Índice general

CAPÍTULO 1

Antecedentes

1.1. Introducción

La seguridad informática ha sido y actualmente es un sector en el cual, empresas importantes de gran prestigio gastan cientos de millones de dólares para protegerse al estar conectados a una red [1], tal es la preocupación que a nivel mundial se registró una inversión en la seguridad informática de 75 billones de dólares en 2015 [2], mientras que, tanto chicas como medianas empresas suelen gastan un mínimo relacionado a este tema. En la actualidad, con la era de la revolución tecnológica por la que se está pasando, las empresas se han visto obligadas a contratar nueva tecnología para su producción, publicidad y/o servicios conectada al mundo de la Internet. Las empresas al estar conectadas a la Internet, están conectadas a millones de usuarios con cientos de posibilidades de acceso a los servicios de las empresas.

Cuando los usuarios se conectan a la red de Internet, están conectados todos los usuarios de la misma simultáneamente, esto conlleva un alto riesgo de inseguridad. Para tratar de disminuir el impacto provocado por amenazas informáticas, existen programas de computadora enfocados a detectar y proteger a los usuarios de la red contra los impactos provocados por las amenazas [3].

Hoy en día, existen diversos tipos de amenazas en la red, algunas son muy conocidas como virus informáticos que son diseñados para infectar archivos, pero no sólo existen ese tipo de amenazas diseñadas cierta forma con una actuación "automatizada". También existen las amenazas humanas o conocidos como Piratas informáticos, los cuáles, por medio de diversas técnicas de vulneración, pueden infectar, tomar el control o incluso obtener información o privilegios de computadoras o servidores con el fin de aprender o poner en práctica nuevas técnicas de vulneración, vender la información obtenida en el mercado negro o inclusive realizar un daño directo a los archivos o computadora objetivo [4][5].

Con el incremento de nuevos servicios web en Internet, se han creado y desarrollado diversos tipos de ataques hacia los servidores que proporcionan estos servicios. En los últimos años han ido en incremento los ataques web, aunque los que han tenido un mayor crecimiento y un gran impacto a nivel global, son los ataques tipo Cross-Site Scripting (de ahora en adelante XSS) [6].

1.2. Descripción del problema

Un ataque XSS ocurre cuando un atacante es capaz de inyectar un script, normalmente JavaScript, en la salida de una aplicación web de forma que se ejecuta en el navegador del cliente. Los ataques se producen principalmente por validar incorrectamente datos de usuario, y se suelen inyectar mediante un formulario web o mediante un enlace alterado.

Existen tres tipos de ataques XSS:

- XSS persistente o directo: este tipo de ataque consiste en embeber código HTML peligroso en sitios que lo permitan por medio de etiquetas <*script*> o <*iframe*>. Es la más grave de todas ya que el código se queda implantado en la web de manera interna y es ejecutado al abrir la aplicación web.

- XSS reflejado: en este tipo de ataque el código malicioso no queda almacenado en el servidor sino que se pasa directamente a la víctima. Es la forma más habitual de XSS. El ataque se lanza desde una fuente externa como un correo aparentemente inofensivo, un mensaje de chat u otro sitio web [8].

- XSS basado en DOM: es una variable de XSS persistente y reflejado. En un ataque XSS basado en DOM, la cadena maligna no es realmente analizada por el navegador de la victima hasta que el JavaScript legítimo de la página web es ejecutado. Estos códigos son ejecutados del lado del cliente, por lo que los filtros utilizados en el servidor no funcionan para este tipo de vulnerabilidades.

A la hora de lanzar un ataque de este tipo, los atacantes pueden utilizar varios tipos de inyección de código distinto. Los más utilizados son:

- Inyección en un formulario: se trata del ataque más sencillo. Consiste en inyectar código en un formulario que después al enviarlo al servidor, será incluido en el código fuente de alguna página. Una vez insertado en el código fuente, cada vez que se cargue la página se ejecutará el código insertado en ella.
- Inyección por medio de elementos: en este tipo de sistema de inyección de código se utiliza cualquier elemento que viaje entre el navegador y la aplicación, como pueden ser los atributos usados en las etiquetas HTML utilizadas en el diseño de la página.
- Inyección por medio de recursos: Aparte de los elementos en la URL y los formularios, hay otras formas en la que se puede actuar como son las cabeceras HTTP. Estas cabeceras son mensajes con los que se comunican el navegador y el servidor. Aquí entran en juego las *cookies*[1] y las sesiones [9].

Los daños potenciales que pueden causar un ataque XSS, pueden afectar tanto a los servidores en donde está contenida la aplicación web o pueden provocar serios problemas para el usuario final, éstos pueden varían en el grado de impacto, pueden ir desde una molestia para el usuario hasta un compromiso completo de la cuenta del mismo. Uno de los efectos más graves de los ataques XSS implica la divulgación de cookies de sesión del usuario, lo que permite a un atacante secuestrar la sesión del usuario y tomar control total de la cuenta. Otros ataques dañinos incluyen la divulgación de los archivos de los usuarios finales, la instalación de programas dañinos para el equipo del usuario final, redirigir al usuario a otra página o sitio web con fines malicioso, o modificar la presentación de los contenidos [10]. Los ataques XSS explotan vulnerabilidades no en

[1] Una cookie es un pequeño elemento de información que un servidor Web envía al navegador al visitar ciertas páginas web y que ambos comparten cada que este navegador vuelve a visitar [7].

el navegador del usuario, sino en las aplicaciones Web de terceros a las que accede el usuario. En este tipo de ataque el navegador no puede distinguir entre el contenido que un usuario haya podido incluir en una petición Web, y el contenido inyectado a través de un ataque XSS [11].

Se han desarrollado nuevas tecnologías que utilizan diferentes técnicas para poder detectar, contrarrestar y protegerse de los ataques tipo XSS [12], algunas de esas tecnologías son aplicadas en Cortafuegos de Aplicaciones Web (WAFs, por sus siglas en inglés), los Sistemas de Detección de Intrusos (IDSs, por sus siglas en inglés) e inclusive, las mismas empresas desarrolladoras de antivirus, han integrado nuevos módulos en sus sistemas en contra de este tipo de ataques [13].

Aunque se tiene registros de los problemas causados y el incremento que ha tenido este tipo de ataque, el principal objetivo de las tecnologías que se lanzan al mercado no es completamente enfocado a este ataque. Tal hecho provoca que al realizar auditorías de las herramientas en ésta parte de vulnerabilidades, se detecten fallos en el sistema, tales como falsos positivos o falsos negativos.

1.3. Solución propuesta

La propuesta para la solución a este problema, es desarrollar un sistema del tipo detector de intrusos con el fin de ayudar a los administradores web a tener una defensa y un alertador de ataques XSS que esté sufriendo su sitio o sistema.

1.4. Estado del arte

El interés por desarrollar sistemas que apoyan el análisis de textos se ha incrementado. En la tabla 1 se mencionan algunos sistemas que hacen uso de estos aplicado a diferentes problemáticas sociales.

Nombre	Descripción	Tipo	Año	Lugar de desarrollo
ChildDefence	La aplicación ChildDefence permite recolectar conversaciones (escritas en inglés) que un niño ha tenido con una persona, provenientes de mensajes de texto o chats en línea, y luego hacer que se analicen en el propio teléfono. La aplicación, ha sido entrenada para identificar si la persona es un niño o un adulto.	Gratuita	2011	Isis Forensics
LIWC	Es un programa de computadora analizador de textos, que determina el porcentaje de emociones expresadas en un texto, con base en diversas categorías.	Comercial	2001	Austin Texas University, EUA
KidsWatch	Es un programa de control parental. Funciona de tal manera que cuando en la conversación de un chat encuentra palabras referentes al sexo, drogadicción, armas, suicidio entre otros se les avisa a los padres acerca del comportamiento sospechoso.	Comercial	2002	Computer Business Solutions

Tabla 1.1: Comparativa de Sistemas que realizan análisis de textos

Dentro de la Escuela Superior de Cómputo, también se encontró un Trabajo Terminal que implementa procesamiento de lenguaje natural y minería de datos para la toma de decisiones. La descripción se encuentra en la tabla 1.

Nombre	Descripción	Tipo	Año	Lugar de desarrollo
Prototipo de sistema de información con minería de datos para la toma de decisiones. (20060106)	Sistema con una adaptación de minería de datos dirigida hacia las PyMES, obteniendo información relevante de sus bases de datos mostrando interpretaciones de los resultados de la minería en enunciados de lenguaje natural.	Trabajo Terminal	2006	ESCOM

Tabla 1.2: Trabajos Teminales relacionados con el procesamiento de lenguaje natural

1.5. Objetivo

1.5.1. Objetivo general

Desarrollar un sistema del tipo detector de intrusos con el fin de ayudar a los administradores web a tener una defensa y un alertador de ataques XSS que esté sufriendo su sitio o sistema.

1.5.2. Objetivos específicos

- Generar de forma artificial los ataques.
- Detectar y alertar de ataques XSS.
- Proteger al sistema de un ataque XSS de manera básica.
- Mostrar al usuario las estadísticas e información sobre los ataques que ha sufrido el sistema portador.

1.6. Justificación

La gran mayoría de los sistemas desarrollados hoy en día enfocados a la detección de intrusos basados en red, no tienen un gran soporte ante los ataques XSS, de tal forma que pueden llegar a fallar teniendo falsos positivos o falsos negativos [14][15], y las herramientas que lo tienen mejor implementado son adquiridas por empresas que puedan absorber el pago debido a su costo alto.

Para intentar solucionar tanto los ataques XSS persistentes como los no persistentes se sugiere implementar un sistema de filtrado y/o análisis, aunque estas soluciones pueden ser propuestos teóricamente como una tarea fácil, llevarlo a la práctica es mucho más complicado. Aunque la mayoría de ataques XSS conocidos están escritos en JavaScript e incrustados en documentos HTML, aunque también se pueden usar otras tecnologías como Java, Flash, ActiveX, etc., para efectuar los ataques, es por ello que es muy complicado la concepción de un proceso de filtrado y/o análisis genérico capaz de tratar el mal uso de dichos lenguajes.

La complejidad para ser detectados radica por una parte, en la utilización de *proxies*[2] de filtrado, especialmente en la parte del servidor, que introduce limitaciones importantes referentes a la escalabilidad y rendimiento de aplicaciones Web. Por otra parte, los scripts maliciosos pueden estar incrustados en los documentos intercambiados de manera ofuscada (por ejemplo codificando el código malicioso en hexadecimal o métodos de codificación avanzados) para no ser detectado ante estos filtros y analizadores [16].

Se considera este proyecto ya que será de ayuda a aquellas empresas y personas que deseen detectar ataques de tipo XSS dirigidos a las aplicaciones instaladas en sus servidores, implementando métodos de análisis de datos, como el aprendizaje máquina orientados a la seguridad informática haciendo más eficiente su funcionamiento. Y así alertar a los administradores para poder prever efectos irreversibles en el sistema o de manera más grave, una toma de control total o escalabilidad de permisos en el sistema anfitrión del servicio.

[2]Es una aplicación que "rompe" la conexión entre el cliente y el servidor [18].

CAPÍTULO 2

Marco Teórico

2.1. Detección de Intrusos

2.1.1. Definición

Detección de intrusos es el proceso de monitorear los eventos que ocurren en un sistema de cómputo o red y analizarlos por firmas o posibles incidentes que son violaciones o amenazas inminentes de violación de políticas de seguridad, políticas de uso aceptable o políticas de seguridad estándar. La prevención de intrusos es el proceso de realizar detección de intrusos e intentar detener el posible incidente detectado. Los sistemas de detección y prevención de intrusos (IDPS por sus siglas en inglés) son principalmente enfocados en identificar posibles incidentes, registrar información de ellos, intentar detenerlos y reportarlos al administrador de seguridad. La intrusión detectada puede ser efectuada desde el exterior y/o interior de una red o segmento que derive de ella. Algunas organizaciones usan los IDPSs con otros propósitos, ya sea para identificar problemas con sus políticas de seguridad, documentar las amenazas existentes o para disuadir a los individuos de violaciones de las políticas de seguridad [19].

2.1.2. Taxonomía de incidentes de seguridad

2.1.3. Modo de operación

Los IDSs están integrados por diversos módulos que trabajan en conjunto con funciones específicas la recolección de datos y el análisis de los mismos efectuados por un sistema, también la generación de alertas y una posible respuesta del tipo pasivo, activo o pro-activo. El registro de los resultados y datos que se obtiene se almacenan en bitácoras. El motor de detección de los IDSs emplea diversas formas de análisis dependiendo de su objetivo, algunas de estas formas son: estadísticos, de Inteligencia Artificial, Sistema Inmune, Machine Learning, como es este caso, entre otras formas. La operación de estos sistemas se puede contemplar en un ambiente aislado o con la interacción de otros controles de seguridad. Este último punto es muy importante tener en consideración, ya que dependiendo de dicha operación, afecta la forma en que opera el IDS y su configuración.

Los IDS pueden ser desarrolladas tanto en hardware como en software, cada uno con sus respectivas ventajas y desventajas. El desarrollo en hardware es un equipo de cómputo que debe ser implementado la arquitectura de una red, lo que implica una instalación y configuración por personas especializadas, la principal

ventaja de éste desarrollo consiste en una independencia de un equipo de cómputo, sino de la robustez de los circuitos integrados y las partes que lo constituyen. El segundo desarrollo, de software, se implementa para una operación dentro de un equipo de cómputo dedicado, el cuál dependerá totalmente del sistema operativo en el equipo, implicando esto una configuración de varios componentes del equipo, así como las propias exigencias que se requieran del equipo de cómputo; memoria, almacenamiento, velocidad de procesamiento, etc.). Su ventaja radica en que pueden ser implementados directamente sobre la aplicación o sistema a monitorear [17].

2.1.4. Justificación de los Sistemas de Detección de Intrusos

Los sistemas de detección de intrusos (IDS por sus siglas en inglés) es un control de seguridad que debe ser implementado junto con otros controles de seguridad para fortalecer yo complicar la acción de una contra-parte, como es el caso de un *cortafuegos*[3]. La implementación de estos dos controles de seguridad son comúnmente empleados ya que el trabajo del cortafuegos el filtrar el tráfico de la red con base a un análisis de filtrado de paquetes o un filtrado de estado. Así, los IDSs reciben tráfico filtrado y reconocido para su análisis de acuerdo a diversos criterios dependiendo de la taxonomía implementada (que se definirá después).

Existen hoy en día entidades que emplean IDS dentro de los cortafuegos, ya que son la primera línea de seguridad defensiva de una entidad, con el objetivo de complementar su sistema de filtrado, y así ser más eficiente y oportuno durante un ataque o intento de intrusión. Pero dicha implementación no es que sea mejor que una de forma separada entre controles, más bien radica en otros factores como la cantidad de dispositivos existentes en la entidad que lo va a implementar, la cantidad de información que va a procesar y principalmente los recursos monetarios disponibles de la entidad, haciendo mención también que al juntar estos controles, el tiempo de procesamiento de los datos dependería mucho del hardware del dispositivo, así haciendo dependiente el flujo sin retardos de la red al dispositivo. También hay que tener en consideración que si la implementación de diferentes controles de seguridad se hace en un mismo dispositivo, existe un mayor riesgo de que si el dispositivo falla o es comprometido, la entidad pueda sufrir un ataque o una intrusión.

[3]Un cortafuegos o *firewall*, por su nombre en inglés, son dispositivos o programas que controlan el flujo del tráfico de red entre redes o computadoras que emplean diferentes posturas de seguridad[20].

Bibliografía

[1] Kaplan J., Sharma S. & Weinberg A. (2011). "Meeting the cybersecurity challenge". McKinsey & Company. Recuperado 12 Marzo 2017, de http://www.mckinsey.com/business-functions/business-technology/our-insights/meeting-the-cybersecurity-challenge

[2] THE EDITORS AT CYBERSECURITY VENTURES. (2014). "The Cybersecurity Market Report covers the business of cybersecurity, including market sizing and industry forecasts, spending, notable M&A and IPO activity, and more..Çybersecurity Ventures. Recuperado 26 Septiembre 2016, de http://cybersecurityventures.com/cybersecurity-market-report/

[3] King, S. (2016). "Assessing the real risk of being online". ComputerWeekly. Recuperado 26 Septiembre 2016, de http://www.computerweekly.com/feature/Assessing-the-real-risk-of-being-online

[4] Computer Hope (2016). "Why do people hack computers?". Computerhope.com. Recuperado 26 Septiembre 2016, de http://www.computerhope.com/issues/ch001530.htm

[5] Cloudbric. (2016). "6 Reasons Why Hackers Want to Hack Your Website". Recuperado 26 Septiembre 2016, de https://www.cloudbric.com/blog/2015/10/6-reasons-why-hackers-want-to-hack-your-website/

[6] Imperva Inc. (2016). "2015 Web Application Attack Report (WAAR)". WAAR 2015. Recuperado de https://www.imperva.com/docs/HII_Web_Application_Attack_Report_Ed6.pdf

[7] Gutierrez, E. (2009). "JavaScript". 1st ed. Barcelona: Ed. ENI, p.233.

[8] Assis, R. (2016). "Primero post de la serie sobre vulnerabilidades XSS". Sucuri Español. Recuperado 19 Diciembre 2016, de https://blog.sucuri.net/espanol/2016/04/pregunte-sucuri-que-es-una-vulnerabilidad-xss.html

[9] (2016). "Qué es y cómo funciona un ataque Cross - Site Scripting". Hostalia. Recuperado 19 Diciembre 2016, de http://pressroom.hostalia.com/wp-content/themes/hostalia_pressroom/images/cross-site-scripting-wp-hostalia.pdf

[10] Ramos Pereira, K. (2016). Çross-Site Scripting". Revistasbolivianas.org.bo. Recuperado 20 Noviembre 2016, de http://www.revistasbolivianas.org.bo/scielo.php?pid=S1997-40442013000100023&script=sci_arttext

[11] (2014). "Su navegador esta desnudo: por qué los navegadores protegidos siguen siendo vulnerables.". Panda Security. Recuperado 27 Noviembre 2016, de http://resources.pandasecurity.com/enterprise/solutions/7.%20WP%20PCIP%20ESP%20Su%20Navegador%20esta%20desnudo.pdf

[12] Greene, T. (2016). "8 cyber security technologies DHS is trying to commercialize". Network World. Recuperado 26 Septiembre 2016, de http://www.networkworld.com/article/3056624/security/8-cyber-security-technologies-dhs-is-trying-to-commercialize.html

[13] (2016). "School of Computer Science and Information Technology University of Nottingham". Firewalls, Intrusion Detection Systems and Anti-Virus Scanners (p. 57). NOTTINGHAM NG8 1BB, UK. Recuperado de http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.107.2262&rep=rep1&type=pdf

[14] Mookhey , K. K., Nilesh, B. (2011). "Detection of SQL Injection and Cross-site Scripting Attacks — Symantec Connect". Symantec.com. Recuperado 26 Septiembre 2016, de http://www.symantec.com/connect/articles/detection-sql-injection-and-cross-site-scripting-attacks10

[15] Tim, K. (2016). "Strategies to Reduce False Positives and False Negatives in NIDS — Symantec Connect". Symantec.com. Recuperado 26 Septiembre 2016, de http://www.symantec.com/connect/articles/strategies-reduce-false-positives-and-false-negatives-nids

[16] Garcia-Alfaro, J. & Navarro-Arribas, G. (2005). "Prevención de ataques de Cross-Site Scripting en aplicaciones Web".Recuperado 25 Noviembre 2016, de http://www-public.tem-tsp.eu/~garcia_a/web/papers/recsi08-xss.pdf

[17] González Márquez, V. (2009). "Sistema de detección de intrusos basado en sistema experto (Tesis de maestría)". Centro de Investigación en Computación. México.

[18] National Institute of Standards and Technology,. (2007). "Guidelines on Securing Public Web Servers"(p. 121). Carlos M. Gutiérrez.

[19] National Institute of Standards and Technology,. (2007). "Guide to Intrusion Detection and Prevention Systems (IDPS)"(p. 9). Scarfone K. & Mell P.

[20] National Institute of Standards and Technology,. (2009). "Guidelines on Firewalls and Firewall Policy"(p. 7). Scarfone K & Hoffman P.