Serie Científica de la Universidad de las Ciencias Informáticas
Vol. 9, No. 9, Septiembre, 2016
ISSN: 2306-2495 | RNPS: 2343
http://publicaciones.uci.cu
Pág. 51-69

Tipo de artículo: Artículo original
Temática: Desarrollo de sistemas informáticos
Recibido: 22/09/2016 | Aceptado: 28/09/2016

Integración de un sistema de detección de intrusos y un escáner de vulnerabilidades para la detección efectiva de ataques informáticos

Integration of a system of detection of intruders and a scanner of vulnerabilities for the effective detection of information-technology attacks

Lázaro, Rodríguez Iturralde[1]

[1]*Universidad de las Ciencias Informáticas, Cuba*

[*] Autor para correspondencia: lacho@uci.cu

Resumen

En el mundo de hoy las empresas y organizaciones son completamente dependientes de la tecnología para llevar a cabo sus objetivos, debido a que las informaciones críticas son almacenadas, procesadas y transmitidas en formato digital. En un entorno donde el desarrollo tecnológico ha posibilitado la conexión a internet desde cualquier lugar y mediante múltiples dispositivos electrónicos, los sistemas informáticos se encuentran constantemente expuestos a múltiples amenazas. Teniendo en cuenta el crecimiento exponencial de los programas malignos, las nuevas vulnerabilidades de las aplicaciones informáticas descubiertas diariamente y la organización cada vez más estructurada de los atacantes informáticos; es evidente la necesidad de contar con un sistema de seguridad que detecte de manera efectiva los ataques a las redes de datos. La UCI no cuenta en la actualidad con un sistema de detección de intrusos (IDS) que permita detectar en tiempo real los ataques cibernéticos que se producen desde las redes externas. El presente trabajo describe la integración del IDS Snort y el escáner de vulnerabilidades OpenVas, mediante la herramienta de seguridad OSSIM, la cual posibilita la correlación de información entre ambos sistemas, para detectar de manera efectiva los ataques informáticos a la red de la UCI.

Palabras Claves: Sistema de Detección de Intrusos, escáner de vulnerabilidades, ataques cibernéticos, ataques informáticos, SIEM, Snort, OpenVas, OSSIM

Serie Científica de la Universidad de las Ciencias Informáticas
Vol. 9, No. 9, Septiembre, 2016
ISSN: 2306-2495 | RNPS: 2343
http://publicaciones.uci.cu
Pág. 51-69

Abstract

In today's world companies and organizations they are completely dependent on technology to accomplish their goals, because critical information are stored, processed and transmitted in digital format. In an environment where technological development has enabled the internet from anywhere through multiple electronic devices, computer systems are constantly exposed to multiple threats. Given the exponential growth of malware, new vulnerabilities discovered daily applications and the increasingly structured organization of computer attackers; Clearly the need for a security system that effectively detect attacks on data networks. The present work illustrates the integration of the IDS Snort and the scanner of vulnerabilities OpenVas, by means of the tool of certainty OSSIM, which makes possible the correlation of information between both systems, to detect of effective way the information-technology attacks to the network of her UCI.

Keywords: *Intrusion detection system, vulnerability scanner, cyber attacks, hacking, SIEM, Snort, OpenVas, OSSIM*

Introducción

Los En el mundo de hoy las empresas y organizaciones son completamente dependientes de la tecnología para llevar a cabo sus objetivos, debido a que las informaciones críticas son almacenadas, procesadas y transmitidas en formato digital. Desde el surgimiento de internet las redes de datos fueron interconectadas y por tanto la información que transita por las mismas quedó expuesta a múltiples amenazas que constantemente están presentes a nivel global.

En la 14 edición anual de la conocida encuesta de seguridad del Instituto de Seguridad de Computadoras - CSI, por sus siglas en inglés - se muestran las pérdidas de cada encuestado. Para tener una idea, de un total de 443 encuestados de diferentes empresas e instituciones, el promedio de pérdidas debido a los incidentes de seguridad es de 234,244 dólares anuales. (RICHARDSON ROBERT 2009)

En la UCI, existe una alta concentración de tecnología y una gran cantidad de proyectos productivos que trabajan con información sensible. La UCI no está exenta de los ataques cibernéticos y los servidores ubicados en la zona desmilitarizada (DMZ), son objetivos claves para este tipo de ataques, debido a que se encuentran expuestos directamente a las amenazas y peligros de Internet. En análisis realizados por los administradores de la red a los flujos de datos externos, se han detectado intentos de conexión fallidos a través de protocolos para la administración remota,

tanto de servidores como de equipos de interconexión, así como la penetración de virus informáticos que han causado efectos indeseables en los servidores centrales y en las estaciones de trabajo.

La UCI no cuenta en la actualidad con un sistema de detección de intrusos que permita detectar en tiempo real los ataques cibernéticos que se producen desde las redes externas. Sin embargo, la utilización de este tipo de sistemas genera una gran cantidad de alertas, que en muchas ocasiones representan falsos positivos, por lo que los administradores de la red pueden pasar por alto ataques reales que se estén produciendo, al no poder identificarlos de manera efectiva entre todas las notificaciones que producen los IDS. De ahí la importancia de la utilización de un IDS que sea efectivo en la generación de alarmas, de manera tal que sus notificaciones estén acordes con los sistemas y las vulnerabilidades reales existentes, que pudieran haber sido detectadas previamente por un escáner de vulnerabilidades.

Materiales y métodos

Con el objetivo de analizar los sistemas que permiten la detección efectiva de ataques informáticos, se explican en este acápite los IDS, como sistemas de detección de ataques por excelencia, los escáneres de vulnerabilidades, cuya información debe ser correlacionada con la de los IDS, para hacer más efectivas las alarmas y disminuir los falsos positivos; y una herramienta que permita integrar ambos sistemas.

Estado del arte

Componentes de un sistema de Detección de intrusos.

Un IDS está compuesto por un sniffer o rastreador, un procesador, un motor de detección y una base de datos.
El rastreador o sniffer de paquetes es un dispositivo usado para intervenir disimuladamente dentro de la red. Funciona de manera similar a un interceptor de llamadas telefónicas, pero éste es usado para datos que circulan sobre la red. Permite a una aplicación o al hardware interceptar datos disimuladamente en el tráfico de la red. El preprocesador toma los paquetes recogidos y los revisa en base a ciertos plugins. Una vez que se determina el tipo de comportamiento del paquete, este se envía al motor de detección. El motor de detección toma los datos que vienen del preprocesador y los plugins, y esa información es revisada a través de un conjunto de reglas. Si las reglas corresponden con la información contenida en algún paquete, estos son enviados al procesador de alertas y almacenadas en la base de datos del servidor. Estos componentes se muestran en la figura 1.(ALBARRAN BRAVO GLADIS and GARDUÑO GÓMEZ NOA 2010)

Serie Científica de la Universidad de las Ciencias Informáticas
Vol. 9, No. 9, Septiembre, 2016
ISSN: 2306-2495 | RNPS: 2343
http://publicaciones.uci.cu
Pág. 51-69

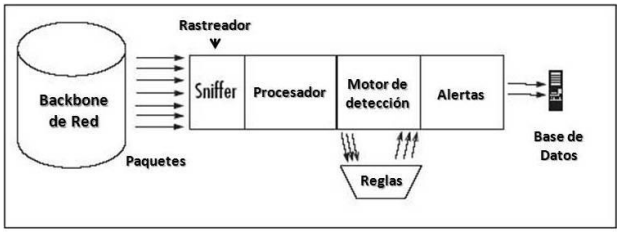

Figura 1. Componentes de un IDS.

Selección del sistema de detección de intrusos a utilizar.

La selección del IDS se decide teniendo en cuenta las políticas de migración a software libre del país y de la UCI. De los IDS basados en software libre la solución más madura, estable y conocida es Snort, el cual es comparable con muchos de los sistemas propietarios.

El funcionamiento de Snort es similar al de un sniffer ya que monitoriza todo el tráfico de la red en búsqueda de cualquier tipo de intrusión e implementa un motor de detección de ataques y barrido de puertos que permite registrar, alertar y responder ante cualquier anomalía previamente definida como patrones.

Está disponible bajo licencia GPL, es gratuito y funciona bajo plataformas Windows y GNU/Linux. Es uno de los más usados y dispone de una gran cantidad de filtros o patrones ya predefinidos, y actualizaciones constantes.

Escáneres de vulnerabilidades

Los escáneres de vulnerabilidades son un conjunto de aplicaciones que nos permiten realizar pruebas de ataque para determinar si una red o un equipo tienen deficiencias de seguridad que pueden ser explotadas por un posible atacante o comunidad de atacantes.

Los escáneres de vulnerabilidades poseen una estrecha relación con las herramientas de detección utilizadas en los sistemas de detección de intrusos. En realidad, en muchos ámbitos se les considera un caso especial de estas herramientas y, generalmente, son utilizados para realizar un análisis de intrusiones.(TORNILV PERRAMÓN XAVIER 2004)

Serie Científica de la Universidad de las Ciencias Informáticas
Vol. 9, No. 9, Septiembre, 2016
ISSN: 2306-2495 | RNPS: 2343
http://publicaciones.uci.cu
Pág. 51-69

Selección del escáner de vulnerabilidades a utilizar

Teniendo en cuenta el cierre del código de Nessus[1] y por ende el cambio a software propietario. La selección del escáner de vulnerabilidades se decide teniendo en cuenta las políticas de migración a software libre del país y de la UCI. De los escáneres de vulnerabilidades basados en software libre la solución más, estable y conocida es OpenVas desarrollado a partir del código de Nessus, este escáner es comparable con muchos de los sistemas propietarios analizados.

Sistema de gestión de eventos e información de seguridad (SIEM)

La tecnología SIEM integra varias herramientas de seguridad con el fin de recoger, ordenar, correlacionar la información sobre el estado de la red; los comportamientos de sistemas y usuarios, la información de estados de máquinas y la información viva en la red, lo que sirve a los administradores de seguridad para encontrar indicios de ataques que hayan ocurrido o que pudieran suceder en un futuro. (ESPINOZA P MARIA *et al.* 2007)

Este tipo de herramientas sirve para automatizar todo el proceso de almacenamiento, tratamiento y explotación de trazas para ofrecer capacidades proactivas ante problemas y facilidades para extraer información concreta.(SEGURIDAD INFORMATICA. RED SOCIAL SOBRE SEGURIDAD INFORMÁTICA 2008)

Entender lo que realmente acontece en una red corporativa es algo muy complejo. Actualmente, es necesario centralizar la retención e interpretación de trazas y eventos generados por los más diversos aplicativos y sistemas de la red.

El concepto de SIEM es relativamente nuevo. Surgió en 1999 y evoluciona gradualmente con nuevas funciones. Una característica importante es el análisis de los datos, lo cual lo diferencia de un administrador de trazas estándar.

La gran mayoría de los sistemas y aplicaciones disponibles en una red corporativa genera eventos que son almacenados en trazas. Esencialmente, es una lista grande de eventos ordenada cronológicamente. Existen protocolos específicos para transportar estos eventos. Un buen SIEM debe ofrecer formas flexibles de recolectar los eventos

La capacidad que poseen los sistemas SIEM para centralizar información de logs de seguridad, permite correlacionar la información de las diferentes herramientas, por lo que es posible utilizar este tipo de sistemas para correlacionar la información de un IDS y un escáner de vulnerabilidades.

[1] El software continúa siendo libre. Las plugins de Nessus constituyen lo privativo del escáner.

Serie Científica de la Universidad de las Ciencias Informáticas
Vol. 9, No. 9, Septiembre, 2016
ISSN: 2306-2495 | RNPS: 2343
http://publicaciones.uci.cu
Pág. 51-69

Sistemas de gestión de eventos e información de seguridad existentes.

La consultora Gartner centrado realizó un estudio de las herramientas SIEM más utilizadas durante el año 2011. De dicho análisis se puede determinar que la única solución basada en software libre es AlienVault, cuyo núcleo es el sistema OSSIM, el cual se distribuye bajo licencia GPL, por lo que es el sistema SIEM objeto de estudio en este capítulo. El resto constituyen herramientas propietarias.(GARTNER S.A 2012)

Open Source Security Information Management (OSSIM).

OSSIM es una solución reconocida por más del 80% de los profesionales del mercado de la seguridad y recibe más de 200.000 descargas anuales con clientes e implantaciones en todos los sectores: empresa de telecomunicaciones Telcos, gobierno, servicios, industrias, entre otros. y en todos los países del mundo.(SOFTWARELIBRE NET 2011)

OSSIM - herramienta de monitorización de seguridad - tiene como objetivo ofrecer un marco para centralizar, organizar y mejorar las capacidades de detección y visibilidad de los eventos de seguridad de la organización.

Es una solución de seguridad, que puede ser personalizada a las necesidades de cada organización. Permite tener una visibilidad de todos los eventos de los sistemas en un punto central y en un mismo formato. Mediante la correlación permite relacionar y procesar la información minimizando así los falsos positivos y falsos negativos.

El producto de la compañía, AlienVault Unified SIEM, aporta una plataforma unificada para la gestión de toda la información relativa a las redes empresariales, y, además de las características de las ofertas puramente SIEM. Ofrece también capacidades adicionales, como son análisis de vulnerabilidades y amenazas, IDS, WIDS, HIDS, y monitorización e inventario de recursos, entre otras

Componentes de Open Source Security Information Management.

Servidor. Es el componente principal de OSSIM. Se encarga de recibir los eventos enviados por los distintos agentes. También realiza las funciones de priorización y correlación

Sensor. Son servidores distribuidos en diferentes segmentos de red, para monitorear los distintos eventos. Esta distribución es en base a los servicios que se van a monitorear. Cada agente o sensor tendrá configurado un conjunto de detectores o monitores, que generan eventos para que el agente los recolecte y reporte al servidor central.

Serie Científica de la Universidad de las Ciencias Informáticas
Vol. 9, No. 9, Septiembre, 2016
ISSN: 2306-2495 | RNPS: 2343
http://publicaciones.uci.cu
Pág. 51-69

Base de datos. Es el lugar donde se almacenan los diferentes eventos recolectados por los agentes, y las configuraciones de las distintas herramientas y OSSIM.

Framework. Es el intermediario entre el servidor central y el usuario. Es la herramienta de administración utilizada para configurar y organizar los diferentes módulos tanto externos como propios que integra OSSIM. Mediante este se puede definir una topología, inventariar activos, definir políticas de seguridad, definir reglas de correlación y unir las diferentes herramientas integradas.(ESPINOZA P MARIA *et al.* 2007)

Funcionamiento básico de Open Source Security Information Management

Los nueve niveles de funcionalidad de OSSIM se muestran en la figura 2 de manera simplificada:

Figura 2. Niveles de funcionalidades de OSSIM**.**

Procesos que tienen lugar dentro de AlienVault OSSIM: las aplicaciones generan eventos de seguridad, los eventos son recogidos y normalizados, los eventos son enviados a un servidor central, valoración del riesgo de cada evento, correlación de eventos, almacenamiento de los eventos, acceso a los eventos almacenados, acceso a la configuración, acceso a métricas e informes, acceso a información en tiempo real del estado de nuestra red.

Los eventos de seguridad son generados por las diferentes aplicaciones y/o dispositivos con que se disponga en la red. Estos eventos son recogidos y normalizados por el sensor, que se encarga además de enviarlos a un servidor central. En un despliegue de la herramienta se puede disponer de tantos sensores como se necesiten. Como ejemplo, se puede situar un sensor dentro de la DMZ, un sensor en cada ciudad o dedicar un sensor para monitorizar cada una de las redes de la corporación.

El Sensor incluye una serie de herramientas entre ellas Snort y OpenVAS que permiten analizar todo el tráfico de red en busca de problemas de seguridad y anomalías. Para poder sacar provecho de esta funcionalidad de AlienVault es imprescindible que el sensor sea capaz de ver todo el tráfico de la red, bien sea utilizando un concentrador, o configurando un puerto espejo en la lógica de red.

Todos los sensores envían sus eventos a un único servidor, que se encarga de efectuar una valoración del riesgo para cada evento, y en el que también tendrá lugar el proceso de correlación. Una vez que estos dos procesos han tenido lugar, los eventos son almacenados en la base de datos.

Para tener acceso a toda esta información, así como a la configuración del sistema y a una serie de métricas e informes se hará uso de la consola web de AlienVault. Desde esta consola web también se tendrá acceso a información en tiempo real a una serie de aplicaciones que facilitan el análisis del estado global de nuestra red.(LORENZO MANUEL JUAN 2009).

Correlación de eventos en Open Source Security Information Management

La correlación de eventos es un proceso que toma como datos de entrada las alertas producidas por uno o varios IDS y proporciona una visión de los eventos ocurridos en la red, a un nivel más alto.

AlienVault OSSIM trabaja directamente con el IDS Snort y el escáner de vulnerabilidades OpenVAS y además incluye un motor de correlación de gran alcance que proporciona análisis de miles de eventos generados por Snort y OpenVAS, con el objetivo de identificar los ataques o problemas de una manera que puede ser fácilmente tratada por los operadores humanos.

Un objetivo importante de la correlación de eventos de seguridad es la lucha contra el enorme volumen de falsos positivos creados por un IDS y dispositivos de seguridad en general. Las organizaciones reciben millones de ellos por día, haciendo imposible que un administrador pueda revisar todo. AlienVault OSSIM con sus reglas y directivas de correlación puede comprobar estos hechos mediante la búsqueda de pruebas para verificar si son ataques reales o no. Por defecto le da un valor bajo a la "fiabilidad" de parámetros de la mayoría de los acontecimientos, que no hará sino crecer en cuanto a los controles previstos por la correlación positiva de resultados del motor.

Implementación y configuración.

El nodo central de comunicaciones de la UCI cuenta con enrutador Cisco que se encarga de encaminar todo el tráfico de red entre la red de área local (LAN) y red de área amplia - WAN. Entre ambas redes se encuentra un cortafuego

Serie Científica de la Universidad de las Ciencias Informáticas
Vol. 9, No. 9, Septiembre, 2016
ISSN: 2306-2495 | RNPS: 2343
http://publicaciones.uci.cu
Pág. 51-69

utilizado como mecanismo de control de acceso a nivel de red. Su principal función es prevenir accesos no permitidos al interior de la red, así como controlar el tráfico de información que circula entre ambas redes permitiendo o denegando los protocolos TCP/IP.

Para dicho control se definen un grupo de listas de control de acceso (ACL) que bloquean todos los puertos de acceso hacia la red UCI que no están permitidos, actúa de barrera entre los servidores de la DMZ y la red LAN UCI. Sólo el tráfico autorizado en las políticas de seguridad locales del cortafuego podrá traspasar el bloqueo.

Una DMZ o red perimetral es una red local o subred localizada entre la red interna de una organización y una red externa. El objetivo de una DMZ es separar la red interna de la red externa. La DMZ se usa habitualmente para ubicar servidores que es necesario que sean accedidos externamente de la red, tales como servidores intercambiadores de correo electrónico, web y servidor de nombres de dominio (DNS).

Los servidores ubicados en la DMZ se encuentran de cara a Internet, por lo que están más expuestos a cualquier ataque cibernético desde las redes externas, responden a direcciones IP oficiales, aunque físicamente tienen un número IP privado que es enmascarado en el traductor de direcciones de red - Network Address Translation - NAT que es un mecanismo utilizado por enrutadores IP para intercambiar paquetes entre dos redes que se asignan mutuamente direcciones incompatibles. Dentro de los servidores ubicados en la DMZ de la UCI se encuentran: servidores DNS, servidor para mensajería instantánea que utiliza el protocolo extensible de mensajería y comunicación de presencia - Extensible Messaging and Presence Protocol- XMPP, servidor intercambiador de correo electrónico, Servidor protocolo de transferencia de datos -File Transfer Protocol – FTP, servidor proxy inverso.

La figura 3 muestra la topología de red del nodo central[2].

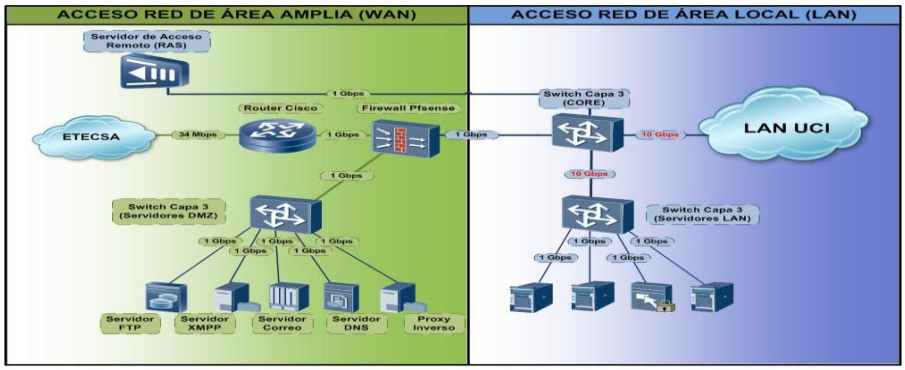

Figura 3. Diagrama de red nodo central UCI.

[2] Solo se reflejan las informaciones necesarias para la ubicación del servidor de Alien Vault OSSIM.

Serie Científica de la Universidad de las Ciencias Informáticas
Vol. 9, No. 9, Septiembre, 2016
ISSN: 2306-2495 | RNPS: 2343
http://publicaciones.uci.cu
Pág. 51-69

En el cortafuego se definen ACL para el acceso solicitado desde las IP externas de la red WAN teniendo en cuenta los protocolos de red permitidos a los servidores de la DMZ de la UCI.

Diseño de la ubicación de OSSIM en el nodo central de la UCI

La UCI cuenta con datos estadísticos que reflejan el comportamiento de eventos de seguridad los que han sido detectados en análisis de las trazas generadas por los servidores de la DMZ. Estos eventos pueden considerarse ataques informáticos y ponen en riesgo su seguridad lógica.

Los protocolos más comunes usados en este tipo de conexión se revelan en la figura 6 sin descartar que cualquier puerto pueda ser usado para provocar una anomalía en la red. Se muestra también un grupo nombrado "desconocidos", donde se encuentran una serie de puertos no conocidos pero que son utilizados para intentos de conexión. Estos son intentos de conexión no permitidos hacia los servidores de la DMZ de la red de la UCI se muestran en la figura 4

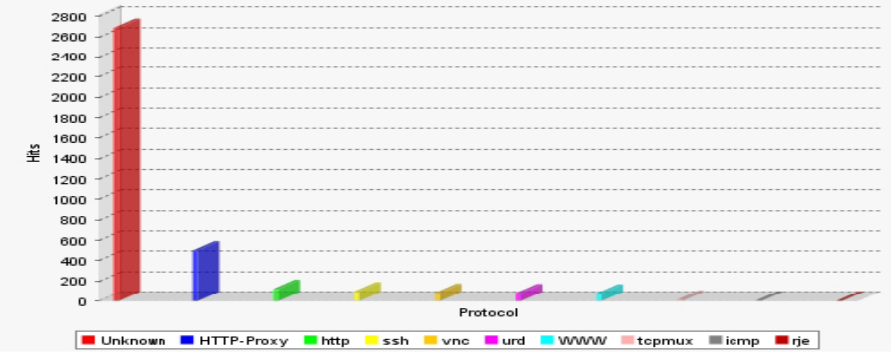

Figura 4.Gráfica de Intentos vs Protocolos[3].

Al analizar esta serie de incidentes de seguridad es de vital importancia garantizar un alto nivel de seguridad para los servidores de la DMZ, por tal razón se definió la ubicación de la herramienta Alien Vault OSSIM detrás del cortafuego. La instalación es centralizada teniendo en cuenta que la cantidad de servidores a monitorear no excede la cantidad de 10 y el nivel de tráfico no es muy alto. Sólo se captura el tráfico de la red WAN, en la red LAN el tráfico es mayor. Además, las características de hardware del servidor donde se instala permiten hacer este tipo de instalación. Será interconectado a un puerto espejo en el swicht L3 que se utilizará para la captura de todo el tráfico de

[3] Información suministrada por los administradores de red de la UCI.

Serie Científica de la Universidad de las Ciencias Informáticas
Vol. 9, No. 9, Septiembre, 2016
ISSN: 2306-2495 | RNPS: 2343
http://publicaciones.uci.cu
Pág. 51-69

red. Esta ubicación permite analizar de manera directa todo el tráfico que entra en la red y que sobrepasa el cortafuego. Permite vigilar que el cortafuego funcione como debe. En redes grandes, el volumen de tráfico puede ser excesivo, por lo que el análisis debe simplificarse convirtiéndose únicamente en un primer análisis para detectar los posibles ataques cibernéticos a que puedan ser expuestos los servidores de la DMZ (VIZCAÍNO DÍAZ MIGUEL LUIS 2003). En la figura 5 se muestra el diagrama de despliegue de Alien Vault OSSIM.

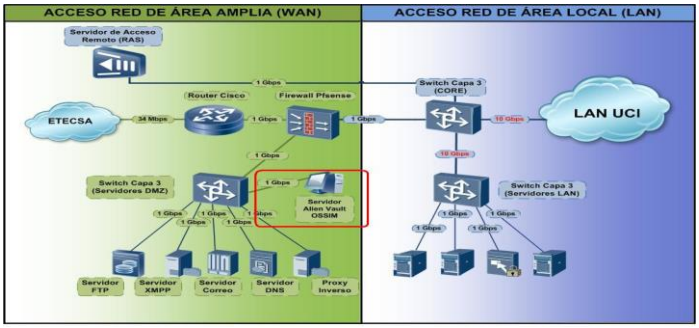

Figura 5. Diagrama de despliegue de Alien Vault OSSIM en el nodo central UCI.

Correlación cruzada a bajo nivel

La correlación cruzada es un mecanismo que se lleva a cabo con eventos que tiene una dirección IP definida. La razón de esto es porque podemos verificar si el destino del evento tiene alguna vulnerabilidad definida en la base de datos. A algunos eventos como los del tipo sistema operativo o control de acceso al medio - media access control - MAC no se les puede aplicar una correlación cruzada, debido a que esos tipos de eventos no tienen una dirección IP de destino definida, sino que únicamente se refieren a un Host en específico.

Escaneo de vulnerabilidades

Para crear reglas de correlación cruzada que sean efectivas ante la detección de eventos de seguridad por parte del IDS, es necesario un escaneo profundo de la subred del entorno de pruebas con el escáner de vulnerabilidades OpenVAS. Esto permite conocer las vulnerabilidades con que constan los servido.

Antes de realizar el trabajo de escaneo es necesario crear un perfil de escaneo donde se introducirán las credenciales - nombre de usuario y contraseña - de los activos a monitorear. Se auto habilitarán todos los plugins por categorías. Esto permite un escaneo a profundidad ya que OpenVas puede hacer una revisión exhaustiva de las máquinas.

Serie Científica de la Universidad de las Ciencias Informáticas
Vol. 9, No. 9, Septiembre, 2016
ISSN: 2306-2495 | RNPS: 2343
http://publicaciones.uci.cu
Pág. 51-69

Reglas de correlación cruzadas

Las reglas de correlación cruzada se crean a partir de los eventos de seguridad recibidos en el servidor por parte del sensor. El nombre del evento constituye el dato de origen detectado por el IDS Snort, se complementa con el nombre de la vulnerabilidad detectada por el escáner de vulnerabilidades OpenVas. Ambos datos forman el plugin_sid que darán lugar a la regla de correlación cruzada a crear por parte del administrador, la cual tendrá la función de generar una alarma para la vulnerabilidad existente una vez recibido un ataque.

Resultados y discusión

El objetivo de la validación es comprobar el funcionamiento real de la correlación cruzada de Alien Vault OSSIM, como método que permite la integración del IDS Snort con el escáner de vulnerabilidades OpenVas.

Red física de entorno de prueba

Teniendo en cuenta la existencia de software que permiten disponer de máquinas virtuales a un coste reducido, la mayoría de los estudios relacionados con la seguridad se realizara a partir de un sistema virtual, el cual permite ser configurado con servicios vulnerables en entornos controlados. De encontrarse en un entorno de red física real, podrían conducir a resultados no deseados o incluso ser víctimas de ataques durante el proceso de estudio.

De este modo se han considerado las siguientes necesidades fundamentales a la hora de definir el sistema. Diseñar un esquema de red vulnerable aislada del interior y en un entorno controlado donde estén presentes las máquinas que van a intervenir en la validación de la propuesta de integración en estudio. Estos sistemas son: un atacante, dos víctimas y la herramienta Alien Vault OSSIM con todos sus perfiles instalados y configurados: sensor, base de datos, servidor, y el framework. En la figura 6 se describe el diseño de la arquitectura de red del entorno de pruebas.

Serie Científica de la Universidad de las Ciencias Informáticas
Vol. 9, No. 9, Septiembre, 2016
ISSN: 2306-2495 | RNPS: 2343
http://publicaciones.uci.cu
Pág. 51-69

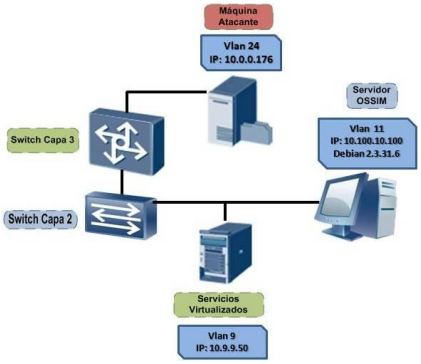

Figura 6. Diseño real de la arquitectura de red física del entorno de pruebas.

Red virtual de entorno de prueba

Una vez configurados los equipos, se prescinde del modelo físico. El trabajo en el modelo virtual de la red, se muestra en la figura 7, donde se describe cada equipo del entorno de pruebas. La máquina 10.0.0.176, mantiene la configuración expuesta anteriormente.

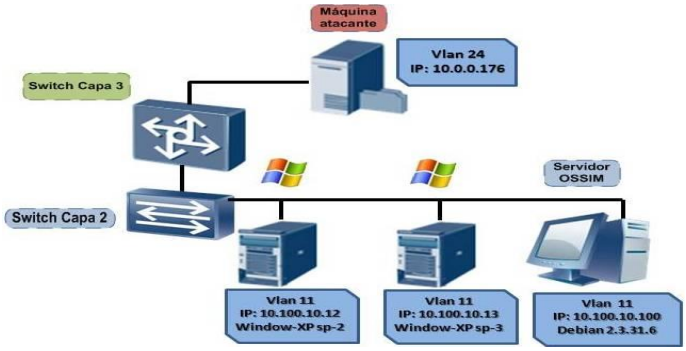

Figura 7. Diseño real de la arquitectura de red virtual del entorno de pruebas.

El objetivo del entorno de pruebas es ejecutar ataques informáticos contra una máquina que presente vulnerabilidades y otra que no las tenga, para comprobar la correlación cruzada del servidor de Alien Vault OSSIM, el cual debe generar alarmas de mayor impacto cuando detecta ataques dirigidos contra sistemas vulnerables.

Resultado del trabajo de escaneo

Para el escaneo del entorno virtual de pruebas se creó el perfil nombrado validación donde se auto habilitaron todos los plugin por categorías y se editaron las credenciales de acceso a los equipos. Como resultado de este escaneo se obtuvieron las siguientes vulnerabilidades clasificadas en: serias, altas, medias, bajas e informativas.

Serie Científica de la Universidad de las Ciencias Informáticas
Vol. 9, No. 9, Septiembre, 2016
ISSN: 2306-2495 | RNPS: 2343
http://publicaciones.uci.cu
Pág. 51-69

A partir de las vulnerabilidades detectadas se hizo una búsqueda de las mismas en la Base de datos de código abierto de vulnerabilidades - open source Vulnerability Database - OSVDB con el objetivo de verificar la existencia de identificadores de Snort y OpenVas que permitan la creación de reglas de correlación cruzada, para la detección de un ataque a partir de un exploit previamente identificado.

Descripción de las vulnerabilidades

La vulnerabilidad elegida para la validación del sistema se identifica dentro de los tickets con el número VUL13 y responde al siguiente nombre: Server Service Could Allow Remote Code Execution Vulnerability (958644), la cual responde al identificador (ID) 49243 en la OSVDB (OSVDB 2012).

La actualización de seguridad corrige la vulnerabilidad al modificar la forma en que el servicio de servidor trata las solicitudes a llamada a procedimiento remoto - remote procedure call - RPC(CORPORATION 2008)

Pruebas de validación.

El exploit escogido para explotar la vulnerabilidad detectada por OpenVas se encuentra disponible para su descarga en la base de datos de exploit - exploit database - EDB con el ID 7132 diseñado para la vulnerabilidad CVE-2008-4250 el cual será utilizado con la herramienta Armitage encargada de realizar el ataque a las máquinas del entorno de pruebas.

Nombre del exploit: *MS Windows Server Service Code Execution Exploit* (MS08-067) (2k/2k3)(DEBASIS 2008).

A partir del plugin_sid de Snort: Snort: "SHELLCODE x86 OS agnostic fnstenv geteip dword xor decoder" y la vulnerabilidad Server Service Could Allow Remote Code Execution Vulnerability (958644), detectada por el escáner de vulnerabilidades OpenVas. Se crea la regla de correlación cruzada 9270 de las 9269 ya existentes.

Antes de comenzar el ataque con Armitage se carga el exploit para la máquina víctima instalada en el entorno virtulizado con la dirección ip 10.100.10.12 y el sistema operativo Windows XP-sp2. El ataque tendrá lugar por el puerto 445. Dentro de las opciones del payload, se activará la creación en la máquina víctima del usuario **ataque** con la contraseña ***1234567*** como se muestra en la figura 8

Serie Científica de la Universidad de las Ciencias Informáticas
Vol. 9, No. 9, Septiembre, 2016
ISSN: 2306-2495 | RNPS: 2343
http://publicaciones.uci.cu
Pág. 51-69

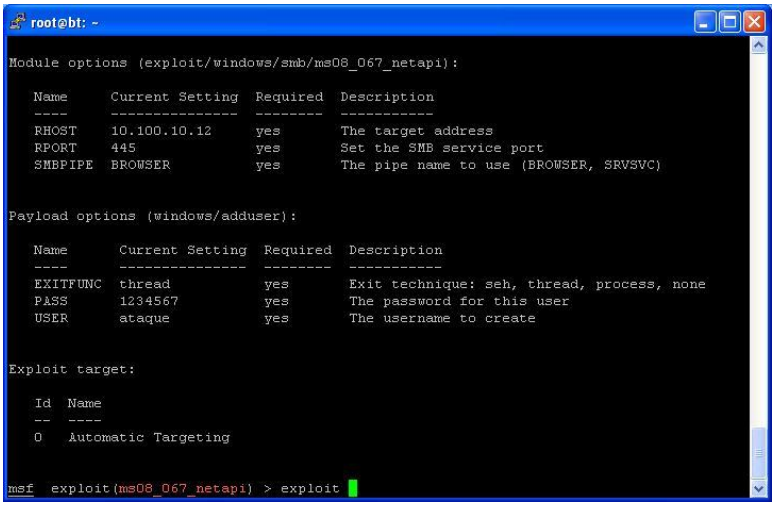

Figura 8. Cargando exploit ms08_067_netapi.

Ataque lanzado contra la PC con Windows XP-sp2

El ataque es lanzado con exito contra la PC con Windows XP-sp2 con ip 10.100.10.12 como se muestra en la figura 9

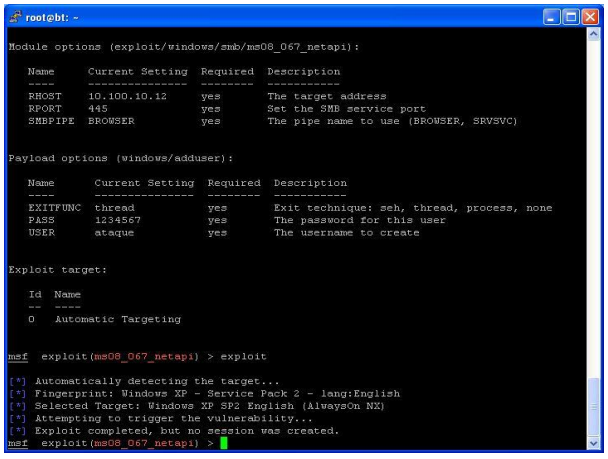

Figura 9. Ataque lanzado con éxito.

Para verificar la efectividad de la herramienta Alien Vault OSSIM se accede al panel de alarmas para constatar que la regla de correlación cruzada es capaz de lanzar la alarma prevista teniendo en cuenta la existencia de la vulnerabilidad en esta máquina. El sistema muestra la alarma en la sección incidencias alarmas.

Serie Científica de la Universidad de las Ciencias Informáticas
Vol. 9, No. 9, Septiembre, 2016
ISSN: 2306-2495 | RNPS: 2343
http://publicaciones.uci.cu
Pág. 51-69

Los eventos de seguridad que son detectados por el IDS Snort se constatan en la sección análisis eventos de seguridad SIEM.

Se reportaron por parte de Snort tres eventos de seguridad en Alien Vault OSSIM: Snort: "NETBIOS SMB srvsvc NetrPath Canonicalize unicode little endian overflow attempt", Snort: snort: "ET ATTACK_RESPONSE Rothenburg Shellcode", Snort: "SHELLCODE x86 OS agnostic fnstenv geteip dword xor decoder".

La máquina víctima antes del ataque solo contaba con el usuario: administrator, una vez lanzado el ataque se crea el usuario ataque, demostrando de esta manera la efectividad del mismo como se muestra en la figura 10

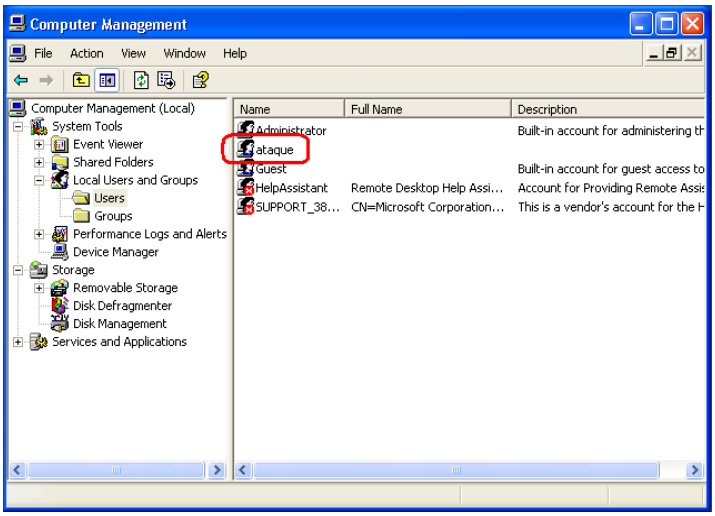

Figura 20. Usuario creado en la máquina víctima.

Ataque lanzado contra la PC con Windows XP-sp3

El ataque es lanzado contra la PC con Windows XP-sp3 con ip 10.100.10.13 como se muestra en la figura 11

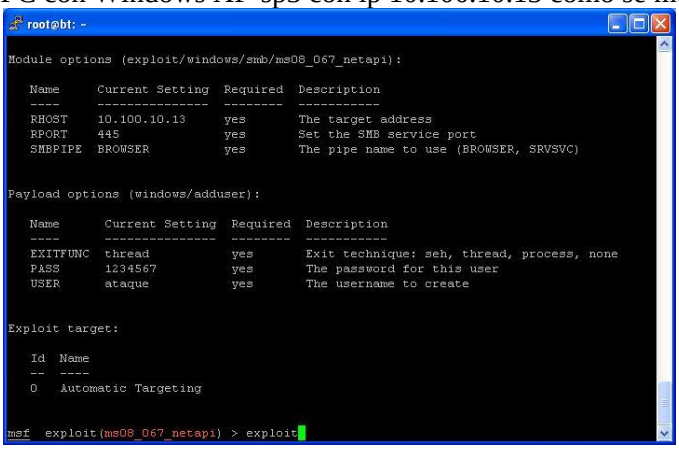

Figura 11. Lanzando Exploit ms08_067_netapi a máquina con Windows XP-sp3.

Serie Científica de la Universidad de las Ciencias Informáticas
Vol. 9, No. 9, Septiembre, 2016
ISSN: 2306-2495 | RNPS: 2343
http://publicaciones.uci.cu
Pág. 51-69

El ataque contra la PC con Windows XP-sp3 no es efectivo pues la misma no cuenta con la vulnerabilidad explotada en la PC con Windows XP-sp2, de manera que se reportan los mismos eventos de seguridad para esta PC sin tener lugar el lanzamiento de ninguna alarma de seguridad por parte de Alien Vault OSSIM.
La herramienta no lanza una alarma de seguridad para la máquina con Windows XP-sp3

Conclusiones

El presente artículo abordó la detección efectiva de ataques informáticos mediante la integración de un sistema de detección de intrusos y un escáner de vulnerabilidades. A partir de un estudio de las principales herramientas de seguridad existentes y teniendo como premisa la selección de herramientas basadas en software libre. En correspondencia con la política del país y de la UCI; se plantea la selección de los siguientes sistemas para la detección efectiva de ataques informáticos: snort como sistema de detección de intrusos, OpenVas como escáner de vulnerabilidades, alien Vault OSSIM como sistema que permite correlación de información y la integración de las dos herramientas anteriores.

Se estudió en detalles el diseño topológico de la red del nodo central de comunicaciones de la UCI, haciendo énfasis en los servidores que se encuentran en la zona desmilitarizada - DMZ - que son los que están expuestos directamente a una gran cantidad de amenazas, y se definió la ubicación del servidor OSSIM para la detección efectiva de ataques informáticos externos a la red de la UCI.

Finalmente se procedió a la validación de la herramienta propuesta mediante su instalación en un entorno de pruebas, en el que se realizaron experimentos con ataques reales para verificar la función de correlación cruzada de OSSIM. La realización de las pruebas permitió detectar que la versión libre de este sistema no tiene implementada la correlación cruzada, lo cual no se especifica en la documentación oficial de OSSIM, por lo que fue necesario realizar una pequeña modificación al código fuente de la misma para habilitar esta funcionalidad. Después de realizada esta modificación se pudo comprobar que, mediante las reglas de correlación cruzada, el sistema es capaz de integrar el IDS Snort con el escáner de vulnerabilidades OpenVas, generando alarmas de mayor impacto ante la ocurrencia de ataques que explotan vulnerabilidades existentes, por lo que se produce una detección más efectiva de los ataques informáticos.

Referencias

ALBARRAN BRAVO GLADIS and GARDUÑO GÓMEZ NOA. Arquitectura de monitoreo en tiempo real de una red, INSTITUTO POLITÉCNICO NACIONAL. ESCUELA SUPERIOR DE INGENIERÍA MECÁNICA Y ELÉCTRICA UNIDAD CULHUACAN, 2010. p.

CORPORATION, M. Boletín de seguridad de Microsoft MS08-067 – Crítico, 2008. [2012]. Disponible en: http://www.microsoft.com/latam/technet/seguridad/boletines/2008/ms08-067.mspx

DEBASIS, M. MS Windows Server Service Code Execution Exploit (MS08-067) (2k/2k3), 2008. [2012]. Disponible en: http://www.exploit-db.com/exploits/7132/

ESPINOZA P MARIA; PINEDA A.JULIA, et al. Implementación de una Herramienta SIM (Security Information Management) en la Red de la Universidad Técnica Particular de Loja, 2007.

GARTNER S.A. Gartner Inc. and/or its Affiliates., 2012. [2012]. Disponible en: http://www.gartner.com/technology/home.jsp

LORENZO MANUEL JUAN. Manual de instalación de AlienVault Open Source SIEM (OSSIM). 2009. [2011]. Disponible en: http://ossim.net/dokuwiki/doku.php?id=installationES

OSVDB, O. S. V. D. Microsoft Windows Server Service Crafted RPC Request Handling Unspecified Remote Code Execution, 2012. [2012]. Disponible en: http://osvdb.org/show/osvdb/49243

RICHARDSON ROBERT. CSI Computer Crime and Security Survey., 2009.

SEGURIDAD INFORMATICA. RED SOCIAL SOBRE SEGURIDAD INFORMÁTICA. Herramientas SIM / SIEM, 2008. [2011]. Disponible en: http://www.seguridadinformatica.es/profiles/blogs/herramientas-sim-siem

SOFTWARELIBRE NET. SegInf Firma Con AlienVault, Creadores De OSSIM. El Acuerdo ABP Como Distribuidor Oficial., 2011.

TORNILV PERRAMÓN XAVIER, A. G. J., JOANCOMARTÍ HERRERA JORDI Aspectos avanzados de seguridad en redes., 2004.

VIZCAÍNO DÍAZ MIGUEL LUIS. Sistemas de Detección de Intrusos.: Departamento de Ingeniería Telemática., Universidad Carlos III de Madrid., 2003. p.