ESTUDIO COMPARATIVO DE LA EFECTIVIDAD DE LOS SISTEMAS DE DETECCIÓN DE INTRUSOS.

Damián Fernando Pinto Niño[1]

Álvaro Ernesto Robles Rincón

Resumen

El presente estudio tiene por objetivo caracterizar las respuestas de un grupo de herramientas de detección de intrusos, permitiendo establecer cual presenta mejor rendimiento frente a diferentes acciones realizadas por medio de troyanos tipo *backdoor*. Las herramientas de detección de intrusos fueron seleccionadas en base a unos requisitos establecidos, de la misma manera se analizó la arquitectura interna de funcionamiento y atributos de cada una de las herramientas, junto con sus ventajas. Además se presenta los criterios de selección tomados para la elección de los troyanos tipo *backdoor* de igual manera se muestra las características de cada uno de ellos y las diversas funciones que ofrecen. Conjuntamente se desarrollan actividades como la caracterización de los parámetros que permitirán efectuar la evaluación de cada una de las herramientas. El resultado final del proyecto es el análisis de cada una de las repuestas brindadas por las herramientas de detección de intrusos dentro de la ejecución de las pruebas, y el estudio de los parámetros de los diferentes troyanos, permitiendo identificar que parámetros son más comunes o no a ser detectados por las herramientas.

Palabras Claves

Herramientas de detección de intrusos, troyanos *backdoor*, arquitectura, parámetros, pruebas.

Abstract

The present study aims to characterize the responses of a group of intrusion detection system (IDS), allowing to establish which features better performance against different actions through backdoor Trojans. The intrusion detection tools were selected based on requirements established in the same manner discussed the internal architecture of operation and attributes of each of the tools, along with its advantages. Also presents selection criteria for selecting taken Trojans backdoor similarly shows the characteristics of each one of them and the various functions they offer. Activities are developed together as the characterization of the parameters that will carry out the evaluation of each of the tools. The end result of the project is to analyze each of the answers provided by the IDS within the execution of the tests, and study the parameters of the different trojans in order to identify which parameters are more common or not to be detected by the tools.

Key words

Intrusion detection system, backdoor trojans, architecture, parameters, tests.

1. Introducción

La gran cantidad de riegos informáticos como virus, troyanos, gusanos, y malware en general, a los cuales se encuentra expuesta la información y/o datos vitales de los usuarios de computadoras, hace necesario que el resguardo de ésta forme parte de las prioridades para las personas, siendo necesario no solo la implementación de hardware que blinde la información, sino también la implementación de software que colabore en esta labor.

Las herramientas de detección de intrusos, son aplicaciones que poseen la versatilidad de funcionar tanto en grandes redes de datos, como en un único computador, permitiendo proteger la información almacenada dentro de los computadores, emitiendo en corto tiempo alertas ante las acciones realizadas por intrusos, remitiendo correos electrónicos con los datos capturados de las acciones y ofreciendo la posibilidad de crear reglas que establezcan el funcionamiento y medidas a ejecutar ante diversas situaciones que se

presenten, haciendo de la labor de resguardo de información una tarea menos compleja.

2. Marco teórico

Los ataques informáticos efectuados por troyanos son cada vez más comunes y están generando preocupación no solo dentro de las empresas también en usuarios normales, los cuales se sienten vulnerables por el hecho de poder ser víctimas en cualquier momento de ataques por terceros. Estudios publicados en Evilfingers.com (portal web especializado en seguridad informática) han demostrado que aproximadamente el 80% de los ataques informáticos son ejecutados mediante troyanos [1]. Los ataques con troyanos logran su objetivo debido a las diversas opciones que les permiten camuflarse. En el año 2010 fue detectada una red de computadores *zombies*[1] que fue creada por medio de un troyano, éste infectó alrededor de 75.000 sistemas en 2.500 organizaciones en todo el mundo, comprometiendo información de vital importancia para las empresas y hogares en los cuales se encontró éste troyano. El estudio reveló que éste troyano era capaz de obtener información como credenciales de acceso corporativo, contraseñas de correo electrónico, de cuentas bancarias, de redes sociales, y alrededor de 2.000 archivos de certificados SSL, esta *botnet*[2] fue llamada *Kneber botnet* y fue encontrada a principios del 2010 [2].

[1] Zombie: Nombre otorgado a un computador que ha sido infectado por algún tipo de malware, sin conocimiento alguno por parte del usuario. [http://www.alegsa.com.ar/Dic/zombie.php]

[2] Botnet: Es un conjunto de computadores infectados por un programa diseñado para automatizar tareas que son controlados de manera remota desde un centro de comando. [http://www.eset.es/centro-de-alertas/diccionario-amenazasas]

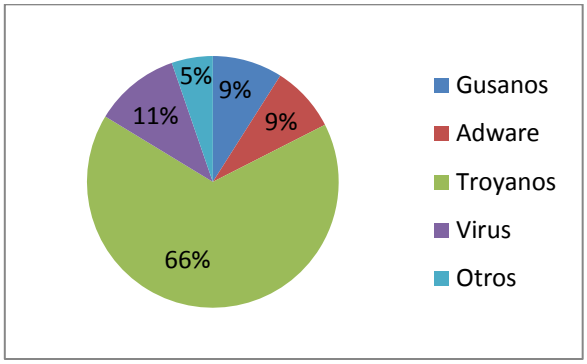
2.1. Debilidades de los computadores frente a los troyanos *Backdoor*

Los troyanos además de aprovecharse de vulnerabilidades que tienen los SO para poder robar información, también reclutan nuevos computadores generando, de esta forma *Botnet* que están empezando a crear gran preocupación dentro de las máximas autoridades informáticas y los desarrolladores de software; tal es así que grandes empresas como Microsoft y organismos federales como la *Federal Trade Commission* (FTC) han comenzado a intensificar su lucha contra las *botnet* mediante acciones legales logrando que se suspendan dominios relacionados con la administración de las mismas [3].

Un motivo que mantiene alarmadas a las grandes compañías mundiales es que las *botnet* atacan vulnerabilidades encontradas en diferentes aplicaciones, y según datos publicados en viruslist.com (portal web dedicado a informar al público aspectos de seguridad y amenazas en Internet), empresas como Microsoft, Adobe y Sun Microsystems, se encuentran dentro de las empresas con más aplicaciones vulnerables a éste tipo de amenazas. Cualquier persona puede ser parte de una *Botnet* sin que sepa que pertenece a una, son difíciles de detectar por las herramientas antivirus existentes, debido que trabajan de la mano con troyanos los cuales son activados por el mismo usuario abriendo puertos sin que el antivirus lo detecte como peligroso [4].

Otro uso que se le dio a los troyanos durante el año 2011 fue el robo de información sobre pagos electrónicos, según el reporte entregado por Pandalabs en su informe anual [5], en el informe se demostró el uso de troyanos antiguos como *Zeus* el cual fue modificado para lograr pasar desapercibido y poder robar ese tipo de información por medio de variantes del mismo troyano.

Figura 1. Códigos maliciosos detectados durante el año 2011



2.2. Herramientas de detección de intrusos (IDS)

Un Sistema de Detección de Intrusos (IDS), es una herramienta informática que permite detectar accesos no autorizados o ataques realizados a un computador o red dependiendo de la herramienta utilizada y de su configuración [6].

En procura de una mayor precisión de los datos a ser obtenidos para el desarrollo del proyecto y poder efectuar una investigación con un buen criterio, es necesario seleccionar un grupo de herramientas IDS que tengan las siguientes características:

- Deben ser HIDS (*Host-Base Intrusion Detection System*). Sabiendo que las pruebas a realizar con los troyanos van a tener lugar en un computador específico, de este modo poder monitorizar los cambios que ocurran en él.

- Software Libre. Este proyecto está orientado a proteger un computador sin tener que invertir en costos elevados y aunque existe un grupo de IDS comerciales, también existen aplicaciones gratuitas de gran utilidad y funcionamiento con las cuales se puede trabajar.

- Basado o no en Snort. Snort es un IDS que posee reconocimiento a nivel mundial por ser funcional, por ser GPL[3], y porqué varios de los IDS que se encuentran en Internet están basados en él, pero sería interesante poder también trabajar con algunos que no sean basados en él para observar las diferencias.

2.3. Troyanos *Backdoor*

En el contexto de la documentación o estudios acerca de troyanos tipo *backdoor* más significativos, la información disponible es escasa, por este motivo se hace necesaria la implementación de este tipo de *malware* según experiencias encontradas en foros y páginas web especializadas en seguridad informática, tomando como referencia la popularidad de los troyanos en internet, y estableciendo popularidad como la cantidad de páginas web donde se encuentre información acerca de los troyanos en base a resultados obtenidos por medio de diferentes motores de búsqueda en internet, de esta forma se seleccionaron 4 troyanos tipo *backdoor* con diferente popularidad, logrando así diversidad de troyanos tipo *backdoor* para realizar las pruebas con los IDS.

Darkcomet RAT

Es un troyano tipo *backdoor* que posee entorno gráfico de fácil uso. Aunque es común encontrarlo clasificado como una herramienta de administración remota, su uso más frecuente es el de troyano y es detectado como tal por las herramientas

[3] GPL (*General Public License*): En español Licencia Publica General, es una licencia que está dirigida a proteger la distribución, modificación y uso de software libre con el objetivo de protegerlo de apropiación que limite a los usuarios de esas opciones.

antivirus, debido a las funciones que incorpora en él [7].

Poison ivy
Es una herramienta de control remoto usada como troyano, posee características para implantarse en el sistema y pasar desapercibido para el antivirus. Ya no existen actualizaciones ni nuevas versiones oficiales desde el 2008, pero aún es utilizado a pesar de ser detectado por los antivirus, debido a que con técnicas de cifrado y ocultación se puede camuflar dentro del computador [8].

Bifrost
Ésta herramienta, permite tener acceso remoto a un computador, posee funcionalidades de captura de datos, imagen y cambio de registros, su funcionamiento es similar a otras herramientas de éste tipo que manejan arquitectura cliente/servidor. Los antivirus la reconocen como código malicioso e impiden su ejecución. Actualmente no tiene una página oficial para su descarga pero es posible encontrarlo descargarlo por medio de internet en foros.

Spy-net
Troyano que permite el uso de equipos de forma remota, tiene capacidades similares a otros troyanos tipos *backdoor*, con la posibilidad de crear conexión directa con el servidor utilizando la arquitectura cliente/servidor, permite la creación de *plugins* para que el troyano se conecte directamente a un servidor FTP [4] o web, además ofrece un entorno estéticamente amigable y moderno para el usuario.

[4] FTP: En ingles *File Transfer Protocol*, es un servicio utilizado para transferir archivos entre dos computadores.

2.4. Arquitectura de los troyanos *backdoor*

La arquitectura de un troyano varía según el ataque que se desee realizar y/o según el tipo de troyano, pero la mayoría de los troyanos tienen una estructura base que consta de tres partes fundamentales: Módulo de seguridad, Módulo de daño, Módulo de comunicación.

Estos módulos conforman la estructura del troyano y poseen subdivisiones con operaciones específicas.

3. Caracterización de las reglas de los IDS a emplear

Las reglas para un IDS son el conjunto de instrucciones que le indican qué tipo de acciones deben ser consideradas como intrusiones o accesos no autorizados al computador. Cada IDS determina cuál debe ser el protocolo a seguir según sus reglas para generar una alerta, incidiendo en la forma en que se caracterizan los IDS.

3.1. Parámetros de caracterización

Una vez identificadas las reglas y por consiguiente las funciones en común que poseen los cuatro IDS seleccionados, se hace necesario realizar una lista de parámetros que permitirán desarrollar el estudio comparativo entre ellos y con base en los resultados obtenidos del estudio proceder a seleccionar el más efectivo de los IDS (ver tabla 1).

Tabla 1. Descripción de los Parámetros de caracterización y de las pruebas

Parámetro	Descripción	Prueba
Registros en el sistema	Reconoce cambios ocurridos en el SO.	Reconocer los cambios en el SO como instalación/desinstalación de software y eliminación de archivos. Alteración a los programas de inicio del SO.
Llaves de registro	Analiza cambios en las llaves de registro.	Alterar llaves de registro utilizando herramientas que posee el troyano.
Conexiones realizadas hacia el agente/cliente	Conexiones que ocurrieron en el SO.	Agregar llaves de registro al SO.
Checksum	Valor que permite verificar la integridad de los archivos del SO.	Realizar conexiones remotas al agente/cliente por medio de algún protocolo. Alterar o modificar un archivo cambiando su checksum y observar las acciones del IDS.
Algoritmo *hash*	Identifica el algoritmo *hash* utilizado.	Identificar el algoritmo utilizado por el IDS y colocar a prueba el algoritmo hash con herramientas que posee el troyano.
Falsos positivos	Mensajes emitidos que no representan una alerta.	Observar alertas emitidas por actividades legítimas.
Ausencia de falsos negativos	Mensajes emitidos con un nivel errado de alerta o que no emitió alerta.	Efectuar acciones a través del troyano al agente/cliente para descubrir eventos no detectados por el IDS.
Carpetas por omisión	Configuración de directorios que tienen los IDS por omisión.	Observar las carpetas que el IDS monitoriza por omisión.
Detección de *Rootkit*	Posibles *Rootkit* en el agente/cliente.	Emplear la función de *rootkit* del troyano para observar la respuesta del IDS.
Frecuencia de escaneo	Tiempo establecido por omisión para el escaneo o intercambio de información entre el cliente y el servidor.	Observar dentro de los archivos de configuración el valor del tiempo establecido para realizar escaneos al cliente.

Cada uno de los parámetros mencionados en la tabla anterior, se convertirá en un punto a evaluar de cada herramienta IDS. También se encuentran las descripciones de las pruebas que se efectuarán a los IDS con los parámetros mencionados en la tabla 1

permitiendo conocer el rendimiento de los IDS.

Una vez establecidos los parámetros a evaluar a cada uno de los IDS, es necesario establecer un valor porcentual para cada parámetro, que permita establecer de forma cuantitativa qué herramienta IDS presenta mejor desempeño que las demás.

4. Resultados de las pruebas a los IDS.

Para calificar los IDS en las pruebas se creó una tabla con valores que clasifican a los IDS con los puntos obtenidos (ver tabla 2) después de realizar las pruebas con los parámetros de la tabla 1.

Tabla 2 Valores y categorías rubricas

Categoría	Rango de valores/puntaje	Clasificación
1	0 – 10	Malo
2	11 – 45	Regular
3	46 – 75	Bueno
4	76 – 100	Excelente

Para la tabla 2 se utilizaron categorías que van de 1 hasta 4 con valores que van desde 0 hasta 100, siendo 1 la categoría con menos puntaje y 4 la categoría con mayor puntaje, con clasificaciones que se encuentran desde malo hasta excelente. La categoría 1 es considerada como mala, la categoría 2 es considerada como regular, la categoría 3 es considerada como buena y la categoría 4 es considerada como excelente. Adicionalmente se creó una rúbrica para evaluar los parámetros de la tabla 1.

Tabla 3 Ejemplo de rúbrica por parámetro

Parámetro							
4		3		2		1	
Aspecto 1		Aspecto 1.1		Aspecto 1.2		Aspecto 1.3	
	60		45		2		0
Aspecto 2		Aspecto 2.1		Aspecto 2.2		Aspecto 2.3	
	40		30		23		0

En la tabla 3 se puede observar un ejemplo de cómo se empleó la rúbrica para cada parámetro de la tabla 1. Cada parámetro con su rúbrica puede tener como mínimo 2 categorías y máximo 4 (1), con aspectos a evaluar en cada categoría (2), con un rango de valores preestablecidos para cada categoría (3) (ver tabla de valores y categorías rubrica) asignados en cada aspecto según la categoría que pertenezca y la importancia que puede representar para cada parámetro.

Una vez establecidos los parámetros a evaluar y las pruebas a ejecutar, es necesario realizar un análisis de los resultados obtenidos por cada herramienta IDS.

4.1. Análisis de las pruebas sobre OSSEC

Las pruebas con OSSEC demostraron lo eficaz que puede llegar a ser esta herramienta para la seguridad informática en el área de HIDS, es una herramienta que no lentifica[5] al SO y si brinda una poderosa

[5] Lentifica: Proviene del verbo lentificar, y según la RAE "*Imprimir lentitud a alguna operación o proceso, disminuir su velocidad.*" [http://buscon.rae.es/draeI/SrvltConsulta?LEMA=lentificar]

ayuda para detectar posibles intrusos dentro del computador, aunque requiere de conocimientos en Linux para la correcta implementación del servidor. Las pruebas demostraron su eficacia al detectar los cambios en el SO como nuevas instalaciones de software, alteración y/o modificación de archivos necesarios para el correcto funcionamiento del SO, pese a que no detectó las conexiones realizadas del troyano, ni acciones como abrir una consola remota, si reconoce cambios de configuración del SO que se pudiesen realizar desde el troyano por medio del *Checksum* que implementa para monitorear los archivos.

4.2. Análisis de las pruebas sobre Snort

Las pruebas con Snort demostraron la efectividad que este IDS posee para detectar las conexiones que se efectuaron al computador a analizar, otorgando información relevante del intruso, como la dirección IP y el nombre del equipo. Para el caso específico en troyanos, Snort trabaja detectando patrones, un modo semejante a las herramientas antivirus, estos patrones se encuentran configurados en las reglas, y estas son actualizadas y descargadas desde el sitio web de Snort. Al emplear las reglas actualizadas que se encontraban en la página oficial de Snort, estas no detectaron las conexiones de los troyanos, por lo cual se decidió crear reglas propias de esta forma al crear las reglas todos los troyanos utilizados fueron detectados.

4.3. Análisis de las pruebas sobre Sguil

Los resultados de las pruebas con Sguil mostraron similitudes a las realizadas con Snort debido a que Sguil está basado en el motor de Snort brindando cualidades que él posee. Sin embargo al utilizar Sguil se disminuyeron los falsos positivos, esto se debe a que las configuraciones y reglas en Sguil son analizadas intentando evitar la generación de falsos positivos. La interfaz gráfica que ofrece Sguil no es amigable y puede en algún momento confundir al administrador, debido que puede llegar a ser totalmente diferente de otras herramientas IDS, aunque como las otras herramientas IDS permite conocer en las alertas datos importantes como dirección IP origen y destino, puerto, hora de recibo de las alertas, nombre del sensor y estatus de la alerta, además, su compleja configuración e implementación no es un punto a favor para él.

4.4. Análisis de las pruebas sobre Prelude

Las pruebas con Prelude mostraron la capacidad que posee para interactuar con los IDS que manejen la arquitectura *Intrusion Detection Menssage Exchange Format* (IDMEF), unificando mensajes y alertas en una sola interfaz, de esta forma se pude utilizar diferentes IDS como agentes o sensores de Prelude, logrando así ser un IDS Hibrido. Para lograr que Prelude trabajara como HIDS se precisó utilizar otro IDS que funcionara de forma nativa como HIDS, en este caso se escogió OSSEC, el cual posee un agente que trabaja tanto en Linux como en Windows. Las alertas emitidas por Prelude con OSSEC fueron en tiempo real y sin mayores diferencias comparadas con las alertas emitidas por el servidor nativo de OSSEC, aunque la interfaz de Prelude es estéticamente más agradable, no representa un punto a favor como tal; la real diferencia o ventaja es la forma de unificar la información de todos los sensores, independientemente si esos sensores involucran otros IDS.

4.5. Conclusiones de las pruebas

Las pruebas demostraron las cualidades y debilidades que tienen los IDS para detectar intrusiones en el caso específicos de los troyanos. En la tabla 4 se puede encontrar

los resultados finales de las pruebas realizadas con los parámetros establecidos en la tabla 1 y evaluados por medio de la rúbrica de la tabla 3, con los valores establecidos en la tabla 2, mostrando como ganador a Prelude y categorizándolo como bueno con un puntaje de promedio de 69,75.

Tabla 4 Puntaje obtenidos por los IDS frente a los troyanos

	OSSEC	Snort	Sguil	Prelude
Darkcomet	52,05	31,5	32,5	69,75
Spy-net	52,05	31,5	32,5	69,75
Poison Ivy	52,05	31,5	32,5	69,75
Bifrost	52,05	31,5	32,5	69,75
Promedio	**52,05**	**31,5**	**32,5**	**69,75**

5. Pruebas de los IDS con los troyanos modificados

Para las pruebas realizadas con los troyanos modificados se tendrá adicionalmente una herramienta antivirus llamada Avira seleccionada a partir de un estudio hecho por *PassMark* [9] donde se hace una comparación de diferentes tipos de antivirus a partir de métricas realizadas por ellos.

Los troyanos serán modificados de tal manera que intenten pasar desapercibidos por la herramienta antivirus y la IDS. Para llevar a cabo esa tarea los troyanos se modificarán por medio de un *crypter*, de esta forma, lograrán tener un cifrado y un código diferente al que tenía originalmente el troyano, intentando de esta forma ser inofensivo ante el antivirus y pasar desapercibido por el IDS. Adicionalmente los troyanos se configurarán de forma diferente, se les asignarán puertos de conexión diferentes y contraseñas al momento de la conexión entre el servidor del troyano y el cliente.

Para estas pruebas solo se utilizará el IDS que obtuvo mayor puntaje en las pruebas anteriores que se encuentran en la tabla 4, para este caso el IDS Prelude, y evaluado con los parámetros de caracterización de la tabla 1.

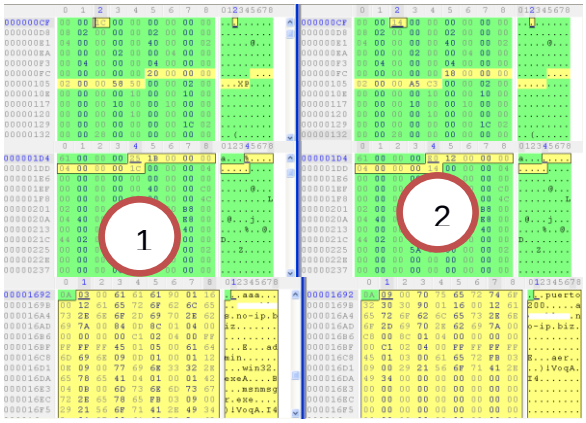
5.1. Análisis y conclusiones de las pruebas sobre Prelude con troyanos modificados

El IDS Prelude demostró la efectividad que posee al trabajar junto con otras herramientas IDS, siendo empleadas como sensor o trabajando conjuntamente con Prelude.

Las pruebas con los troyanos modificados ante el IDS Prelude fueron similares a las pruebas realizadas con los troyanos sin modificar. Los troyanos en todas las pruebas lograron no ser detectados por la herramienta antivirus Avira.

En las pruebas con los IDS un troyano logró no ser detectado por la herramienta IDS Prelude, al analizar las razones por las cuales no fue detectado se puede deducir que al utilizar el *crypter* solo generó efecto ante el antivirus, pero el cambio de puerto y contraseña evidenció cambios fundamentales en el código como se puede ver en la figura 2 al ser analizado por medio de un editor hexadecimal, a la derecha (1) se encuentra el troyano sin modificar y la izquierda(2) se encuentra el troyano modificado, los colores verdes indican las partes del código iguales entre el troyano modificado y sin modificar, y el color amarillo indica las partes que fueron modificadas.

Figura 2 Comparación hexadecimal de del troyano no detectado



Adicionalmente se puede observar por medio del *software Wireshark* la firma que deja el troyano cuando realiza la conexión TCP/IP entre el cliente y el servidor del troyano, siendo está a su vez la firma que usa el IDS para detectar el troyano, como se puede observar en la figura 3 y la figura 4, las firmas son diferentes, por ende el IDS no puede reconocer que un troyano se conectó con el computador que él se encuentra analizando.

Figura 3. Firma del troyano *poison* detectado por el IDS

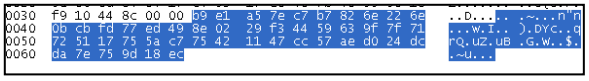
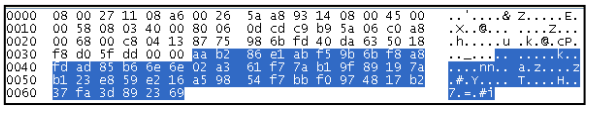


Figura 4. Firma de *poison* no detectada por el IDS



En la tabla 5 se evidencia que el troyano *poison* logró disminuir el puntaje final obtenido por Prelude al lograr no ser detectado por el IDS.

Tabla 5. Puntaje obtenidos por los IDS Prelude frente a los troyanos modificados

Troyanos	Prelude
Darkcomet	69,75
Spy-net	69,75
Poison	52,05
Bifrost	69,75
Promedio	**65,32**

En conclusión con la información obtenida del troyano se evidencia las razones por las cuales el IDS no logró detectarlo, la razón fundamental por la cual el troyano no fue detectado por el IDS no radica exclusivamente en el uso de un *crpyter* puesto que los otros troyanos fueron detectados por el IDS aún siendo modificados por él, radica en el cambio de puerto y el uso de contraseña para la conexión entre el cliente y el servidor del troyano, debido que al cambiar esas opciones que *poison* posee por omisión logra generar un flujo diferente en el código, generando una firma nueva y totalmente diferente, caso contrario con los otros troyanos analizados, que aún siendo modificados, cifrados y con puertos y contraseñas diferentes fueron detectados por el IDS.

6. Conclusiones

Después de realizar el estudio se puede concluir que:

El uso de herramientas informáticas tales como IDS y antivirus permiten obtener un nivel de seguridad general pero no total, razón por la cual se debe estar en constante investigación para el uso de nuevos métodos y herramientas de protección.

El uso de troyanos mostró la vulnerabilidad que aún poseen tanto las herramientas IDS

como los antivirus frente al empleo de este tipo de *malware*. A pesar que, las herramientas IDS brindan mayor protección comparadas con las herramientas antivirus, las herramientas IDS son más complejas de administrar, y requieren de personal calificado para su uso y mantenimiento.

Este proyecto de grado demostró la importancia que ofrece el uso de herramientas IDS en ámbito de la seguridad informática, dando a conocer las debilidades y fortalezas que estas herramientas poseen en el caso específico de troyanos, dejando un precedente y una semilla para estudios posteriores que se deseen desarrollar para mejorar la detección de troyanos o para mitigar otro tipo de ataques o intrusiones.

Referencias

[1] J. Mieres.(2009). Ataques informáticos, debilidades de seguridad comúnmente explotadas. Evil Fingers. [Online]. Available: https://evilfingers.com/publications/white_AR/01_Ataques_informaticos.pdf

[2] Netwitness. (2010, Enero). "Kneber Botnet" Targets Corporate Networks and Credentials. [Online]. Available: http://netwitness.com/about/press-releases/2010-netwitness-discovers-massive-zeus-compromise

[3] Y. Namestnikov. (2011). Desarrollo de las amenazas informáticas en el segundo trimestre de 2011. [Online]. Available: http://www.viruslist.com/sp/analysis?pubid=207271138

[4] Seguridad informática, Purificación Aguilera López, editorial IDETEX

[5] Pandalabs(2012, enero) Informe Anual PandaLabs 2011 [Online]. Avaliable: http://prensa.pandasecurity.com/wp-content/uploads/2012/01/Informe-Anual-PandaLabs-2011.pdf

[6] The Information Assurance Technology Analysis Center (IATAC). (2009, Septiembre). Intrusion Detection Systems. N° 6. [Online]. Available: http://iac.dtic.mil/iatac/download/intrusion_detection.pdf

[7] Darkcodersc Software. (2011) DarkComet Remote Administration Tool Project. [Online]. Available: http://www.darkcomet-rat.com/about

[8] Poison Ivy.(2006, Septiembre). About Poison Ivy. [Online]. Available: http://www.poisonivy-rat.com/

[9] K. Lai y D. Wren. (2010, Enero). Internet Security Products Performance Benchmarking. [Online]. Available: http://www.passmark.com/ftp/antivirus_10-performance-testing-ed4.pdf