UDLAP®

Fuente: Academia, UDLAP

Fecha: 6 de octubre, 2015.

¿Cómo detectar intrusos en Internet?

Autor: Dr. Vicente Alarcón Aquino, Director Académico Computación, Electrónica y Mecatrónica, UDLAP.

La aparición en los últimos años de las redes informáticas y fundamentalmente del Internet ha sido el factor principal que ha hecho que la seguridad informática sea transcendental en el uso de sistemas informáticos. Desde el momento en que una computadora se conecta a Internet, se abren ante los usuarios toda una nueva serie de posibilidades; sin embargo, éstas traen consigo toda una serie de nuevos y, en ocasiones complejos tipos de ataque o intrusiones. Dichos ataques pueden ser caracterizados como anomalías en el comportamiento usual del flujo de datos en dicha red de comunicaciones. Un sistema de detección de intrusos (o IDS por sus siglas en inglés, Intruder Detection System) es una herramienta de seguridad encargada de monitorear los eventos que ocurren en un sistema informático en busca de intentos de intrusión. Se define intento de intrusión como cualquier intento de comprometer la confidencialidad, integridad, disponibilidad o evitar los mecanismos de seguridad de una computadora o red. Las intrusiones se pueden producir de varias formas: atacantes que acceden a los sistemas desde el Internet, usuarios autorizados del sistema que intentan ganar privilegios adicionales para los cuales no están autorizados y usuarios autorizados que hacen un mal uso de los privilegios que se les han asignado.

Un IDS recolecta y analiza información procedente de distintas áreas de una red de comunicaciones con el objetivo de identificar posibles fallos de seguridad. Este análisis en busca de intrusiones incluye tanto los posibles ataques externos como los internos. Debido a que la seguridad de una red de comunicaciones es vulnerable a ataques e intrusión, y el uso de Firewalls (un firewall es un dispositivo que permite o deniega las transmisiones de una red a la otra. Un uso típico es situarlo entre una red local y la red Internet como dispositivo de seguridad para evitar que los intrusos puedan acceder a información confidencial) ya no es suficiente para frenar este fenómeno, es por ello que se ha optado por el uso de sistemas capaces de observar y analizar el tráfico en una red de comunicaciones para la detección de intrusos. La detección de intrusiones permite a las organizaciones proteger sus sistemas de las amenazas que aparecen al incrementar la conectividad en red y la dependencia que tenemos hacia los sistemas de información. Los IDS han ganado aceptación como una pieza fundamental en la infraestructura de seguridad de una organización.

Para diseñar un IDS existen dos tipos de técnicas: la basada en detección de anomalías y la basada en patrones (o firmas). La técnica basada en patrones tiene la limitante de que

únicamente puede ser capaz de detectar ataques conocidos y es la técnica usada por la mayoría de sistemas comerciales. Las firmas utilizadas en estos IDS usualmente son simples patrones que permiten detectar ataques previamente registrados. Mientras que la técnica basada en detección de anomalías, utilizada de forma limitada por un pequeño número de IDS, se centra en identificar comportamientos inusuales en una computadora o una red y funcionan asumiendo que los ataques son diferentes a la actividad normal. Esto es, la detección de anomalías permite detectar ataques nuevos y totalmente desconocidos. Los IDS basados en detección de anomalías detectan comportamientos inusuales y de esta forma tienen la capacidad de detectar ataques para los cuales no tienen un conocimiento específico. Los resultados generados por los IDS basados en la detección de anomalías pueden producir información que puede ser utilizada para definir firmas en la detección basada en patrones. En el campo de detección de anomalías se han desarrollado distintos diseños que permiten trabajar de manera eficiente [1-3]; sin embargo, aún no se ha alcanzado un estado definitivo en el cual la detección de intrusos se lleve a cabo de forma confiable. Para mejorar el nivel de confiabilidad de la detección se pueden colocar varios IDS en diferentes puntos de la red con el fin de combinar la información y reducir el número de falsas alarmas.

Referencias

1. V. Alarcon-Aquino, J. M. Ramirez-Cortes, P. Gomez-Gil, O. Starostenko, Y. Garcia-Gonzalez, Network Intrusion Detection Using Self-Recurrent Wavelet Neural Networks with Multidimensional Radial Wavelons, in Information Technology and Control, Vol. 43, No. 4, December 2014; pp. 347-358 [pdf]

2. V. Alarcon-Aquino, P. Gomez-Gil, J.M. Ramirez-Cortes, Design of an Intruder Detection System Using Neural Networks, Chapter in Don't Be Mocked, Secure Your System E-Book, Edited by Ewa Dudzic, Ed. Hakin9 Media 02-682 Warszawa, Poland. Pages: 75-86, October 2012 [pdf]

3. V. Alarcon-Aquino, J. A. Barria, Anomaly Detection in Communication Networks Using Wavelets, IEE Proceedings-Communications, Vol.148, No.6; December 2001; pp. 355-362 [pdf]

Tags: Computación, Dr. Vicente Alarcón Aquino, Electrónica y Mecatrónica, Firewalls, redes informáticas, seguridad informática, sistema de detección de intrusos, técnica basada en detección de anomalías, técnica basada en patrones, VAC

Acerca del autor: Doctor en Ingeniería Eléctrica y Electrónica por el Imperial College London, en Londres Inglaterra. Durante su trayectoria profesional se ha desempeñado como profesor del Departamento de electrónica de la Universidad de las Américas Puebla; de 1998 al 2001 participó como Instructor en el Laboratorio de comunicaciones y procesamiento de señales y como asistente de investigación en el Departamento de eléctrica y electrónica del Imperial College London en un proyecto apoyado por la Comisión Europea FP7; en el verano del 2017 realizó una

estancia de investigación en el Departamento de informática en King´s College London; igualmente, ha formado parte de múltiples comisiones de evaluación en PNPC, FOMIX y becas al extranjero, colaborado en diversos proyectos de investigación apoyados por el CONACYT y evaluado proyectos de innovación, de infraestructura y de ciencia básica sometidos al mismo organismo. El Dr. Alarcón es fundador y director desde enero 2010 del Laboratorio de comunicaciones y procesamiento de señales con apoyo de dos proyectos de investigación FOMIX-CONACYT. El Dr. Alarcón es Senior Member del IEEE desde el 2014, Miembro de la Academia Mexicana de Ciencias desde el 2012 y pertenece al Nivel 1 del Sistema Nacional de Investigadores, donde ingresó desde el 2004. Actualmente es profesor de tiempo completo y Director Académico del Departamento de Computación, Electrónica y Mecatrónica de la Universidad de las Américas Puebla, donde ha dirigido 55 tesis de licenciatura, 15 de maestría y 4 de doctorado. Ha participado de manera sistemática como revisor de artículos científicos para revistas indexadas y para congresos internacionales. Es editor huésped de la revista indexada “Journal of Universal Computer Science”, cuenta con más de 150 artículos en congresos y revistas científicas internacionales, tiene más de 700 citas a sus artículos de investigación y fue el primero en publicar un artículo científico sobre el uso de la teoría de wavelets para la detección de anomalías en redes de comunicaciones. Sus áreas de interés incluyen seguridad en redes, procesamiento de señales utilizando wavelets, redes de comunicaciones y detección de anomalías.