EN SUS SISTEMAS, INICIANDO PROCEDIMIENTOS DE GESTIÓN DE INCIDENTES.

INCONVENIENTES

- SOLO PUEDE DETECTAR AQUELLOS ATAQUES QUE SE CONOCEN, POR TANTO DEBE CONSTANTEMENTE ACTUALIZARSE CON FIRMAS DE NUEVOS ATAQUES.
- ESTAN DISEÑADOS PARA UTILIZAR FIRMAS BIEN DEFINIDAS LO QUE IMPIDE DETECTAR VARIANTES DE ATAQUES COMUNES. DETECTORES DE UTILIZACION INDEBIDA BASADA EN ESTADO PUDEN SUPERAR ESTA LIMITACION, PERO NO SE UTILIZAN EN IDS ORDINARIOS.

uno de los valores especiales accept (dejar pasar el paquete), drop (rechazar el paquete), queue (pasar el paquete al espacio de usuario) ó return (detener esta cadena y examinar la siguiente regla de la cadena).

Las tablas en Iptables son:

- Filter. Es la tabla por defecto, contiene las cadenas predefinidas input (para paquetes de entrada), forward (para paquetes que serán en-rutados a través del equipo) y output (para paquetes generados localmente).
- NAT. Se consulta esta tabla cuando se encuentra un paquete que crea una nueva conexión, consta de tres cadenas predefinidas: prerouting (para alterar paquetes tan pronto lleguen), output (para alterar paquetes generados localmente) y postrouting (para alterar paquetes para la salida).
- Mangle. Se utiliza esta tabla para alterar paquetes especializados, hasta el kernel 2.4.17 tenía dos cadenas predefinidas: prerouting (para alterar paquetes de entrada antes de en-rutarlos) y output (para alterar paquetes generados localmente antes de en-rutarlos). Desde el kernel de Linux 2.4.18 se soportan tres cadenas predefinidas más: input (para paquetes de entrada), forward (para alterar paquetes que serán enrutados a través del equipo) y postrouting (para alterar paquetes para la salida). Por último en Iptables se utilizan diferentes opciones: de comandos (- A FORWARD, añade una o más reglas al final de una cadena, etc.), de parámetros (-p tcp especificación del protocolo, etc.), etc.

Cortafuegos de filtrado dinámico de paquetes ó "statefull inspection". La arquitectura de cortafuegos tipo "firewall" con inspección "statefull" operan en la capa de red (L3, Level-3), a diferencia de los cortafuegos de filtrado de paquetes que examinan un paquete IP en base a la información de la cabecera, los cortafuegos "statefull" siguen la pista de cada conexión que atraviesa todos los interfaces del cortafuegos y se asegura que sean válidas.

Un cortafuegos "statefull" puede examinar no sólo la información de la cabecera sino también los contenidos del paquete hasta la capa de aplicación para determinar más cosas acerca del paquete además de la información sobre su origen y destino IP. Un "cortafuegos de inspección statefull" también monitoriza el estado de la conexión y recopila la información en una tabla de estado. Debido a esto, las decisiones de filtrado no sólo se basan en reglas definidas por el administrador (como ocurre en los cortafuegos de filtrado estático de paquetes) sino también en el contexto que se ha establecido por medio de los paquetes anteriores que han pasado a través del cortafuegos.

Como medida de seguridad añadida contra el "escaneo de puertos" los "cortafuegos de inspección statefull" cierran los puertos hasta que sea pedida la conexión al puerto específico. La empresa CheckPoint utiliza esta arquitectura de cortafuegos en su modelo FireWall-1.

Pasarela de nivel de circuito, controlan el nivel de transporte, operan como cliente para el servidor y como servidor para el cliente (proxy – server). Proporcionan servicios genéricos proxy, disponen de estado interno y registran las actividades de los protocolos. Un ejemplo es "SOCKS Gateway", proporciona acceso socket vía "rconnect", "rlisten", "rbind" a través de la pasarela con autenticación.

Las ventajas que presentan los cortafuegos con arquitectura "pasarela de nivel de circuito": son independientes de las aplicaciones; permiten filtrado de conexiones existentes; incorporan autorización y "logging"; filtrado de posibles servicios UDP.

Los principales inconvenientes: no consideran la información específica de la aplicación; no pueden distinguir contenido http; es necesario la modificación de la aplicación.

Pasarelas del nivel de aplicación ó servidores proxy ó filtros del nivel de aplicación, operan en la capa de aplicación y pueden analizar datos de aplicación; existen "proxies estándar" totalmente construidos para los servicios de aplicación más típicos (http, ftp, smtp, etc.) y "proxies de servicio genérico" que permiten construir a medida proxies para protocolos menos conocidos como por ejemplo h.323, etc.

Los cortafuegos con arquitectura de filtro de aplicaciones operan sobre los servicios del nivel de aplicación. Por ejemplo "proxies estándar" para telnet, ftp, smtp, http, etc. que proporcionan conocimiento

IDS BASADO EN RED (NIDS)

VENTAJAS

- PUEDE MONITORIZAR GRANDES REDES.
- EL IMPACTO QUE INTRODUCE EN LA RED ES REDUCIDO DEBIDO A QUE ES UN DISPOSITIVO PASIVO.
- PUEDE HACERSE MUY SEGURO CONTRA ATAQUES E INCLUSO HACERSE INVISIBLE PARA MUCHOS ATACANTES UTILIZANDO HARDWARE (DE NIVEL 2 CON DIRECCIONES MAC) TIPO PUENTE Ó SWITCH.

INCONVENIENTES

- DIFICICULTAD PARA PROCESAR TODOS LOS PAQUETES EN UNA RED GRANDE O MUY CARGADA DE TRÁFICO.
- PUEDE FALLAR A LA HORA DE RECONOCER UN ATAQUE LANZADO DURANTE PERIODOS DE ELEVADO TRÁFICO.
- MUCHAS DE LAS VENTAJAS DE LOS NIDS NO SE APLICAN A LAS REDES MODERNAS BASADAS EN SWITCH (CON VLAN).
- NO PUEDE ANALIZAR NORMALMENTE INFORMACION CIFRADA.
- NO PUEDE DECIR SI UN ATAQUE A TENIDO O NO ÉXITO. SOLO PUEDE PERCIBIR QUE SE INICIO UN ATAQUE.
- TIENE PROBLEMAS AL TRATAR ATAQUES DE RED QUE UTILIZAN FRAGMENTACION DE PAQUETES.

IDS BASADO EN APLICACIÓN (AIDS)

VENTAJAS

- PUEDE MONITORIZAR LA INTERACCION ENTRE USUARIO Y APLICACIÓN, LO CUAL PERMITE SEGUIR LA PISTA DE ACTIVIDAD NO AUTORIZADA A USUARIOS INDIVIDUALES.
- NORMALMENTE PUEDE OPERAR EN ENTORNOS CIFRADOS YA QUE ESTABLECE INTERFAZ CON LA APLICACIÓN EN PUNTOS FINALES DE LA TRANSACCIÓN, DONDE LA INFORMACION SE PRESENTA A LOS USUARIOS NO CIFRADA.

INCONVENIENTES

- PUEDE SER MAS VULNERABLE QUE LOS HIDS A ATAQUES YA QUE LOS "LOG" DE LAS APLICACIONES DE LOS AIDS NO SE PROTEGEN TAN BIEN COMO LOS "REGISTROS DE AUDITORIA" DE LOS SISTEMAS OPERATIVOS UTILIZADOS POR LOS HIDS.
- NO PUEDE DETECTAR TROYANOS U OTROS ATAQUES DE ALTERACION DE SOFTWARE.
- ES ACONSEJABLE UTILIZAR UN AIDS EN COMBINACION CON UN HIDS Y/O UN NIDS.

Fig. 2.- Ventajas e inconvenientes de los IDS basados en red (NIDS) y de los IDS basados en aplicación (AIDS).

IDS BASADO EN HOST (HIDS)

VENTAJAS

- PUEDE MONITORIZAR EVENTOS LOCALES A UN HOST (Ó MAQUINA DE COMPUTACION), PUEDE DETECTAR ATAQUES QUE NO PUEDEN VERSE UTILIZANDO UN NIDS.
- FRECUENTEMENTE PUEDE OPERAR EN UN ENTORNO EN QUE EL TRAFICO DE RED ESTA CIFRADO, CUANDO LAS FUENTES DE INFORMACION BASADAS EN HOST SE GENERAN ANTES DE QUE LOS DATOS SE CIFREN Y/O DESPUES DE QUE LOS DATOS SE DESCIFREN EN EL HOST DESTINO.
- NO SE VE AFECTADO POR REDES CONMUTADAS (CON VLAN).
- CUANDO EL HIDS OPERA SOBRE "REGISTROS DE AUDITORIA" DEL SISTEMA OPERATIVO, PUEDE AYUDAR A DETECTAR TROYANOS U OTROS ATAQUES QUE IMPLIQUEN BRECHAS EN LA INTEGRIDAD DEL SOFTWARE (APARECEN COMO INCONSISTENCIAS EN LA EJECUCION DEL PROCESO).

INCONVENIENTES

- MAS DIFICIL DE GESTIONAR, YA QUE LA INFORMACION DEBE CONFIGURARSE Y GESTIONARSE PARA CADA HOST (Ó MAQUINA) MONITORIZADA.
- PUESTO QUE AL MENOS LAS FUENTES DE INFORMACION (Y A VECES PARTE DE LOS MOTORES DE ANALISIS) DEL HIDS RESIDEN EN EL HOST OBJETIVO DE LOS ATAQUES, EL HIDS PUEDE VERSE ATACADO E INHABILITADO COMO PARTE DE UN ATAQUE.
- NO ES MUY ADECUADO PARA DETECTAR ATAQUES DE EXPLORACION Y VIGILANCIA DE TODA LA RED YA QUE EL HIDS SOLO VE LOS PAQUETES DE RED RECIBIOS O EMITIDOS POR ESTE HOST.
- PUEDE INHABILITARSE POR CIERTOS ATAQUES DE DENEGACION DE SERVICIOS.
- CUANDO EL HIDS UTILIZA LOS "REGISTROS DE AUDITORIA" DEL SISTEMA OPERATIVO COMO FUENTE DE INFORMACION, LA CANTIDAD DE INFORMACION PUEDE SER INMENSA, LO QUE EXIGE ALMACENAMIENTO LOCAL ADICIONAL EN EL SISTEMA.
- UTILIZA RECURSOS DE COMPUTACION DE LOS HOST QUE MONITORIZA, POR TANTO CAUSA UN COSTO EN EL RENDIMIENTO DE LOS SISTEMAS MONITORIZADOS.

Figura 3. Ventajas e inconvenientes de los IDS basados en host (HIDS).

específico de la aplicación, por ejemplo, los "proxy ftp" conocen los comandos ftp, los "proxy http" saben sobre activeX, Javascript, Java, etc. Este tipo de cortafuegos posee estado interno y "logging".

Las ventajas que presentan los cortafuegos con arquitectura "filtro de aplicaciones": permiten autenticación y control sofisticados, por ejemplo generando perfiles, permiten crear contabilidad y registro de accesos para ofrecer dicha información a los IDS/IPS, posibilitan reglas de granularidad muy fina. Los principales inconvenientes: el filtrado es individual para cada servicio (eso implica que se necesita un proceso de automatización), se basa en niveles de protocolo inferiores que no son fiables.

En general, los cortafuegos son dispositivos del tipo mecanismos de seguridad que se concentran en un punto, en ellos se puede implantar políticas de seguridad de granularidad fina. Así mismo presentan características de registro (ó "logging") para crear perfiles. Como aspectos negativos: necesitan un mantenimiento continuo (los IDS se utilizan para re-configurarlos), presentan problemas con los túneles VPN (SSL sin cliente ó IPsec con clientes) y dispositivos móviles laptops, palms, etc. WiFi, WiMax, etc. La detección de intrusiones es el proceso de identificar y responder a todo tipo de actividad maliciosa dirigida a máquinas de computación, aplicaciones o recursos de red utilizando IDS (Sistemas de Detección de Intrusiones) e IPS (Sistemas de Prevención de Intrusiones).

Posibilidades e incapacidades de los cortafuegos.

Los cortafuegos pueden llevar a cabo algunas tareas, como por ejemplo:

- Sirven como foco para las decisiones de seguridad.
- Pueden hacer cumplir una política de seguridad, por ejemplo relativa al control de acceso.
- Pueden registrar la actividad de Internet de forma eficiente.
- Pueden limitar la exposición a los problemas de seguridad en una parte de una red.

Los cortafuegos son incapaces de realizar tareas como:

- No pueden proteger contra atacantes de dentro.
- No pueden proteger contra conexiones que no vayan a través de él, si por ejemplo existe un módem detrás de un cortafuegos que proporciona servicio PPP/SLIP/CSLIP para acceso a subred, el cortafuegos no puede proporcionar protección alguna contra tráfico malicioso procedente de usuarios conectados por llamadas telefónicas.
- No pueden proteger contra amenazas completamente nuevas.
- No pueden proteger completamente contra virus informáticos.
- No pueden autoconfigurarse correctamente, eso supone un coste de operación a tener en cuenta.

Enfoques fundamentales relativos a la política de un cortafuegos.

Básicamente existen dos enfoques totalmente opuestos:

- Estrategia de denegación por defecto. Consiste en que todo lo que no esta explícitamente permitido esta denegado. Examina los servicios necesitados por los usuarios de la red protegida. Considera las implicaciones de seguridad de estos servicios y de que forma estos servicios pueden proporcionarse de forma segura. Sólo permite aquellos servicios que pueden proporcionarse de forma segura y para los que existe una necesidad legítima. Deniega cualquier otro servicio.
- Estrategia de permiso por defecto. Consiste en que todo lo que no esta explícitamente prohibido está permitido. Permite todos los servicios que no se consideren peligrosos. Por ejemplo, NFS (Network File System) y X-Windows no se permiten a través del cortafuegos; o por ejemplo, las conexiones telnet entrantes sólo se permiten a una máquina específica.

Funciones, dimensión, metodos y arquitectura de los IDS.

Las funciones principales de un IDS son:

- Monitorizar. Se trata de examinar y procesar información acerca de las actividades del sistema (computadora, aplicación, red) a proteger.
- Generar informes. Se trata de generar información acerca del sistema monitorizado dentro de una infraestructura de seguridad del sistema.
- Responder. Se trata de reaccionar y responder a la intrusión detectada (por ejemplo, cerrando una co-

nexión TCP, bloqueando puertos TCP/UDP, avisando al administrador(es) de seguridad utilizando SMS/MMS, correo electrónico, buscapersonas, etc.

Las dimensiones de todo IDS son:

- Enfoque de análisis. La detección de firmas de ataque identifica patrones que corresponden a ataques conocidos. Los tipos de ataques deben ser conocidos anticipadamente, periódicamente debe existir una función de actualización por ejemplo a través de Internet que haga llegar las últimas firmas de ataque al IDS/IPS personal (basado en software) ó corporativo con plataforma hardware-software.
- Enfoque de detección de anomalías. Identifica formas de desviación no aceptables del comportamiento esperado, para ello utiliza "perfiles de comportamiento".

Un ejemplo son las técnicas de detección de anomalías en el funcionamiento de los protocolos TCP/IP. Los principales métodos utilizados por los IDS son:

- Procesamiento de registros de auditoria. El IDS examina los ficheros de "log", se opera de forma off-line, se examinan los eventos auditables, la información auditable en base a un proceso de auditoria; un ejemplo es el proceso de auditoria "syslog" de Unix.
- Procesamiento de información de red (NIDS, Network Intrusión Detection). Se monitoriza el tráfico de red en tiempo real, se sospecha de patrones específicos, como por ejemplo "/etc/passwd", se utilizan firmas de comportamientos anómalos o indebidos, se avisa antes de que el daño pueda ocurrir.
- Detección de anomalías. Se utilizan perfiles de comportamiento normal en base a capturar las expectativas acerca de las actividades de computación y red del usuario y del sistema. Se estima el perfil inicial, se hace un ajuste muy fino de los perfiles utilizando toda la información de la fuente.

Básicamente la arquitectura de todo IDS consta de los siguientes componentes:

- Sensor. Se encarga de proporcionar la información necesaria acerca del ente a proteger.
- Gestor del sistema. Se encarga de mantener el control sobre los componentes internos, la comunicación (cifrada) con y sobre el IDS.
- Motor de procesamiento. Se encarga de: reducir los datos irrelevantes, identificar las evidencias de intrusión claves, tomar la decisión sobre el tipo de respuesta a aplicar.
- Base de conocimientos. Se encarga de mantener los perfiles de los usuarios y datos y de las firmas de ataque.
- Archivo de auditoria. Se encarga de almacenar las actividades del sistema a proteger.
- Alarmas.
- Interfaz de usuario gráfico (GUI) de relación con los administradores de seguridad.

Limitaciones de los IDS.

Un IDS no puede realizar entre otras las siguientes funciones:

- Compensar la debilidad o pérdida de mecanismos de seguridad en la infraestructura de protección. Tales mecanismos son cortafuegos, mecanismos de identificación y autenticación, mecanismos de control de acceso, mecanismos de detección y limpieza de virus informáticos y código malicioso (troyanos, spyware, malware, adware, grayware, gusanos, etc.), mecanismos de cifrado de enlaces y túneles VPN, etc.
- Detectar, informar y responder de forma instantánea a un ataque cuando exista carga de procesamiento elevada en una máquina de computación o tráfico elevado en la red.
- Detectar ataques nuevos o variantes de los existentes de los que no se disponga de firma de ataque para comparar (los IDS necesitan actualizarse periódicamente con nuevas firmas de ataque).
- Responder de forma efectiva a ataques lanzados por atacantes muy sofisticados (por ejemplo con fragmentación muy retardada, etc.).
- Investigar automáticamente ataques sin intervención humana.
- Resistir a ataques muy sofisticados diseñados para sortear ó derrotar al IDS.
- Compensar los problemas relacionados con la fidelidad de las fuentes de información.
- Tratar de forma efectiva con redes conmutadas y configuraciones VLAN muy atípicas.

Tecnología IPS.

La tecnología IPS es una mejora de la tecnología IDS que puede bloquear y prevenir ataques que no hayan sido descubiertos a través de técnicas heurísticas, de detección de comportamientos, de detección de paquetes anómalos, etc. combinadas con las tradicionales firmas de los ataques reduciendo el número de falsos positivos y negativos. Trabajan en base a vulnerabilidades y no sólo sobre sus métodos de explotación. Los IPS pueden detectar que se esta explotando una

REGLAS:

EMISOR	RECEPTOR	PUERTO	PROTOCOLO	ACCION	RAZON
*	*	53	UDP	OK	Petición DNS
Externo	Interno	123	UDP	OK	Acceso NTP
*	*	69	UDP	NO	No TFTP
Externo	*	513	TCP	NO	No RLOGIN desde el exterior

Figura 4. Algunos elementos utilizados en las reglas de un cortafuegos de "filtrado de paquetes".

Figura 5. Conjunto de reglas de filtrado de paquetes de un cortafuegos

Regla	Sentido	Dirección origen	Dirección destino	Protocolo	Puerto origen	Puerto destino	ACK	Acción
A	Entrante	Externa	Interna	TCP	>1203	25	1 ó 0	Permitir
B	Saliente	Interna	Externa	TCP	25	>1203	1	Permitir
C	Saliente	Interna	Externa	TCP	>1203	25	1 ó 0	Permitir
D	Entrante	Externa	Interna	TCP	25	>1203	1	Permitir
E	Cualquiera	Cualquiera	Cualquiera	Cualquiera	Cualquiera	Cualquiera	1 ó 0	Denegar

A- Permite correos electrónicos entrantes
B- Permitir que salgan *reconocimientos* del puerto 25, poner bit ACK =1 para impedir que salgan nuevas conexiones TCP.
C y D- Similar para el correo saliente.
E- Deniega el resto del tráfico.
Nota: Cualquier regla de filtrado que permite paquetes TCP entrantes / salientes por conexiones salientes / entrantes debe exigir bit ACK = 1.

vulnerabilidad, por ejemplo de "buffer oveflow" sin importar en que aplicación o como lo hace el atacante. Incorporan una técnica "in-line" en la cual todo el tráfico pasa a través de dispositivos que eliminan los paquetes sospechosos sin necesidad de enviar por ejemplo paquetes RST (para resetear una conexión TCP) para tirar abajo la conexión establecida.

Capacidades complementarias de un IDS.

Algunas de las capacidades complementarias de un IDS son las siguientes:

Valoración de vulnerabilidades.

Sirven para determinar si una red o host es vulnerable a ataques conocidos y son en esencia "detectores de uso indebido" en modo batch que operan sobre el estado de seguridad de un sistema en un instante de tiempo concreto produciendo resultados a partir de las rutinas de comprobación especificadas.

Verificadores de integridad de ficheros.

Utilizan funciones criptográficas unidireccionales no lineales del tipo resumen (ó hash) del mensaje (por ejemplo MD5, SHA1, etc.) u otros ckecksum criptográficos (como MAC, Código de Autenticación de Mensajes; funciones lineales como el CRC no son lo suficientemente robustas), para ficheros y objetos críticos; se comparan con valores de referencia y se señalan las diferencias o cambios encontrados. Son muy valiosas para quienes realizan un examen forense de los sistemas que han sido atacados, ya que permiten un diagnóstico rápido y fiable de la "huella de un ataque-intrusión".

Honey-pots/honey-nets y padded-cells.

Los honey-pots son "sistemas de computación señuelo" que se encuentran diseñados para atraer a un potencial atacante lejos de los sistemas críticos, es decir desviar a dicho atacante del acceso a sistemas críticos, recoger información acerca de la actividad del atacante e incitarlo a permanecer en el sistema el tiempo suficiente para que los administradores puedan responder. Los honey-pots se encuentran llenos con información fabricada para que aparente ser valiosa pero a la que un usuario legítimo del sistema no debería acceder. Una honey-net es una generalización en forma de red de una honey-pot, es decir una "red señuelo" simulada para atraer a posibles atacantes y desviarles de los sistemas críticos de la organización así como para estudiar su modo de ataque, debe incluir trafico falso interno entre los sistema de computación señuelo para engañar al atacante e información sin valor pero con apariencia interesante; puede implementarse en uno o varios equipos. Un padded-cell más que intentar atraer a los atacantes con datos seductores, opera conjuntamente con un IDS tradicional y cuando este detecta algún atacante, lo transfiere de modo imperceptible a un "host padded-cell" especial. Una vez situado el atacante en el "padded-cell" se lo contiene dentro de un entorno simulado donde no pueda causar daño.

Puntos de vista en torno a un ataque-intrusion.

Definir lo que se considera un ataque (intrusión) es difícil ya que existen dos perspectivas o puntos de vista:

- El punto de vista del atacante se caracteriza normalmente por la intención y el riesgo de la exposición.
- El punto de vista ó perspectiva de la víctima se caracteriza por sus manifestaciones que pueden o no incluir daños.

Algunos ataques no producen manifestaciones y algunas manifestaciones aparentes son causadas por el malfuncionamiento de la red o los sistemas de computación. Algunos ataques implican la participación involuntaria de máquinas adicionales, normalmente victimas de ataques anteriores.

Para que ocurra una intrusión debe existir un acto abierto por parte de un atacante y una manifestación observable por parte de la víctima planeada que resulte de ese acto. Es posible crear taxonomías que organicen los ataques desde cada punto de vista. La visión de la víctima de un ataque normalmente se enfoca en manifestaciones como:

- ¿Qué sucedió?.
- ¿Quién es el afectado y de que forma?.
- ¿Quién es el intruso-atacante?.
- ¿Dónde y cuando se originó ?.
- ¿Cómo y por qué sucedió la intrusión?.

El atacante puede tener una visión bastante diferente:

- ¿Cuál es mi objetivo?.
- ¿Qué vulnerabilidades existen en el sistema objetivo?.
- ¿Qué daño u otras consecuencias son probables?.
- ¿Qué "scripts" de explotación u otras herramientas de ataque se encuentran disponibles?.
- ¿Cuál es mi riesgo de exposición?.

Problemas típicos de los IDS

Limitaciones para analizar grandes flujos de datos.- Comienzan los problemas con flujos de 1/10 Gbps e inferiores menos, dependiendo del número y tipo de funcionalidades simultáneas que active.

Limitaciones para poder analizar tráfico cifrado de red.- Especialmente los NIDS (Network IDS) no son capaces de descifrar tráfico y si el ataque se hace a través de SSL o una VPN puede pasar inadvertido y en algunos casos ni se alerta de ello.

Falsos negativos.- Existen causas (el IDS no tiene una regla para una nueva vulnerabilidad, o porque no es capaz de gestionar todo el tráfico, etc.) a veces se pierden opciones a la hora de descubrir un ataque y se pasa inadvertido.

Falsos positivos.- Se necesita una configuración muy personalizada y a medida para que el IDS no genere alertas que no corresponden a ataques reales.

Complejidad de la administración.- Es difícil la administración de los diferentes registros generados en toda la red y su correlación con la información almacenada en los IDS. Muchos administradores de red revisan los "log" como históricos al día siguiente dificultando o impidiendo una actuación eficaz.

Opciones de despliegue de NIDS

Existen muchas opciones a la hora de localizar IDS basados en red (ó NIDS) y situar sus sensores con diferentes ventajas asociadas a cada localización:

Detrás de cada cortafuegos externo, en la DMZ (Zona Desmilitarizada) de la red. Ventajas: (1) Ve los ataques que se originan desde el exterior y que penetran las defensas perimetrales de la red corporativa. (2) Pone de relieve los problemas con la política ó el rendimiento del cortafuegos de red. (3) Ve los ataques que pueden ser objetivo el servidor web, ftp, etc. que normalmente residen en esta DMZ. (4) Aunque el ataque entrante no sea reconocido, el NIDS puede reconocer el tráfico saliente que resulta de un servidor comprometido.

Fuera de un cortafuegos externo. Ventajas: (1) Documenta el número de ataques que se originan en Internet con destino a la red corporativa ó intranet. (2) Documenta los tipos de ataques que se originan en Internet con destino la red corporativa a proteger.

En troncales de red principales. Ventajas: (1) Monitoriza gran cantidad de tráfico de red, de modo que aumenta la posibilidad de observar ataques. (2) Detecta actividad por parte de usuarios no autorizados dentro del perímetro de seguridad de una organización.

En subredes (físicas ó VLAN con swithes) críticas. Ventajas: (1) Detecta ataques a sistemas críticos y recursos. (2) Permite enfocar la atención en recursos limitados para los activos de red considerados del máximo valor.

Motivos para utilizar tecnología ID.

El objetivo de la detección de intrusiones es caracterizar las manifestaciones de los ataques-intrusiones para poder identificar positivamente todos los ataques verdaderos sin identificar falsamente los "que no son ataques".

Los motivos de utilizar la tecnología de detección de intrusiones (ó ID) pueden ser muy variadas, por ejemplo: (1) Algunos usuarios pueden estar interesados en recoger información forense ("evidencias") para localizar y perseguir a los intrusos vía legal. (2) Para disparar acciones a la hora de proteger los recursos de computación. (3) Como diagnóstico para poder identificar y corregir vulnerabilidades, etc.

Un IDS adecuadamente desplegado proporciona avisos que indican que un sistema esta bajo ataque incluso aunque el sistema no sea vulnerable al ataque específico. Estos avisos pueden ayudar a los usuarios y administradores a alterar su postura de defensa de la instalación para aumentar la resistencia al ataque. Además un IDS puede servir para confirmar la configuración y operación segura de otros mecanismos como por ejemplo cortafuegos, anti-virus, anti-spideware, etc.

Este artículo se enmarca en las actividades desarrolladas dentro del proyecto *LEFIS-APTICE: Legal Framework for the Information Society II* (financiado por Socrates 2005. *European Commission*).

Bibliografía

- Areitio, J. y Areitio, G. "Identificación y análisis en torno a PKI". REE Nº 596/597. Julio/Agosto 2004.
- Areitio, J. y Areitio, G. "Análisis del control de acceso para la seguridad de TIC". REE. Nº 591. Febrero 2004.
- Areitio, J. "Determinación del ROSI elemento clave del análisis de riesgos de seguridad". REE. Nº 589.
- Douligeris & Serpanos "Network Security: Current Status and Future Directions. Wiley- IEEE Press. 2005.
- Cole, E., Krutz, R.L. and Conley, J. "Network Security Bible". John Wiley & Sons. 2005.