ISSN: 1692-7257 - Volumen 2 – Número 22 - 2013

Revista Colombiana de Tecnologías de Avanzada

Recibido: 20 de junio de 2012
Aceptado: 27 de septiembre de 2012

# USE OF INTRUDER DETECTION SYSTEMS AND AGENT TECHNOLOGY IN INTELLIGENT DATA NETWORK MONITORING

# APLICACIÓN DE LOS SISTEMAS DE DETECCIÓN DE INTRUSOS Y LA TECNOLOGÍA DE AGENTES EN EL MONITOREO INTELIGENTE DE REDES DE DATOS

**PhD. Carlos Parra Ortega, Ing. Jaime Herrera Vergara**

**Universidad de Pamplona,** Facultad de Ingenierías y Arquitectura.
Ciudadela Universitaria. Pamplona, Norte de Santander, Colombia.
Tel.: +(57) (7) 5685303, Fax: +(57) (7) 5685303, Ext. 144.
E-mail: carapa@unipamplona.edu.co; jaime_herrera5@hotmail.com

**Abstract:** This paper is result of a degree thesis where some solutions to this problem are proposed. A prototype of multi-agent system is proposed for make passive monitoring of networks, in order to detect intruders who are carrying out attacks to the net. The prototype incorporates different types of agents to execute each task in the process of attack detection. The main component of the prototype is a mechanism through email messages between agents to notify the administrator of a network that is occurring anomalies in the system being monitored.

**Keywords:** Intrusion detection systems, multi-agent systems, JADE, Networks attacks.

**Resumen:** Este artículo es el resultado de un trabajo de grado donde se plantean algunas soluciones a este tipo de amenazas. Se plantea un prototipo de un sistema multi-agente que hace monitoreo pasivo de redes, para detectar intrusos que estén realizando ataques. El prototipo incorpora diferentes tipos de agentes para ejecutar cada uno las tareas del proceso de detección de ataques. El componente principal del prototipo es un mecanismo de alertas a través de mensajes entre agentes para dar aviso al administrador de una red que esta ocurriendo anomalías en el sistema que se esta monitoreando.

**Palabras clave:** Sistemas de detección de intrusos, Sistemas multi-agente, JADE, ataques a redes.

## 1. INTRODUCCIÓN

La seguridad en sistemas informáticos es un tópico de alta importancia hoy en día, debido a que nuestros sistemas de información están interconectados con otros sistemas a través de internet o redes propietarias. La información como activo de una organización debe cuidarse de accesos no autorizados, o intentos de modificación. Por esta razón, se han realizado trabajos en cuanto a brindar seguridad en redes a través de diversos métodos, entre ellos se tienen los sistemas de detección de intrusos – IDS (Debar *et al.*, 1999), (Mira, 2003), (Ferreira y Parra, 2003), y los sistemas basados en agentes de software (Santos, 2001), y finalmente sistemas mixtos (Herrera, 2012), de los cuales sus características se exponen en este documento.

La siguiente sección muestra las generalidades sobre los sistemas de detección de intrusos, los sistemas multi-agente se explican en el capítulo tres, mientras que el diseño, montaje y prueba del mecanismo de monitoreo de redes se describe en el

capítulo cuatro. Los resultados de las pruebas se muestran en el capítulo cinco, y finalmente se presentan las conclusiones de este trabajo en el capítulo seis.

## 2. SISTEMAS DE DETECCIÓN DE INTRUSOS

Un Sistema de Detección de Intrusos o IDS *(Intrusion Detection System*) es un hardware, software o combinación de ambos que monitorea la red de un sistema de información en busca de actividad maliciosa. Un IDS envía alarmas al administrador de la red advirtiendo la presencia de actividad intrusa, inusual, no autorizada o potencialmente dañina en el momento en que se esta produciendo, lo que permite percatarse de una situación en la que la seguridad aparente de la red no lo es. Hay que destacar que un IDS se limita a notificar de situaciones anómalas y/o peligrosas en la red, y por tanto no interviene activamente en su prevención (Santos, 2001). La detección de intrusiones permite a las organizaciones proteger sus sistemas de las amenazas que aparecen al aumentar la cantidad de conexiones entre equipos de red y la dependencia que se tiene hacia los datos almacenados en sistemas de información.

### 2.1 Clasificación de los IDS

La clasificación de los sistemas de detección de intrusos ha sido tratada en numerosos trabajos (Axelsson, 2000), (Zurutuza, 2005). La clasificación más común se realiza en base a tres criterios funcionales de los IDS. Estos son:

- Fuentes de información. Se refiere al origen de los datos que se usan para determinar si una intrusión se ha llevado a cabo. Puede ser una máquina o los paquetes capturados en una red.
- Análisis. Se trata del método de detección utilizado. La información recogida en el paso anterior puede ser analizada mediante diferentes estrategias. Puede ser detección de anomalías o detección de uso indebido.
- Tipo de respuesta. Una vez se ha determinado si ha sucedido alguna intrusión, los IDS pueden o bien responder de forma activa ante la misma, o bien registrar la detección y no realizar acción alguna. Se puede presentar ambos tipos de respuesta en algunos IDS.

### 2.2 Ataques informáticos

En informática la palabra “ataque” cosiste en aprovechar alguna debilidad o falla (vulnerabilidad) en el software, en el hardware, e incluso, en las personas que forman parte de un ambiente informático; a fin de obtener un beneficio, causando un efecto negativo en la seguridad del sistema, que luego repercute directamente en los activos de la organización (Mieres, 2009).

Un ataque informático siempre se efectúa por medio de redes o servicios de Internet, aprovechando las vulnerabilidades de un sistema operativo, aplicación, servidor, red y por otros medios. Las finalidades de los ataques son:

- Obtener accesos a una aplicación.
- Robar información de la empresa, de los proceso de esta, clientes (cuentas bancarias, dirección, teléfono etc.).
- Afectar el funcionamiento normal del servicio que presta la organización.
- Utilizar el sistema de un usuario como un “rebote” para un ataque.

La anatomía de un ataque informático esta basada en las exploraciones realizadas por Mieres (Mieres, 2009). Puede ejecutarse en cinco etapas:

- Reconocimiento. Esta etapa involucra obtener información con respecto a una potencial víctima que puede ser una persona u organización.
- ***Scanning*** (Exploración). En esta segunda etapa se utiliza la información obtenida en la fase 1 para sondear el blanco y tratar de obtener información sobre el sistema víctima como direcciones IP, nombres de host, datos de autenticación, entre otros. Se utiliza el escaneo de puertos.
- ***Gaining Access*** (Obtener acceso). En esta instancia comienza a materializarse el ataque a través de la explotación de las vulnerabilidades y defectos del sistema (Flaw exploitation) descubiertos durante las fases de reconocimiento y exploración.
- ***Maintaining Access*** (Mantener el acceso). Una vez se accede al sistema, se buscará implantar herramientas que permitan volver a acceder en el futuro desde cualquier lugar donde tenga acceso a Internet. Para ello, se usan utilidades como *backdoors*, *rootkits* y troyanos.
- ***Covering Tracks*** (Borrar huellas). Una vez que el atacante logró obtener y mantener el acceso al sistema, intentará borrar todas las huellas que fue dejando durante la intrusión para evitar ser detectado por el profesional de seguridad o los administradores de la red. En consecuencia, buscará eliminar los archivos de registro (log) o alarmas del Sistema de Detección de Intrusos (IDS).

## 3. TECNOLOGÍA DE AGENTES

La definición del término "agente" en el contexto computacional es muy amplia, puesto que los atributos asignados a los agentes provienen de varias disciplinas que van desde la Psicología hasta la Inteligencia Artificial y la Ingeniería de Software.

A pesar de esto, diferentes autores han intentado definir lo que es un agente (Wooldridge, 2002) establece que un agente es un sistema computacional que se sitúa en algún entorno y es capaz de actuar de forma autónoma para alcanzar sus objetivos de diseño, también hay definiciones operacionales en el sentido de que un agente es una entidad que percibe y actúa sobre un entorno a través de sensores y responder según su función en el mismo entorno a través de efectores, asumiendo que cada agente puede percibir sus propias acciones y aprender de la experiencia para definir su comportamiento (Russell & Norvig, 2005). Esta definición se esquematiza en la figura 1.

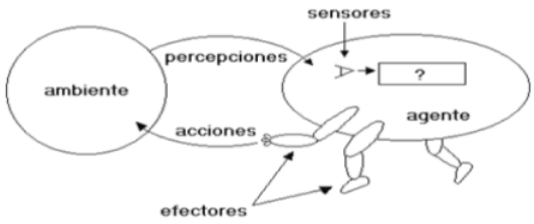


*Fig. 1: Esquema de un agente (Russell & Norvig, 2005)*

A los agentes se les asignan una serie de atributos o propiedades (Morales, 2002), entre las cuales se tienen las siguientes:

- Autonomía
- Sociabilidad
- Reactividad
- Iniciativa
- Movilidad
- Veracidad
- Benevolencia
- Inteligencia
- Racional
- Coherencia
- Adaptabilidad

Uno de los campos de aplicación de la tecnología de agentes se relaciona con la automatización de procesos y monitoreo de eventos en redes, debido a su naturaleza distribuida, y a que los agentes pueden instanciarse en varias máquinas diferentes en una red, y comunicarse entre sí.

## 4. DISEÑO Y MONTAJE DEL SISTEMA DE MONITOREO DE REDES

Como plataforma de implementación de los agentes se escogió al entorno JADE (http://jade.tilab.com) , puesto que proporciona facilidades en cuanto a la coordinación de agentes, seguridad, comunicación, movilidad, redundancia, y muchos otros servicios básicos en una arquitectura distribuida, además de estar implementada en lenguaje java, que permite el desarrollo de aplicaciones sobre esta tecnología sin coste alguno y la flexibilidad del código lo hace verdaderamente atractivo.

La distribución de las funcionalidades del prototipo se realiza generalmente en una arquitectura distribuida basada en capas con diferentes funcionalidades a distinto nivel. En la figura 2 se puede apreciar la manera en que se diseñó esta arquitectura de implementación. Físicamente se requieren al menos dos máquinas en una red: una de ellas desempeña las funciones de máquina atacante, y la otra sería la víctima, donde también se instalan el IDS y el sistema multi-agente.

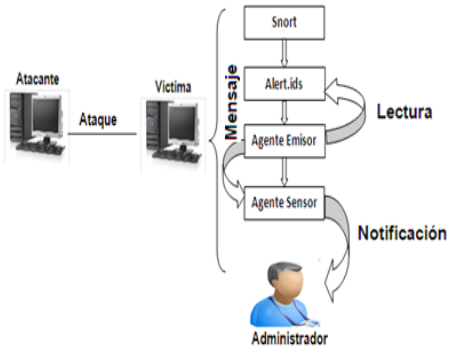


*Fig. 2: Esquema de implementación del sistema de monitoreo basado en agentes*

La función de cada capa es la siguiente:

- **Atacante.** A partir de esta máquina se lanzan los ataques con el fin de aprovechar alguna vulnerabilidad o falla, para obtener un beneficio, causando un efecto negativo en la seguridad del sistema, que luego pasa directamente en los activos de la empresa u organización. Se utilizará como ataque el escaneo de puertos mediante el programa nmap (http://nmap.org/man/es/index.html#man-description)
- **Víctima**. Es la máquina a la cual el atacante intenta acceder a ella.

- **IDS Snort.** (http://www.snort.org) Es la capa encargada de capturar el tráfico que circula por interface de red en busca de patrones que correspondan a ataques, una vez encontrado un patrón de ataque, *snort* lanza una alerta que es almacena en el directorio *C:\Snort\log\alert.ids*. Puede estar instalada en la máquina víctima o en otra que esté en la red local.
- **Agente Emisor.** El agente emisor es el encargado de hacer la lectura del archivo de alertas arrojado por el IDS snort, verificando periódicamente que se hayan producido alarmas de intrusión en la red. Una vez observada una alerta envía un mensaje al agente sensor notificándole que hay una anomalía en la red.
- **Agente Sensor.** El agente sensor es el encargado de recibir los mensajes de anomalía que envía el agente emisor, al llegar un mensaje de anomalía notifica al administrador de la red a través de un correo que en que hay un patrón de ataque.
- **Administrador.** El administrador de la red es el encargado de velar por la seguridad de la red que se encuentre en perfecto estado.

Este sistema de monitoreo se implementó en la red local de la Universidad de Pamplona, en el laboratorio de informática del departamento de Idiomas.

## 5. EJECUCIÓN DE PRUEBAS Y DISCUSIÓN DE RESULTADOS

Para simular los ataques a la red, se utilizó el programa Nmap, para hacer un ataque de escaneo de puertos, con el fin de detectar conexiones TCP completas y conexiones parciales revisando paquetes SYN. El objetivo final de estas pruebas es analizar el comportamiento del IDS *Snort* y los agentes según los diversos ataques realizados.

Después del ataque de escaneo de puertos mediante esta herramienta, el detector de intrusos *Snort* produjo las siguientes alertas, que se pueden observar en la figura 3.

```
[**] [133:27:1] (dcerpc2) Connection-oriented DCE/RPC - Invalid major version: 71 [**]
[Classification: Potentially Bad Traffic] [Priority: 2]
06/21-16:08:52.785500 00:0F:FE:AC:41:18 -> 00:0F:FE:AC:54:BA type:0x800 len:0x48
172.25.2.225:1513 -> 172.25.2.219:135 TCP TTL:128 TOS:0x0 ID:47038 IpLen:20 DgmLen:58 DF
***A**** Seq: 0x938733D5  Ack: 0xCE215929  Win: 0xFFED  TcpLen: 20
[Xref => http://msdn.microsoft.com/en-us/library/cc201989.aspx]

[**] [129:15:1] Reset outside window [**]
[Classification: Potentially Bad Traffic] [Priority: 2]
06/21-16:10:45.351866 00:0F:FE:AC:41:18 -> 00:0F:FE:AC:54:BA type:0x800 len:0x3C
172.25.2.225:2024 -> 172.25.2.219:445 TCP TTL:255 TOS:0x0 ID:2746 IpLen:20 DgmLen:40
*****R** Seq: 0x11A34B0F  Ack: 0x0  Win: 0x200  TcpLen: 20
```

*Fig. 3: Alerta del IDS Snort sobre escaneo de puertos*

Donde la siguiente es la interpretación de la amenaza potencial según el archivo log de Snort.

- 06/21-16:08:52.785500: Marca de tiempo
- 133:27:1: Numeración asociada a la descripción de la alerta
- Connection-oriented DCE/RPC: nombre dela alerta.
- Potentially Bad Traffic: clasificación de la alerta contenida en el archivo classification.config.
- Priority: 2 prioridad de la alerta
- dcerpc2: procesador que genero la alerta.
- 172.25.2.225:1513: origen del cual se genera la alerta y el puerto por el cual se está efectuando.
- 172.25.2.219:135 destino de quien genera la alerta y el protocolo al cual se está atacando.

El sistema multi-agente reacciona cuando el agente emisor dentro de su comportamiento cíclico revisa el archivo log en busca de nuevas alarmas, y una vez la encuentra bloquea durante dos segundos las lecturas posteriores para enviar al agente sensor un mensaje indicando la ocurrencia de la alarma. El resultado de esos comportamientos se puede observar en la figura 4.

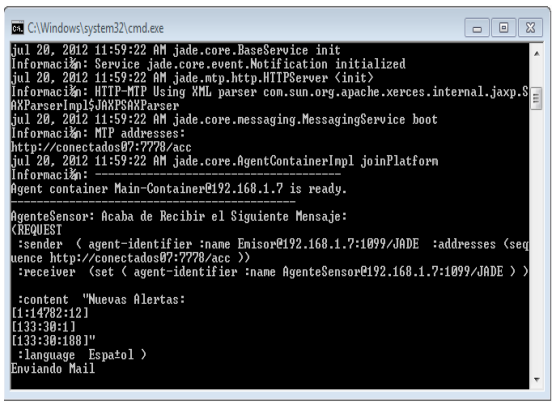


*Fig. 4: Comportamiento visible de los agentes al ser detectada una alarma de intrusión*

Este comportamiento es el encargado de enviar un mensaje con la identificación de la alerta al agente sensor. El agente sensor al igual que el agente emisor esta implementado con los mismo comportamiento, el comportamiento cíclilco se implementa con el fin de estar recibiendo mensajes del agente emisor, y el comportamiento simple se encarga de enviar al correo del administrador la alerta. Una vez se recibe un mensaje, se envía un correo electrónico al administrador del sistema. El cual se puede apreciar en la figura 5.

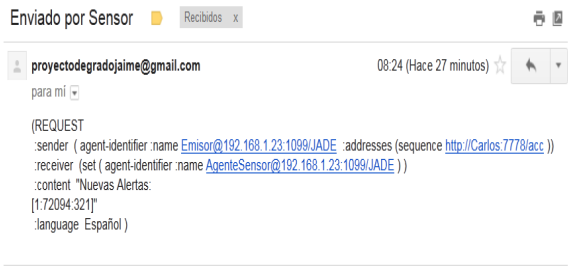


*Fig. 5: Mensaje que recibe el administrador de la red al producirse una alerta de intrusión*

## 6. CONCLUSIONES

Como resultado de este trabajo, se logró demostrar que es posible que los sistemas multi-agente interactúen con los IDS para llevar a cabo labores de monitoreo de redes, para detectar intrusos que estén realizando ataques. Las herramientas de código abierto como *Snort* y JADE pueden integrarse para así poder actuar de forma mas rápida ante una anomalía que se presente en forma de intrusión en una red.

Además el resultado de la experimentación permitió además visualizar la explotación de las vulnerabilidades expuestas, descubrir patrones de ataques, encontrar información sobre el atacante.

Se lograron conocer cuáles son las vulnerabilidades de una red local basada en Windows y establecer a futuro políticas de seguridad que minimicen los riesgos cuando que alguno de estos ataques pasivos sea llevado a cabo. Como trabajo posterior se puede recomendar la inclusión de agentes móviles, o la generación de alertas hacia dispositivos móviles como un siguiente paso para la generación de alarmas de intrusión en redes.

## REFERENCIAS

Russell, Stuart y Norvig, Peter. *Inteligencia Artificial, Un Enfoque Moderno.* McGraw-Hill. 1995.

Wooldridge, M. *Introduction to MultiAgent Systems.* John Wiley & Sons. 2002.

Montelongo, José. *Coordinación Distribuida Basada en Agentes de Sistemas de Manufactura Flexible.* Universidad de Guadalajara. 2002.

Santos, Javier. *Sistema Distribuido de Detección de Intrusos Basado en Agentes Inteligentes.* 2001.

Mira Alfaro, José. *Implantación de un Sistema de Detección de Intrusos en la Universidad de Valencia.* Universidad de Valencia. 2003.

H.Debar, M.Dacier and A.Wespi. *Towards a taxonomy of intrusion-detection systems.* Chalmers University of Technology. 1999.

Axelsson, S. *Intrusion Detection Systems: A Taxonomy and Survey.* Technical Report. Chalmers University of Technology. 2000.

Ferreira, E. y Parra, C. *Detección de intrusos en redes utilizando Snort.* Tesis Esp. UIS. 2003.

Herrera, Jaime. Monitoreo Inteligente de Redes utilizando tecnología de agentes y sistemas de detección de intrusos. Tesis de grado. Universidad de Pamplona. 2012.

Zurutuza, U. *Revisión del estado actual de la investigación en el uso de data mining para la detección de intrusiones.* Escuela Politécnica Superior de Mondragón. 2005.

Jorge Mieres. *Ataques informáticos Debilidades de seguridad comúnmente explotadas.* 2009. https://www.evilfingers.com/publications/white_AR/01_Ataques_informaticos.pdf