

## VIII Evento Internacional de Redes y Telecomunicaciones

### CITMATEL 2003

**Título:** Actualidad de la tecnología de detección de intrusos en las redes.

**Autor:** MSc. Walter Baluja García

Dpto. Telemática.CUJAE.

[walter@tesla.cujae.edu.cu](mailto:walter@tesla.cujae.edu.cu)

### RESUMEN

Desde hace más de una década los problemas de la seguridad en las redes de datos han preocupado a la comunidad internacional. Muchas han sido las soluciones halladas para mitigar esta dolencia inherente a las redes TCP/IP por sus características. Filtrado de paquetes, detección de intrusos, antivirus y otros se emplean de manera cotidiana, muchas veces en convivencia y para tranquilidad de los responsables de seguridad de las redes.

Actualmente, sin embargo, las redes de computadoras y sus problemas de seguridad tienen características que no son las mismas que 5 o 10 años atrás, situaciones que adicionan complejidad a las medidas o mecanismos de protección y a la labor del personal que se ocupa de estos menesteres.

En el presente trabajo se hace un análisis de las características actuales de las redes de datos y de los ataques a que son sometidas, aspectos que condicionan el empleo de nuevos y complejos mecanismos de defensa. Posteriormente se exponen los retos encontrados por la detección de intrusos para adaptarse a esta realidad.

Así también se explican las tendencias en el desarrollo de los IDS que le permiten mantenerse como la primera opción a la hora de asegurar las redes: operación distribuida y administración centralizada, homogeneidad en la información, empleo de técnicas de inteligencia artificial, uso de agentes móviles y otros.

## **Actualidad de la tecnología de detección de intrusos en las redes**

Desde hace más de una década los problemas de la seguridad en las redes de datos han preocupado a la comunidad internacional. Muchas han sido las soluciones halladas para mitigar esta dolencia inherente a las redes TCP/IP por sus características. Filtrado de paquetes, detección de intrusos, antivirus y otros se emplean de manera cotidiana, muchas veces en convivencia y para tranquilidad de los responsables de seguridad de las redes.

Actualmente, sin embargo, las redes de computadoras y sus problemas de seguridad tienen características que no son las mismas que 5 o 10 años atrás, situaciones que adicionan complejidad a las medidas o mecanismos de protección y al trabajo del personal que se ocupa de estos menesteres. En síntesis podemos mencionar algunas:

- *Diversidad, fuerza y profundidad de los ataques.* Los ataques tienen características disímiles. Persisten en su efectividad ataques de denegación de servicios como el syn flooding, smurf y otros. Cobran fuerza los ataques distribuidos, los ataques a sitios web y a sus bases de datos. La mayor parte de los ataques reflejan un gran conocimiento de las características y debilidades de los sistemas sin que sea sinónimo de gran conocimiento por parte de los atacantes.
- *Cada vez más computadoras que proteger.* Las redes de computadoras son muy grandes. Cada empresa, universidad o entidad, posee una red que llega a todos los rincones de la misma y que es utilizada por la mayor parte del personal correspondiente. Esto multiplica el número de posibles puntos vulnerables, intrusos y otros. Así mismo crece el número de servidores y la cantidad y variedad de servicios que estos ofrecen.
- *Numerosos y veloces enlaces a otras redes.* Las posibilidades de acceso a otras redes son inmensas. Las soluciones de acceso telefónico enlaces a Internet, conexiones a redes experimentales, corporativas o con otros fines son muy comunes. Esto hace crecer el número de puntos de acceso a una red y por tanto la complejidad de control del flujo de información en cada acceso.

- Distribución de gran cantidad de puntos a proteger por toda la red. Son decenas y hasta cientos las computadoras cuya protección se hace indispensable en cada lugar. La información sensible de cada entidad y los servicios de la misma se hayan dispersos en diferentes segmentos de red por diferentes causas.
- Redes corporativas. Es muy común que cada empresa o entidad tenga una red nacional o regional. Esto permite potenciar el trabajo evitando gastos de transporte y de otros medios de comunicación. Por lo tanto existen numerosos enlaces de alta velocidad y gran cantidad de servidores a proteger ubicados en una especie de backbone controlado por la empresa.

### **Los Sistemas Detectores de Intrusos**

De manera general puede afirmarse que los sistemas detectores de intrusos (IDS) son herramientas con cierta inteligencia que automatizan la detección de intentos de intrusión en una red de computadoras. Esta identificación puede resultar inmediata o en un plazo de tiempo muy corto. Es por eso que en muchas ocasiones se emplea el término de *tiempo real*. [2]

Dentro de la gran familia de IDS se presentan dos grandes grupos partiendo de la base informativa de su trabajo: los sistemas basados en normas y los sistemas adaptables.

Los primeros actúan a partir de bases de datos que contienen todos los patrones de ataques conocidos hasta el momento de salida del producto. Estas bases deben ser actualizadas de manera periódica, para que la herramienta se mantenga cumpliendo sus objetivos. No hacer esto puede traer como consecuencia que cualquier nuevo ataque, por simple que sea, tenga éxito en sus intenciones de penetrar o alterar el funcionamiento de la red.

En el caso de los sistemas adaptables se trata de incorporar técnicas avanzadas, como la inteligencia artificial, para reconocer y aprender nuevos patrones de ataques. Este grupo de herramientas presupone una mayor complejidad, por lo que su desarrollo se observa, esencialmente, en entornos de investigación.

### **¿Qué puede hacer un IDS?**

Debe adelantarse a cualquier comentario que estas herramientas no constituyen la solución a todos los problemas de seguridad de la red. Los IDS introducen novedosos

métodos de trabajo permitiendo establecer la llamada defensa en profundidad y complementando el trabajo realizado por soluciones ya establecidas y maduras como los cortafuegos. Abajo se relacionan algunas de sus posibilidades:

- Detectar ataques en el momento que está ocurriendo o poco tiempo después de haber ocurrido.
- Automatizar la búsqueda de nuevos patrones de ataque (principalmente, modificaciones de ataques conocidos) gracias a las herramientas estadísticas de búsqueda, y al análisis de tráfico anómalo.
- Monitorización y análisis de las actividades de los usuarios. De esta forma se puede saber los servicios que usan los usuarios, e incluso estudiar el contenido de este tráfico, en busca de elementos anómalos.
- Auditoría de configuraciones y vulnerabilidades de determinados sistemas. Mediante el análisis de tráfico y de logs pueden descubrirse sistemas que tienen servicios habilitados cuando en realidad no deberían tenerlos.
- Análisis de comportamiento anormal. Si se detecta una conexión fuera de hora, reintentos de conexión fallidos y otros, existe la posibilidad que se esté en presencia de una intrusión. Un análisis detallado del tráfico y los logs puede revelar una máquina comprometida o un usuario con su contraseña al descubierto.
- Disminuye la complejidad de las tareas de administración de la seguridad en la red. Se automatizan tareas como la actualización de reglas, la obtención y análisis de logs, la reconfiguración de cortafuegos y otros.

### **Características de las herramientas**

Para enfrentar el estado beligerante existente en las redes la comunidad de expertos en seguridad ha trabajado intensamente ofreciendo soluciones a manera de estrategias,

herramientas y mecanismos variados. Sigue sin existir la herramienta única que resuelve todo los problemas mientras, ese protagonismo recae en el personal que administra la seguridad de la red. Las herramientas detectoras de intrusos poseen tres características específicas que a continuación se enumeran:

- Balance entre complejidad en la administración y potencialidad de la herramienta. En muchos casos resulta compleja la instalación, puesta en marcha y configuración de los programas, incluso para especialistas. Este problema se multiplica, salvo algunas excepciones, por la cantidad de herramientas a utilizar. Cuando se está ante una herramienta de grandes posibilidades de detección, configuración y otros, se necesita gran conocimiento y tiempo para poder configurarla.
- Costo elevado. Una buena parte de las herramientas de seguridad, sobre todo en plataformas Microsoft son comerciales. A partir de necesitar varias herramientas y sus licencias, la inversión crece.
- Falta de integración de las herramientas. No existen soluciones de software y/o hardware que provean de soluciones integrales. Cada herramienta de seguridad funciona de manera independiente. Son pocos los casos, normalmente solo los de un mismo fabricante, que utilizan bases comunes o trabajan en modo coordinado. Más aún si de soluciones libres se trata.

## **Retos**

Resulta evidente entonces que la comunidad que fabrica, desarrolla e investiga tiene ante sí grandes retos. De manera general se considera que las generaciones actuales de IDS emplean un número limitado de técnicas para detectar intrusiones y por el contrario los intrusos cada vez amplían sus habilidades y hasta incluyen formas de obligar al IDS a mal funcionar.

Los retos que hoy enfrentan estas herramientas pueden resumirse como sigue:

*Automatización y Sofisticación de los ataques:* La mayor parte de los ataques pueden ser realizados utilizando herramientas programadas para ese fin. Esto aumenta

potencialmente el número de intrusos y la rapidez de ejecución del ataque. Se ejecutan varias tareas que atacan las principales funcionalidades de los sistemas y aprovechan bien todas las debilidades del mismo. También es muy común el empleo de numerosos puntos esparcidos por toda la red para atacar un determinado objetivo, logrando una mayor potencia, velocidad e impersonalidad. Esto último se conoce como ataque distribuido.

*Descubrimiento veloz de las vulnerabilidades:* La detección de nuevas vulnerabilidades se hace mucho más rápido en la actualidad. Hoy día son muchos más los internautas capacitados para descubrir fallos en los sistemas que usan, hay muchos “aficionados” a estudiar las fuentes o hacerle pruebas críticas a los mismos (algo que generalmente no se cumple en las últimas etapas de la producción del software que se expide mundialmente). Además, existen todas las facilidades para difundir rápidamente la vulnerabilidad, con buenas o malas intenciones.

*Incremento de ataques a la infraestructura:* Los intrusos son más capaces y conocen en detalle cual es el funcionamiento de Internet. Lanzan ataques a puntos cruciales de la infraestructura como son los servidores de nombres (DNS) y servidores de mensajería. Esto incluye los ataques a los propios IDS.

*Empleo de cifrado para ocultar información de ataques.* Descifrar la paquetería que es analizada por los IDS es demasiado costoso a partir del total desconocimiento de los algoritmos y llaves usadas. Esto hace que la detección del ataque tenga que hacerse en el destino del mismo, una vez que se llevó a cabo.

*Aumento del tráfico y los servicios en las redes.* Los IDS de red tienen que operar a velocidades y con eficiencia extrema dado el enorme aumento de las velocidades en entornos locales y amplios. Aquellos que basan su funcionamiento en el análisis de logs necesitan estar preparados para procesar gran cantidad de datos de fuentes heterogéneas.

*Operación en entornos de alta automatización de tareas.* Los propios IDS tienen la automatización como una de sus ventajas. En estos casos suelen cometerse errores en

la ejecución de respuestas automáticas. Además, se producen muchos falsos positivos y negativos.

### **Tendencias en el trabajo de desarrollo**

El trabajo de fabricantes, desarrolladores e investigadores está matizado por la búsqueda de respuesta a todos los retos planteados y a las necesidades de las redes de todo el planeta. Hay líneas en las que se trabaja con prioridad y ya se observan los primeros resultados [6]:

- Integrar la información proveniente de diferentes sensores. Emplean esta facilidad para evitar los falsos positivos y negativos.
- Mejorar las posibilidades de capturar información útil para el trabajo forense.
- Ampliar las posibilidades de detector código maligno. (adjuntos de correo, Java, ActiveX).
- Desarrollar facilidades para la detección de ataques DoS (Denial of Services), ataques distribuidos y otros.
- Identificar nuevas formas de ataques. Aprender a través de mecanismos como las redes neuronales y los algoritmos genéticos.

Estas líneas de trabajo representan la respuesta de los IDS a los retos expuestos. En gran parte de los casos se requiere la aplicación de las técnicas más novedosas en el procesamiento y recolección de la información, la programación y otros. Se trata, además, de minimizar la intervención del ser humano en el accionar del IDS.

### **Soluciones encontradas**

Trabajando en las líneas definidas y reconociendo las características de las redes de datos de la actualidad, se han ido encontrando algunas respuestas que satisfacen en gran medida las necesidades existentes. Los IDS que hoy se desarrollan se

caracterizan por contar con funcionamiento distribuido y la aplicación de novedosas técnicas:

- *Operación distribuida.* Debido a la cantidad y, en muchos casos la dispersión de los puntos a proteger, una misma herramienta debe estar funcionando en varias computadoras al mismo tiempo. Normalmente esto se ha resuelto instalando el o los programas en cada lugar y esto significa repetir bases, reportes, configuración y multiplicar los esfuerzos de administración. A lo que se refiere es a compartir las bases de datos y configuración, a la utilización de datos de cada punto para confeccionar reportes y tomar decisiones.

- *Administración centralizada.* Concentrar todo el esfuerzo de administración en un solo lugar. Desde allí se configura, actualiza, analiza el funcionamiento, se estudian los reportes y se toman decisiones. De esta forma, se pueden recoger los datos y las alarmas en un único lugar. La comunicación entre las estaciones vigilantes y la estación de control debe ser segura, o de lo contrario se pone en peligro toda la infraestructura de seguridad.

En esta línea, el IETF está trabajando en un estándar para la comunicación de alarmas proveniente de los IDS (IDWG, Intrusion Detection Working Group), basado en XML (para especificar el contenido) y HTTP (para transportarlo). Puede encontrarse información en <http://www.ietf.org/html.charters/idwg-charter.html>. En el año 2001 este grupo publicó los Internet Draft: The Intrusion Detection Exchange Protocol (IDXP) y Intrusion Detection Message Exchange Format Data Model and Extensible Markup Language (XML).

Por otro lado, existe otro proyecto paralelo, desarrollado por el DARPA, para comunicar sus IDS, llamado CIDEF (Common Intrusion Detection Framework), que se basaba en un formato similar a Lisp. Se puede encontrar información en <http://www.gidos.org/>.

- *Fusión de datos de diferentes sensores* [3]. En ambientes de funcionamiento distribuido se requiere la recolección y análisis de datos en un solo punto central, comúnmente desde donde se administra el sistema. A partir de este trabajo se evalúan situaciones, se toman decisiones y se ejecutan tareas. La aplicación de

la fusión de datos requiere de algoritmos matemáticos y heurísticos, inteligencia artificial, reconocimiento de patrones y otros.

- *Minería de datos*. Con este trabajo se filtra, transforma y organizan extensos volúmenes de información que se obtienen mediante la recolección. Permite reconocer nuevos patrones de ataques y nuevos ataques en sí.
- *Redes Neuronales* [4]. Básicamente una red neuronal es un proceso estadístico que pretende emular los procesos mentales. En los IDS, se pueden usar para decidir si un paquete o un grupo de estos constituyen un ataque o no. Conseguir preparar la red de forma adecuada es una tarea difícil. Estas redes se “entrenan” con paquetes normales capturados de la red donde se va a instalar. Lamentablemente no existe un procedimiento adecuado de automatización del diseño, por lo que se requiere que un experto supervise la elección de parámetros y realice muchas pruebas para buscar el diseño que ofrece un rendimiento óptimo. Un cambio significativo en la red (por ejemplo, la aparición de tráfico nuevo) puede producir multitud de falsos positivos. Además, la actualización del IDS es complicada. Esta técnica, aunque carece de elementos que automaticen su configuración, entrenamiento y otros, se perfila como uno de los grandes motores que impulsará la adaptabilidad de los IDS.
- *Agentes Móviles* [5]. El empleo de agentes móviles ofrece una gran cantidad de posibilidades: disminución de la carga o el tráfico en la red en entornos de trabajo distribuido, independencia de plataforma, adaptación y configuración dinámica, escalabilidad y otros. Representa un cambio radical en el modo de ejecutar algunas tareas.

### **Facilidades de operación**

Hoy los IDS ofrecen diferentes facilidades que les permite adaptarse al entorno de trabajo de las redes de computadoras. La aplicación de las técnicas expuestas arriba les permite desarrollar un trabajo más completo a la hora de detectar intrusiones.

El hecho de analizar los datos de todos los nodos en un punto común permite obtener conclusiones imposibles de alcanzar con los análisis independientes que se puedan realizar en cada nodo. Para que esta labor sea realmente efectiva deben emplearse las técnicas mencionadas: agentes móviles, fusión y minería de datos, redes neuronales y otros. Este examen permite:

- *Detectar ataques simultáneos.* Se puede obtener a partir de la detección de incidencias con una misma dirección ip que se efectúan en cercanos en el tiempo. Si las incidencias son representativas de un mismo tipo de ataque hay gran certeza.
- *Detectar reconocimientos.* Esto es muy importante ya que estos reconocimientos son, en un alto por ciento de las veces, la antesala de un ataque. Dentro de este caso se encuentra la detección de vulnerabilidades para encontrar un punto vulnerable por donde penetrar el sistema.
- *Detectar de ataques distribuidos.* Cuando el ataque tiene los mismos patrones y se registra desde varias direcciones ip diferentes. Este pudiera ser un ataque desde una sola fuente que emplea *spoofing ip*.
- *Ejecutar reacciones defensivas globales.* A partir de los análisis en los nodos se puede filtrar las direcciones origen de los ataques. Mediante el análisis central puede filtrarse bloques de direcciones en los nodos a partir de reconocer ataques distribuidos o filtrar anticipadamente una dirección ip que aún no ha atacado alguno de los puntos protegidos. También puede filtrarse en un punto que proteja todos los nodos en lugar de en cada nodo particular si se estima que el ataque se va a extender o se ha extendido a varios nodos.

## **Conclusiones**

La tecnología de detección de intrusiones es joven y tiene grandes retos ante sí. Aunque desde hace muchos años se habla de IDS hace muy pocos se ha logrado disponer de herramientas capaces de responder a las expectativas de la comunidad internacional.

En las redes actuales el trabajo de los IDS se dificulta debido al enorme número de usuarios, nodos y servicios en red. Puede hablarse de un medio hostil en el que los detectores de intrusos tienen que aplicar las técnicas más modernas para poder cumplir su misión.

Hoy se empiezan a dar los primeros pasos para convertir realmente a los IDS en sistemas inteligentes, que puedan prescindir de la intervención del hombre para prevenir, detectar y eliminar los ataques en la red.

### **Bibliografía**

- [1]. Ant, Allan, "Intrusion Detection Systems (IDSs): Perspective". 2002.
- [2]. Baluja, Walter, "Acercamiento a los sistemas detectores de intrusos." Telem@tica Revista Digital de las Tecnologías de la Información y las Comunicaciones, Año I No. 2 ISSN: 1729-3804. 2001.
- [3]. Bass, Tim, "Intrusion detection systems and multisensor data fusion", Communications of the acm, April 2000/Vol. 43, No. 4.
- [4]. Díaz Vizcaíno, Luis Miguel, "Sistemas de Detección de Intrusos", Universidad Carlos III de Madrid. 2002.
- [5]. Krugel, Christopher, Toth Thomas, "Applying Mobile Agent Technology to Intrusion Detection", Distributed Systems Group Technical University Vienna. 2001.
- [6]. Networked Systems Survivability Program, "State of the Practice of Intrusion Detection Technologies". CERT. January 2000.