ESPE

UNIVERSIDAD DE LAS FUERZAS ARMADAS

INNOVACIÓN PARA LA EXCELENCIA

DEPARTAMENTO DE ELÉCTRICA Y ELECTRÓNICA

CARRERA DE INGENIERÍA EN ELECTRÓNICA, REDES DE LA INFORMACIÓN Y COMUNICACIÓN DE DATOS

TRABAJO DE TITULACIÓN PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN ELECTRÓNICA REDES DE LA INFORMACIÓN Y COMUNICACIÓN DE DATOS

TEMA: ANÁLISIS Y DISEÑO DE UN PROTOTIPO PARA UN SISTEMA DE GESTIÓN DE EVENTOS DE SEGURIDAD INFORMÁTICA UTILIZANDO OSSIM.

AUTORA: LUZÓN GUZMÁN GINA IVANOVA

DIRECTOR: DR. ESPINOSA ORTIZ NIKOLAI DANIEL, PhD

SANGOLQUÍ

2017

UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

DEPARTAMENTO DE ELÉCTRICA Y ELECTRÓNICA

CARRERA DE INGENIERÍA EN ELECTRÓNICA, REDES DE LA INFORMACIÓN Y COMUNICACIÓN DE DATOS

CERTIFICACIÓN

Certifico que el trabajo de titulación, "ANÁLISIS Y DISEÑO DE UN PROTOTIPO PARA UN SISTEMA DE GESTIÓN DE EVENTOS DE SEGURIDAD INFORMÁTICA UTILIZANDO OSSIM." realizado por la señorita LUZÓN GUZMÁN GINA IVANOVA, ha sido revisado en su totalidad y analizado por el software anti-plagio, el mismo cumple con los requisitos teóricos, científicos, técnicos, metodológicos y legales establecidos por la Universidad de Fuerzas Armadas ESPE, por lo tanto me permito acreditarlo y autorizar LA señorita LUZÓN GUZMÁN GINA IVANOVA para que lo sustente públicamente.

Sangolquí, 16 de enero del 2017.

Dr. Nikolai Daniel Espinosa Ortiz

TUTOR ACADÉMICO

UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

DEPARTAMENTO DE ELÉCTRICA Y ELECTRÓNICA

CARRERA DE INGENIERÍA EN ELECTRÓNICA, REDES DE LA INFORMACIÓN Y COMUNICACIÓN DE DATOS

AUTORÍA DE RESPONSABILIDAD

Yo, GINA IVANOVA LUZÓN GUZMÁN, con cédula de identidad N° 110502751-8, declaro que este trabajo de titulación "ANÁLISIS Y DISEÑO DE UN PROTOTIPO PARA UN SISTEMA DE GESTIÓN DE EVENTOS DE SEGURIDAD INFORMÁTICA UTILIZANDO OSSIM" ha sido desarrollado considerando los métodos de investigación existentes, así como también se ha respetado los derechos intelectuales de terceros considerándose en las citas bibliográficas.

Consecuentemente declaro que este trabajo es de mi autoría, en virtud de ello me declaro responsable del contenido, veracidad y alcance de la investigación mencionada.

Sangolquí, 16 de enero del 2017.

Gina Ivanova Luzón Guzmán

C.C. 110502751-8

ESPE
UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

DEPARTAMENTO DE ELÉCTRICA Y ELECTRÓNICA

CARRERA DE INGENIERÍA EN ELECTRÓNICA, REDES DE LA INFORMACIÓN Y COMUNICACIÓN DE DATOS

AUTORIZACIÓN

Yo, GINA IVANOVA LUZÓN GUZMÁN, autorizo a la Universidad de las Fuerzas Armadas ESPE publicar en la biblioteca Virtual de la institución el presente trabajo de titulación "ANÁLISIS Y DISEÑO DE UN PROTOTIPO PARA UN SISTEMA DE GESTIÓN DE EVENTOS DE SEGURIDAD INFORMÁTICA UTILIZANDO OSSIM" cuyo contenido, ideas y criterios son de mi autoría y responsabilidad.

Sangolquí, 16 de enero del 2017.

Gina Ivanova Luzón Guzmán

C.C. 110502751-8

DEDICATORIA

“Hay una fuerza motriz más poderosa que el vapor, la electricidad y la energía atómica: la voluntad.”

Albert Einstein

Al Divino Niño Jesús, a la Virgencita del Cisne,

A mi familia,

Son mi alma y corazón,

La razón que me levanta todos los días.

AGRADECIMIENTOS

Agradezco a la Virgen del Cisne y al Divino Niño, por todas las experiencias vividas, por sus bendiciones y por su guía para concluir este sueño anhelado, la culminación de mi carrera.

A mis padres, Irma y Eduardo, por su amor, sacrificio, enseñanzas, apoyo y por brindarme las herramientas necesarias para luchar cada día, son excelentes padres mi gratitud hacia ustedes es infinita y espero poder día a día retribuir a su esfuerzo.

A mi abuelita Fidelina, por sus bendiciones, enseñanzas, y sobre todo la dedicación y amor con que cuidó de mí durante toda su vida, y aún lo continúa haciendo desde el cielo.

A mis abuelitos Vicente y Delia, por el cariño, esfuerzo y dedicación con el que siempre han cuidado de nosotros.

A mis hermanos Tania y Lalo, por brindarme su amor y apoyo incondicional, su compañía y paciencia me han ayudado siempre a seguir mis metas.

A mi amor por estar a mi lado siempre a pesar de lo bueno, lo malo; por aceptarme como soy, por su inteligencia y apoyo para lograr culminar esta etapa de la vida.

A mis amigos, profesores y jefes que, con sus consejos, paciencia, críticas y apoyo me han permitido crecer como persona y a nivel profesional.

Gracias a totales.

ÍNDICE DE CONTENIDO

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

RESUMEN

En este proyecto de titulación se busca analizar una herramienta para realizar la gestión, monitoreo y registro de eventos de seguridad de informática, desarrollando un prototipo de gestor basado en herramientas de software libre, que se ajuste a cualquier modelo de red a través de un fácil despliegue y bajo costo. Dentro de la gestión se busca mejorar la disponibilidad y el marco entorno a la seguridad de la red, la monitorización se la realiza mediante mecanismos que permiten verificar el estado de los equipos que conforman la red, además de generar un registro ordenado de eventos que en su medida pueden dañar o no la disponibilidad y autenticidad de la información. El propósito de este trabajo es diseñar un prototipo portable (máquina virtual) basado en la plataforma de código abierto OSSIM, misma que permite una gestión centralizada e intuitiva, que facilita la detección de eventos y vulnerabilidades en la red. Se detalla la arquitectura, configuración y análisis de los resultados obtenidos con la herramienta, tomado en cuenta la aplicación de directrices de seguridad establecidos por entidades de normalización internacionales ISO/INEN.

PALABRAS CLAVES

- **GESTIÓN DE RED**
- **SEGURIDAD DE LA INFORMACIÓN**
- **DETECCIÓN DE EVENTOS**
- **DETECCIÓN DE VULNERABILIDADES**
- **POLÍTÍCAS DE SEGURIDAD**

ABSTRACT

This project aims to analyze a tool to perform the management, monitoring and registration of computer security events, developing a prototype manager based on free software tools, which will fit any network model through an easy Deployment and low cost. Within the management it is sought to improve the availability and the framework around the network security, the monitoring is done through mechanisms that allow to verify the state of the equipment that make up the network, in addition to generating an ordered register of events that in Their measurement may or may not damage the availability and authenticity of the information. The purpose of this paper is to design a portable prototype (virtual machine) based on the open source OSSIM platform, which allows a centralized and intuitive management that facilitates the detection of events and vulnerabilities in the network. It details the architecture, configuration and analysis of the results obtained with the tool, taking into account the application of safety guidelines established by ISO / INEN international standardization entities.

KEYWORDS

- **NETWORK MANAGEMENT**
- **INFORMATION SECURITY**
- **EVENT DETECTION**
- **VULNERABILITY DETECTION**
- **SECURITY POLICIES**

CAPÍTULO 1: MARCO TEÓRICO

1.1. Introducción

En los últimos años el crecimiento de las redes de información y el surgimiento de nuevas tecnologías han provocado que paralelamente se haya incrementado el número de incidentes, amenazas y vulnerabilidades de la red, poniendo en riesgo la disponibilidad, confidencialidad e integridad de la información.

El impacto generado a nivel económico, político y social, por incidentes de seguridad, se ha convertido en un punto clave de análisis, por lo que muchas organizaciones invierten gran cantidad de dinero adquiriendo dispositivos de seguridad que permitan proteger su infraestructura tecnológica, sin que esto sea suficiente.

Existen algunas herramientas de seguridad informática y normas internacionales establecidas, que ayudan a los administradores de red a mejorar su desempeño en la labor de control y gestión de la seguridad, las cuales permiten conocer comportamientos intrusivos y anormales en los sistemas administrados, además de establecer pautas, reglas y políticas que ayudan a mejorar la protección de la información. Por ello que la implementación de normativas acompañadas de herramientas especializadas de seguridad, son indispensables para toda organización, ya que permiten una administración centralizada y monitoreo activo de posibles incidentes de seguridad para salvaguardar la información.

1.2. Seguridad de la Información y Seguridad Informática

Para lograr desarrollar estrategias de seguridad de la información efectivas dentro de una organización, es necesario comprender que esto no sólo es cuestión de colocar e instalar equipos tecnológicos especializados, sino que requiere de un estrecho relacionamiento con los objetivos propios de negocio, además de una participación activa de altos ejecutivos que permita

enfocar a la seguridad informática y de la información como un aliado estratégico, para lograr los objetivos y metas de la organización.

Bajo este esquema es importante conocer dos definiciones esenciales. La primera es *seguridad* definida como una “característica que indica que un sistema está libre de todo peligro, daño o riesgo" (Villalón Huerta, 2000), y la segunda hace referencia al principal activo de toda organización al cual se busca proteger la *información* definida como "conjunto de datos con un significado, que reduce la incertidumbre o que aumenta el conocimiento de algo" (Chiavenato, 2006).

Continuamente se confunde seguridad informática y seguridad de la información, estos conceptos importantes y diferenciables. La *seguridad informática* “consiste en la implantación de un conjunto de medidas técnicas destinadas a preservar la confidencialidad, la integridad y la disponibilidad de la información pudiendo, además, abarcar otras propiedades, como la autenticidad, la responsabilidad, la fiabilidad y el no repudio.” (ISO/IEC, 27001:2005), mientras que la *seguridad de la información* “es la disciplina que nos habla de los riesgos, de las amenazas, de las buenas prácticas y esquemas normativos, que nos exigen niveles de aseguramiento de procesos y tecnologías para elevar el nivel de confianza…y disposición final de la información” (Cano, 2007), abarcando la protección de toda la información que puede encontrarse en diferentes medios o formas, a diferencia de la primera que se enfoca sólo en medios informáticos.

Estos conceptos deben estar siempre interconectados para lograr que la organización se desarrolle bajo un entorno de seguridad efectivo acorde a sus necesidades de negocio.

1.2.1. Seguridad de la Información

La información el activo más valioso de toda organización es imprescindible que la seguridad de la información forme parte de los objetivos que rigen el negocio. Los costos derivados de la falta de seguridad no solo se

limitan a costes económicos, sino que también afectan la imagen y desarrollo de la misma.

La *seguridad de la información* no solo establece la necesidad de implementar mecanismos de seguridad física y de red como video vigilancia, control de accesos, detección de incendios, firewalls, etc., sino también se encarga de definir objetivos claros a partir de los cuales se desarrollará las políticas, procedimientos y esquemas normativos que serán aplicados en las diversas áreas de la organización para lograr procesos confiables.

Para lograr un aseguramiento de la información las políticas de seguridad y normativas definidas deben regirse en los tres principios fundamentales de la información: confidencialidad, integridad y disponibilidad:

1) Confidencialidad: asegurar la privacidad de la información permitiendo el acceso sólo para aquellos usuarios autorizados.

2) Integridad: preservar la exactitud y veracidad de la información, así como los métodos de su procesamiento.

3) Disponibilidad: garantizar que los usuarios autorizados tienen acceso a la información y sus activos asociados cuando estos lo requieran.

1.2.2. Seguridad Informática

Las organizaciones consientes de la importancia de su información tienen como objetivo disminuir los riesgos y mejorar la protección de sus datos, tratando de implementar soluciones que no requieran fuertes inversiones en hardware y software, y sin la necesidad de una gran estructura de personal. Para ello es necesario conocer los riesgos a los que se somete la información, definir procedimientos adecuados y planificar e implementar controles de seguridad.

En la actualidad, la mayor parte de la información reside en equipos informáticos, soportes de almacenamiento y redes de datos, para ello la

seguridad informática describe el conjunto de implementaciones técnicas para la protección de la información y disminución de riesgos, abarca el despliegue de diferentes tecnologías de hardware y software como: antivirus, firewalls, sistemas detección de intrusos, análisis de tráfico, correlación de eventos, etc., que basados en controles y normativas de seguridad establecidas, permiten que los recursos de la organización se utilicen de la manera adecuada, asegurando la disponibilidad y confiabilidad de la información.

1.2.2.1. Conceptos básicos en seguridad informática

- Información: Es un conjunto organizado de datos procesados y seleccionados que proporcionan valor a una organización, mejorando su competitividad y capacidad de desarrollo.
- Vulnerabilidad: Es una debilidad del sistema informático que puede ser utilizada para causar daños en el sistema y violar la disponibilidad, confiabilidad e integridad de la información. Se generan debido a fallos tanto a nivel de hardware, software como también humano, es por ello que no existen sistemas cien por ciento seguros.
- Amenaza: Es la probabilidad de ocurrencia de un suceso o evento que potencialmente pueden causar daños o pérdidas en el sistema.
- Ataque: Es la acción intencional e injustificada dirigida por una amenaza, que intenta violar la seguridad global o de uno de sus componentes, para tomar el control, desestabilizar o dañar al sistema informático.
- Riesgo: Es la probabilidad de que ocurra un ataque por parte de una amenaza. Se debe elaborar análisis de riesgos tomando la probabilidad de una amenaza y la magnitud del impacto sobre el sistema si ésta llega a materializarse, esto permite tomar decisiones para proteger mejor al sistema.
- Evento: Puede ser referido como un "incidente" o "accidente". Es una o más ocurrencias indeseadas e inesperadas, que tienen probabilidad de comprometer o impedir la operación normal del sistema.

- Política: Es un conjunto de normas y prácticas que regulan el manejo, protección y distribución de recursos de una organización, expresada formalmente por la persona o grupo de personas que dirige y controla una organización al más alto nivel.
- Control: Es una medida que modifica un riesgo. Los controles incluyen cualquier proceso, política, dispositivo, práctica u otras acciones que modifiquen el riesgo.

1.2.2.2. Elementos de la Seguridad Informática

La seguridad informática tiene como finalidad proteger los elementos activos relacionados con el entorno de la organización, entre los que se encuentran:

- Información: Es considerada el activo más importante dentro de la organización, la componen un conjunto de datos estructurados y seleccionados que brindan poder y valía. Todo sistema de seguridad debe tener como eje la preservación de la confidencialidad, integridad, y disponibilidad de la información.

- Usuarios: Son las personas o individuos autorizados para el uso de recursos de la organización para realizar múltiples operaciones con distintos propósitos. Las amenazas y ataques generados por usuarios son constantemente la principal razón de los problemas de seguridad que puede tener la organización, es imprescindible elaborar controles y políticas que minimicen los riegos de una pérdida de información.

- Tecnologías de la Información y Comunicación (TIC): Son una parte fundamental para el desarrollo y competitividad de una organización, son un conjunto de herramientas computacionales (hardware y software), que se encargan del procesamiento, implementación, almacenamiento, distribución y respaldo de la información. Estas herramientas permiten brindar al usuario facilidades y servicios para realizar sus distintas actividades laborales. La seguridad informática

hace uso de las TIC para desarrollar e implementar soluciones paralelas a las tecnologías emergentes y que permitan atenuar los riegos a los que está expuesta la información.

1.2.2.3. Principios de la Seguridad Informática

Los sistemas de seguridad informática son mecanismos físicos necesarios para implementar y mantener estrategias de seguridad de la información, sus funcionalidades se sustentan en los tres principios de la información como se muestra en la Tabla 1:

Tabla 1
Principios de la Seguridad Informática

Principios	Descripción
Confidencialidad	Propiedad de que la información no sea puesta a disposición de, o se divulgue a, individuos, entidades o procesos no autorizados (ISO/IEC, 27001:2005). Por ello los sistemas de seguridad informática deben proteger a la organización de intrusiones y accesos no autorizados. Previniendo la divulgación y obtención indebida de información prioritaria o sensible, a través de asignación de roles para cada usuario del sistema.
Integridad	Propiedad de mantener la exactitud y completitud de los activos (ISO/IEC, 27001:2005). En base a esto los sistemas de seguridad informática deben asegurar la veracidad y precisión de los datos a través de métodos de acceso controlado, de duplicación, sincronización, entre otros, que permitan verificar la autenticidad de la fuente y contenido de los datos.
Disponibilidad	Propiedad de ser accesibles y utilizables ante la demanda de una entidad autorizada (ISO/IEC, 27001:2005). Es decir, los sistemas de seguridad informática deben mantenerse en funcionamiento permanente, brindando acceso únicamente a usuarios autorizados cuando estos lo requieran y denegándolo a los no autorizados, además de ser capaz de recuperarse rápidamente en caso de fallo.

1.3. Amenazas Informáticas

Una amenaza es un evento o suceso capaz de atentar contra la seguridad de la información, causando pérdida de información, interrupción de sistemas y daños materiales. Las amenazas surgen a partir de vulnerabilidades del sistema, por lo que una amenaza sólo puede existir si existe una vulnerabilidad que pueda ser aprovechada. Las vulnerabilidades son el resultado de fallos en el sistema y de las limitaciones propias de la organización. Cada amenaza materializada exitosamente se convierte en un ataque directo contra el sistema, y a su vez provocan riegos para los elementos activos de la organización que son afectados en mayor o menor grado. Las amenazas informáticas pueden ser causadas por:

- Usuarios: Que de forma intencionada o no, aprovechan las vulnerabilidades del sistema para acceder a los datos o programas. Estos usuarios a pesar de tener acceso autorizado a los recursos del sistema pueden ocasionar pérdidas en el mismo; representan el mayor problema ligado a la seguridad de un sistema informático.
- Intrusos: Son personas no autorizadas que acceden de forma ilícita al sistema, para sustraer información o hacer uso indebido de los programas (servicios) de la organización.
- Programas Maliciosos: Creados y desarrollados en base a las vulnerabilidades comunes de los sistemas, con el fin de dañar o hacer un uso ilícito de los recursos del sistema.
- Siniestros: Pueden ocurrir debido a una mala manipulación del sistema o por catástrofes naturales (terremoto, inundación, etc.) que generan la pérdida de equipos e información.

Existen muchos tipos de amenazas a las que la organización está expuesta, independientemente de su probabilidad de ocurrencia es recomendable realizar continuamente un análisis interno que permita determinar las vulnerabilidades del sistema informático y generar controles de seguridad que disminuyan los riesgos.

1.4. Ataques Informáticos

Un ataque informático es un conjunto de acciones generadas por un elemento (atacante) o amenazas que, mediante un sistema informático, busca desestabilizar o dañar otro sistema ajeno. El atacante aprovecha las vulnerabilidades o debilidades del sistema para comprometer al menos uno de los principios de la información confidencialidad, integridad y disponibilidad, estas vulnerabilidades se dan en cualquiera de los activos de la organización ya sea a nivel de software, hardware, e incluso, de usuario. Para disminuir los daños provocados de un ataque informático se debe conocer las vulnerabilidades más comunes que pueden ser aprovechadas y sus riesgos, esto permitirá comprender las metodologías de ataque, para implementar estrategias de seguridad efectivas.

Analizar y comprender las diferentes etapas que conforman un ataque genera varias ventajas y herramientas que pueden ser utilizadas de forma táctica para contrarrestar las habilidades del atacante y mitigar las vulnerabilidades potenciales. La Figura 1 muestra las cinco etapas comunes de ataque informático al momento de ser ejecutado:

Figura 1 Etapas de Ataque Informático

i. Reconocimiento

La fase de reconocimiento es una etapa inicial y preparatoria en la que el atacante obtiene toda la información necesaria sobre su víctima que puede ser una persona u organización antes de iniciar el ataque. Para la búsqueda de información se pueden utilizar varios mecanismos como motores de búsqueda (Google, Yahoo, Bing, Ask, etc.), ingeniería social (manipulación de usuarios para captar información confidencial), recolección de datos útiles en contenedores de basura, publicaciones impresas, localización de enrutadores, firewalls, servidores de correo, servidores web, sistema de nombres de dominio (DNS).

ii. Escaneo

Esta segunda etapa el atacante utiliza la información recolectada previamente en el reconocimiento y realiza un escaneo y análisis para detectar vulnerabilidades específicas que permitan acceder al sistema. En esta fase se realiza un estudio de la red utilizando programas de análisis de paquetes, mapeo de puertos, descubrimiento de redes, escáner de vulnerabilidad, desincriptación de datos.

iii. Ganar Acceso

Esta es una de las etapas más importantes en la que empieza a materializarse el ataque, utilizando los defectos y vulnerabilidades descubiertos durante el reconocimiento y escaneo, el atacante accede al sistema y lo invade con técnicas de desbordamiento de buffer, denegación de servicios, filtrado de contraseñas, secuestro de sesiones.

iv. Mantener el Acceso

Una vez que el atacante ha conseguido ingresar el sistema y puede manipular toda la información interna, su prioridad es implementar herramientas que le permitan tener un acceso permanente desde cualquier lugar. Durante esta fase el atacante hace uso de los recursos propios del sistema para escanear, analizar y materializar ataques a otros sistemas, por

ello trata de permanecer indetectable removiendo la evidencia de su penetración al sistema a través de puertas traseras, encubridores.

v. Borrar Huellas

En la quinta etapa el atacante intentará borrar todas las huellas o evidencias de sus actividades ilícitas durante la intrusión, para evitar ser detectado por administradores de red o policías, por ello buscará eliminar los archivos de registro, alarmas del Sistema de Detección de Intrusos (IDS), crear túneles, además ocultar y encriptar archivos dentro de una imagen o audio.

1.4.1. Ataques Internos

Los ataques internos son generados por usuarios desde el interior de la organización, son lo más comunes, pues de forma intencionada o no, dichos usuarios con acceso autorizado provocan incidentes de seguridad y atentan contra la confiabilidad, disponibilidad e integridad de la información, a través del sabotaje corporativo, robo de información, destrucción del sistema informático, etc.

Los ataques que surgen del interior de la organización pueden ser más serios que los externos, debido a que el atacante conoce la infraestructura de red y su funcionamiento, inhabilitando a mecanismos de protección como firewalls y sistemas de prevención de intrusos (IPS).

1.4.2. Ataques Externos

Los ataques externos son iniciados por individuos (intrusos) desde afuera de la organización, a pesar de no tener un acceso autorizado a los recursos realizan un análisis de vulnerabilidades que les permita acceder y provocar daños en los sistemas informáticos, principalmente lo hacen a través de la Internet o servidores de acceso que les permita evadir cualquier dispositivo de seguridad perimetral como firewalls.

1.4.3. Otros tipos de Ataques Informáticos

Un ataque es la materialización de una amenaza también puede clasificarse en cuatro categorías generales de acuerdo al método que utilice la amenaza para invadir al sistema informático, en la Figura 2 se puede observar los cuatro tipos:

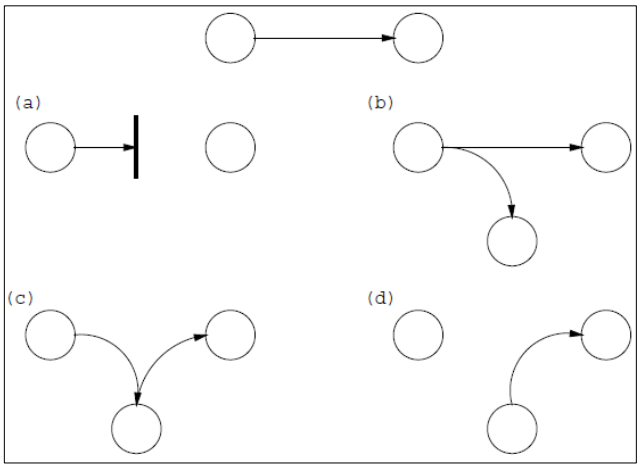


Figura 2 Flujo Normal de información entre emisor y receptor y posibles amenazas; (a) Interrupción, (b) Interceptación, (c) Modificación y (d) Fabricación.

Fuente: (Villalón Huerta, 2000)

- Interrupción: Cuando un usuario o intruso provoca que uno de los recursos del sistema se destruya o quede inutilizable. Este es un ataque contra la disponibilidad. Por ejemplo, Flooding, Net Flood y SYN Flood son ataques de Denegación de Servicio (DoS) que saturan y desactivan el sistema informático.

- Interceptación: Cuando un intruso consigue acceso a un recurso del sistema atentando contra la confidencialidad de la información. Por ejemplo, ataques de autenticación a través de Spoofing-Looping, Exploits, BackDoors y uso de Diccionarios que tienen como finalidad interceptar el nombre y clave de un usuario legítimo para, una vez ingresado al sistema, realizar acciones en su nombre.

- Modificación: Cuando un intruso luego de penetrar el sistema consigue alterar o cambiar un recurso, eliminándolo o convirtiéndolo en inutilizable, atentando contra la integridad de la información. Por ejemplo, ataques a través de borrado de huellas, Tampering, por JavaScript, Java Applets, Visual Script que permiten la modificación de datos o ficheros sin autorización.
- Fabricación: Abarca la interrupción y modificación, el intruso accede al sistema y modifica su contenido creando un recurso similar al atacado de forma que sea difícil distinguir entre el original y el falsificado, atentado contra la autenticidad de la información. Por ejemplo, ataques a través de ActiveX, que falsifican certificados de autorización para ejecutar programas o códigos maliciosos.

Bajo este esquema existen diversos tipos de ataques que pueden ser realizados sobre cualquier tipo de red, sistema operativo, protocolos, etc., basados en vulnerabilidades comunes que al no ser controladas a través estrategias de seguridad son fácilmente explotados y provocan daños en los recursos activos de la organización. A continuación, se describen algunos tipos de ataques comunes.

1.4.3.1. Ataques por Denegación de Servicio (DoS)

Tienen como objetivo impedir el acceso a los servicios y recursos de la organización durante un período indefinido de tiempo. Por lo general, está dirigido hacia los servidores, saturando su capacidad de procesamiento a través de cientos de miles de peticiones que colapsan el sistema, dejándolo inaccesible al resto de usuarios.

Son ataques eficaces que aprovechan las vulnerabilidades relacionadas con la implementación del protocolo TCP/IP, y que pueden actuar contra cualquier equipo con sistema Windows (2003, 2008, 2012, 2012 R2, etc.), Linux (Debian, Mandrake, RedHat, Suse, etc.), Unix (HP-UX, AIX, IRIX, Solaris, etc.) o cualquier otro sistema operativo. El objetivo de un ataque por

denegación de servicio no reside en recuperar o alterar datos, sino en dañar la credibilidad de las organizaciones y potencialmente imposibilitar el desarrollo normal de sus actividades disminuyendo su competitividad durante largos o cortos periodos de tiempo.

Existen muchas herramientas que se controlan de forma remota, y permiten realizar ataques DoS entre los más conocidos se tienen los siguientes:

- *Inundación (Flooding)*

Este tipo de ataques tienen como objetivo inundar o saturar los recursos del sistema, de tal forma que consume sus capacidades de memoria, almacenamiento y ancho de banda. El atacante satura el sistema con mensajes que requieren establecer conexión, enviando paquetes con IP origen falsas, correspondientes a la víctima. Los receptores responden al mensaje, pero al no recibir respuesta se acumula buffers con información de las conexiones abiertas, sin dejar lugar a conexiones legítimas.

Cuando varios equipos activan una denegación de servicio, el proceso se conoce como sistema distribuido de denegación de servicio (DDOS, Distributed Denial of Service). Los ataques DDoS son considerablemente difíciles de rastrear debido a las capacidades de ocultación incorporadas en las herramientas.

Existen varias formas de realizan ataques Flooding utilizando diversos protocolos como ICMP, UDP, IGMP, TCP y HTTP, todos ellos con el fin de saturar los recursos del sistema y generar denegación de los servicios. En la Tabla 2 se muestra algunos de los ataques Flooding que se pueden realizar y la capa OSI a la que afectan.

Tabla 2
Descripción de Ataques Flooding

Nombre	Capa OSI	Descripción
Ping de la Muerte	L3: Red	Envío de paquetes ICMP que explotan fallos del sistema operativo →

ICMP echo request flood o Ping Flood	L3: Red	Envío masivo de paquetes ping, que implican una respuesta por parte de la víctima con el mismo contenido que el paquete de origen.
SMURF	L3: Red	Ataque por saturación ICMP que usurpa la dirección de origen para redirigir las múltiples respuestas hacia la víctima.
IGMP Flood	L3: Red	Envío masivo de paquetes IGMP (protocolo de gestión de grupos de internet)
UDP Flood	L4: Transporte	Envío masivo de paquetes UDP
TCP SYN Flood	L4: Transporte	Envío masivo de solicitudes de conexión TCP
TCP ACK Flood	L4: Transporte	Envío masivo de acuses de recibo de segmentos TCP
HTTP / HTTPS Flood	L7: Aplicación	Ataque de un servidor web mediante el envío masivo de peticiones
DNS Flood	L7: Aplicación	Ataque de un servidor DNS mediante el envío masivo de peticiones

- Syn Flood

El SYN Flood es de los más famosos ataques del tipo DoS, y trata de saturar el sistema a través de establecer conexiones incompletas entre dos hosts. Se basa en la vulnerabilidad del protocolo TCP/IP para establecer una conexión. Dicha conexión se establece en el esquema que muestra la Figura 3: el cliente envía un paquete SYN; si el servidor acepta la conexión, éste debería responderle con un SYN/ACK; para que el cliente responda con un ACK y así se complete y finalice la conexión.

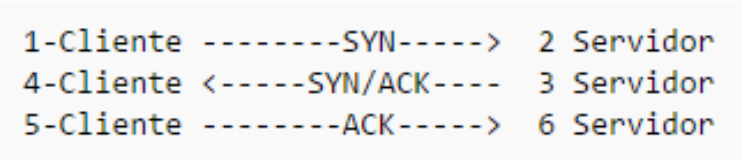


Figura 3 Esquema de Conexión TCP/IP

En la Figura 4 se observa como el ataque SYN Flood aprovecha esta vulnerabilidad de TCP/IP de tal forma que el ataque desde una dirección IP inexistente, envía una petición de conexión a través de un paquete SYN hacia la víctima (servidor), el servidor responde un SYN/ACK, pues a pesar de que el protocolo ICMP reporta que el origen es inexistente, TCP ignora el mensaje y sigue intentando terminar la conexión con el atacante de forma continua, provocando que la víctima espere cierta cantidad de tiempo a que el atacante responda.

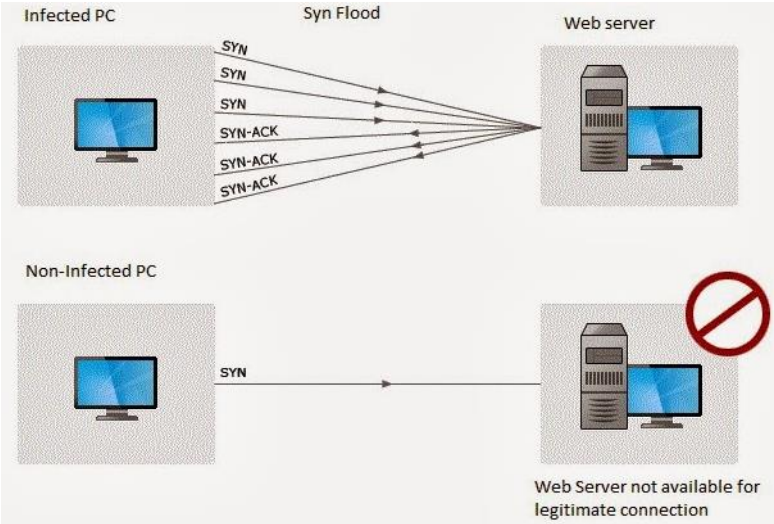


Figura 4 Ataque DoS - Syn Flood

A pesar de ser un proceso sencillo, el establecimiento de una conexión siempre consume recursos, y al crearse muchas peticiones incompletas provoca inactividad de la víctima, esperando mucho tiempo respuestas a las peticiones. Esto ocasiona lentitud en los servicios y al superar el límite de conexiones semi abiertas posibles la víctima deja de responder las peticiones verdaderas y deniega el servicio.

- *Tormenta Broadcast (Broadcast Storm)*

Su funcionalidad es sencilla y a su vez devastadora. El atacante falsifica la dirección IP de la víctima para enviar una serie de peticiones repetitivas ICMP con esa IP origen, hacia un grupo de direcciones IP tipo broadcast,

provocando que cientos o miles de hosts envíen una respuesta a la víctima cuya dirección IP figura en el paquete ICMP. Los hosts seguirán propagando tráfico de broadcast y multicast una y otra vez, saturando la red y consumiendo recursos de procesamiento por lo que la víctima parecerá estar inactiva o extremadamente lenta.

1.4.3.2. Ataques por Códigos Malignos (Malware)

Los códigos malignos o malware son un tipo de software que tiene como objetivo infiltrarse o dañar un sistema de información o recurso específico sin el consentimiento de su propietario, para obtener algún beneficio para su creador o distribuidor.

Los ataques por códigos maliciosos son cada vez más especializados y sofisticados, su detección en algunos casos es compleja y requiere muchos recursos. Y sus desarrolladores hacen un gran esfuerzo para evadir su eliminación y para causar un daño permanente en los equipos infectados. Actualmente hay organizaciones dedicadas a desarrollar y distribuir malware que buscan el reconocimiento de la comunidad acompañado de beneficios financieros. Esto ha traído consigo una gran variedad de códigos maliciosos de los cuales se puede nombrar algunos.

- *Caballo de Toya (Troyanos)*

Los troyanos son programas que están disfrazados, que aparentan tener una función útil y que invitan al usuario a ejecutarlo ocultando un software malicioso. Su función es permitir la administración remota del equipo donde se hallan alojados, de forma oculta y sin el consentimiento de su propietario.

Este malware puede causar grandes daños al sistema y atenta directamente contra la integridad y confiabilidad de la información, eliminando archivos o instalando más programas indeseables o maliciosos que permiten el acceso remoto de intrusos. Afortunadamente a diferencia de los virus y

gusanos, no puede reproducirse por sí mismo e infectar más equipos, y usualmente se encuentra en forma de archivo ejecutable (.exe, .com).

- *Virus*

Un virus es un programa informático creado para producir daños en el equipo deteriorando su rendimiento, y que al ejecutarse actúa de forma transparente al usuario y se propaga infectando otros softwares ejecutables dentro del mismo equipo. Además, tienen la capacidad de reproducirse a sí mismo y distribuirse con ayuda de usuario, a la mayor cantidad de equipos posible a través de medios extraíbles (CD, DVD, memory flash, etc.) o por medio de la red (local o internet).

- *Gusanos*

Los gusanos son un tipo de malware que tienen la propiedad de duplicarse a sí mismo. Aprovechan las vulnerabilidades propias del equipo infectado para provocar daños utilizando las partes automáticas de un sistema operativo. A diferencia de los virus, el gusano se propaga activamente enviando copias de sí mismo a través de la red local o Internet, infectando el entorno en minutos generando un colapso de la red. Con frecuencia, están ocultos en mensajes de correo electrónico y mensajes instantáneos como archivos adjuntos que, buscan persuadir al usuario para ser ejecutados.

- *Rootkit*

Son un conjunto de herramientas usadas para modificar el sistema operativo de un equipo, escondiendo los procesos realizados por un intruso remoto, permitiendo así que el malware permanezca oculto al usuario. Su función es esconder de sí mismo y de otros programas, los procesos, archivos, directorios, claves de registro, y puertos que permiten al intruso mantener el acceso al equipo infectado para dirigir acciones o extraer información sensible.

- *Spyware*

Es un programa malicioso que busca recopilar información sobre una persona u organización, a través del equipo infectado sin el conocimiento del propietario para transmitir a un atacante remoto. Una de las formas más comunes para distribuir spyware es mediante troyanos unidos a software deseable descargado de Internet. Cuando el usuario instala el software esperado, el spyware es puesto también.

Actúan como programas espía que capta la información del usuario como aplicaciones instaladas, historial de sitios web, contraseñas, actividad financiera o personal. Puede provocar daños en el rendimiento del equipo, problemas de estabilidad e inclusive robos de identidad.

1.4.3.3. Ataques por Autenticación de Usuarios (Fuerza Bruta)

Los ataques por autenticación tienen como objetivo engañar al sistema informático ingresando al mismo como un usuario legítimo. Generalmente el atacante utiliza las sesiones ya establecidas por la víctima o herramientas que le permitan le permitan obtener nombres de usuario y su respectiva contraseña.

La obtención de identificadores de usuarios y contraseñas es uno de los principales objetivos buscados por atacantes informáticos, pues a pesar de que en la actualidad existen sistemas de autenticación complejos, las contraseñas son el control de seguridad más utilizado y expandido en cualquier tipo de sistema informático. Para lograr captar está información se han desarrollado varias herramientas que facilitan el desarrollo del ataque.

- *Suplantación de Identidad (Spoofing)*

Los ataques por suplantación de identidad tienen como objetivo actuar en nombre de otros usuarios para realizar transacciones financieras o sustraer información sensible sin consentimiento de los propietarios. Para conseguir el identificador de usuario legítimo y la contraseña el atacante realiza una recolección de información, que muchas veces es fácilmente captada con

Ingeniería Social, ya que los usuarios, por desconocimiento facilitan a extraños sus identificaciones ya sea a través de llamadas telefónicas o correos electrónicos.

Entre los ataques tipo Spoofing se encuentran el IP Spoofing, DNS Spoofing y Web Spoofing. El más común es por IP, donde el atacante sustituye su dirección IP origen por la de un equipo de la red que ha establecido algún tipo de confianza, basada en el nombre o la dirección IP suplantada con un tercer equipo víctima del ataque. En este caso, las respuestas de la IP víctima que recibe los paquetes de datos irán destinados a la IP falsa del atacante.

- *Puertas Traseras (Backdoors)*

Las puertas traseras son una secuencia especial de código en un programa que permiten evitar los métodos usuales de seguridad como autentificación para acceder al sistema. Esta es una vulnerabilidad aprovechada por los atacantes pues habitualmente estos trozos de código son insertados por los programadores para agilizar la tarea de probar código fuente durante la fase de desarrollo, y al no ser eliminados se genera una falla de seguridad que permite al atacante ingresar fácilmente a los sistemas y controlarlos de forma remota para su beneficio personal.

- *Exploits*

Este tipo de ataques utilizan fragmentos de software o agujeros en los algoritmos de encriptación, administración de claves, o errores en los programas utilizados, estos agujeros generan vulnerabilidades de seguridad que pueden ser aprovechas y explotadas por los atacantes para conseguir un comportamiento no deseado del mismo acceso al sistema informático y a su información. Los exploits pueden tomar forma en distintos tipos de software, como por ejemplo scripts, virus informáticos o gusanos informáticos, para acceder al sistema y encontrar las vulnerabilidades del mismo.

- *Diccionarios*

Este tipo de ataques tiene como objetivo averiguar las contraseñas de usuarios válidos aprovechando la utilización de palabras comunes o predecibles, a los sistemas, aplicaciones, cuentas, etc. Los Diccionarios son archivos con millones de palabras, las cuales pueden ser posibles claves de los usuarios. Este método utiliza la obtención por Fuerza Bruta para descubrir las contraseñas de la víctima.

En muchos casos los ataques por fuerza bruta se simplifican e involucran algún tiempo de prueba y error, pues las contraseñas de acceso son obtenidas fácilmente porque involucran el nombre o dato familiar del usuario y, además muy pocas veces cambia lo que las hace bastante predecibles. Cuando las contraseñas no poseen datos fácilmente predecibles se hace uso de programas especiales y diccionarios. Dicho programa especial es el encargado de probar cada una de las palabras del diccionario, encriptándolas mediante el algoritmo utilizado por el sistema atacado, y compara la palabra encriptada con el archivo de claves real, hasta encontrar la contraseña de acceso al sistema.

1.4.3.4. Ataques por Inyección de Código

Este tipo de ataques intentan inyectar código que es interpretado/ejecutado por la aplicación, como resultado de fallas de seguridad habituales por la falta de validación apropiada de entradas y salidas de datos. Al introducir códigos malintencionados dentro de la aplicación se puede eliminar o modificar datos, instalación de malware, modificación de los privilegios de usuario, denegar de accesos e inclusive llegar a tomar el control del equipo.

Entre algunos de los métodos para este tipo de ataques son: Inyección SQL, secuencias de comandos en sitios cruzados (XSS) y falsificación de petición en sitios cruzados (CSRF). El método más utilizado es la inyección SQL, que consiste en la inserción de código en variables especificadas por el

usuario las cuales se concatenan con comandos SQL y se ejecutan el código dañino.

1.5. Sistema de Gestión de Seguridad de la Información (SGSI)

La información es el activo más valioso de muchas organizaciones por lo que es necesario protegerla adecuadamente frente a amenazas que puedan poner en peligro la seguridad del activo. La Organización Internacional para la Estandarización junto a la Comisión Electrotécnica Internacional (ISO/IEC) desarrolló el concepto del Sistema de Gestión de Seguridad de la Información (SGSI) sobre el que se construye la norma ISO/IEC 27001. Definiéndola como un proceso sistemático, documentado y conocido por toda la organización.

Dentro de la norma ISO/IEC se establece que los sistemas SGSI deben tener como objetivo principal el resguardo de la información manteniendo su disponibilidad, confidencialidad e integridad, para lograr la eficiencia del negocio, brindando información precisa y completa que esté disponible de manera oportuna a aquellos con una necesidad autorizada.

Conseguir la seguridad total en una organización es imposible, sin embargo, se puede disminuir la exposición al riesgo debido a vulnerabilidades y amenazas que se generan día a día para los activos de la información, a través de la implementación de controles de seguridad de la información. Estos controles deben ser seleccionados, definidos, implementados, mantenidos y mejorados eficazmente conforme sea necesario.

Los sistemas SGSI funcionan bajo un esquema de mejora continua en cual, constantemente se supervisa y evalúa la eficacia de los controles y procedimientos implementados, además de identificar los riesgos emergentes, logrando obtener un nivel de seguridad altamente satisfactorio reduciendo al mínimo los riesgos. Todo este proceso sistemático permite que la organización alcance sus objetivos de negocio y mantenga y mejore su competitividad.

1.5.1. Normas para la Seguridad de la Información

Existen varias herramientas para la gestión de la seguridad de la información, que ayudan a establecer y definir aspectos claves para la implementación y mantenimiento de estrategias de seguridad efectivas. Una de estas herramientas son las normas ISO/IEC que proveen estándares y guías relacionados con sistemas de gestión aplicables en cualquier tipo de organización y con cualquier herramienta específica.

La serie ISO/IEC 27000 es un conjunto de estándares que proporcionan pautas para establecer e implementar un sistema de gestión de la seguridad de la información (SGSI), tomando en cuenta que la aplicación estará influenciada por las necesidades propias de cada organización, objetivos, requisitos de seguridad, procesos, tamaño y estructura.

1.5.1.1. Norma ISO/IEC 27002:2013

La norma *ISO/IEC 27002:2013 Tecnología de la Información. Técnicas de seguridad. Código de buenas prácticas para la gestión de la seguridad de la información*, establece las directrices y principios generales para el comienzo, la implementación, el mantenimiento y la mejora de la gestión de la seguridad de la información, mediante objetivos de control (aspectos a analizar para garantizar la seguridad de la información) y controles (medidas a tomar).

La seguridad de la información se logra mediante la implementación de un conjunto adecuado de controles, incluyendo políticas, procesos, procedimientos, estructuras organizacionales y funciones de software y hardware. Estos controles deben ser establecidos, implementados, monitoreados, revisados y mejorados, donde sea necesario, para asegurar que se cumplan los objetivos específicos de seguridad y de negocios de la organización. (ISO/IEC, 270002:2013)

El primer paso para la implementación de un SGSI consiste en identificar los requisitos de seguridad. Existen tres fuentes principales de requisitos de seguridad:

a) La evaluación de los riesgos para la organización, teniendo en cuenta la estrategia y objetivos globales de la organización. A través de una evaluación de riesgos, se identifican las amenazas a los activos, se evalúa la vulnerabilidad y la probabilidad de ocurrencia y se calcula el impacto potencial; (ISO/IEC, 270002:2013)
b) Los requisitos legales, reglamentarios y contractuales que una organización, sus socios comerciales, contratistas y proveedores de servicios deben satisfacer y su entorno sociocultural; (ISO/IEC, 270002:2013)
c) El conjunto de principios, objetivos y requisitos de negocio para el manejo, procesamiento, almacenamiento, comunicación y archivo de la información que una organización ha desarrollado para apoyar sus operaciones. (ISO/IEC, 270002:2013)

Los resultados de la evaluación de riesgos permitirán a la organización determinar la acción de gestión y los controles apropiados para proteger los activos contra estos riesgos, colocando prioridades para gestionar cada uno de ellos. La norma ISO/IEC 27005 proporciona orientación sobre gestión de riesgos de seguridad de la información, incluyendo asesoramiento sobre evaluación, tratamiento, aceptación, comunicación, monitoreo y revisión de riesgos. La ISO/IEC 27002: 2013 está formada por 14 dominios de control de seguridad que contiene un total de 35 categorías principales de seguridad y 114 controles.

1.5.1.1.1. Selección de Controles

La norma establece un marco de controles que pueden considerarse como principios para la gestión de la seguridad de la información, que son aplicables a la mayoría de las organizaciones. La selección de los controles dependerá de las decisiones organizativas basadas en los criterios de

aceptación de riesgos, las opciones de tratamiento de riesgos y el enfoque general de gestión de riesgos aplicados a la organización y también estará sujeta a toda la legislación nacional e internacional pertinente. (ISO/IEC, 270002:2013)

Las categorías de control o dominios de control contienen un objetivo de control que indica lo que se va a lograr; y uno o más controles que se pueden aplicar para lograr el objetivo de control.

1.5.1.1.2. Dominios de Control

Cada dominio define controles que contienen una o más categorías de seguridad. Dependiendo de las circunstancias y el tipo de organización se deben aplicar uno o todos los dominios que sean necesarios, cada organización debe identificar que controles aplicar y la importancia de los mismos dentro de sus procesos de negocio. Dentro de cada dominio, se especifican los objetivos de los distintos controles para la seguridad de la información.

i. Políticas de la Seguridad de la Información.
ii. Organización de la Seguridad de la Información.
iii. Seguridad de los Recursos Humanos.
iv. Gestión de los Activos.
v. Control de Accesos.
vi. Criptografía.
vii. Seguridad Física y Ambiental.
viii. Seguridad de las Operaciones.
ix. Seguridad de las Comunicaciones.
x. Adquisición de sistemas, desarrollo y mantenimiento
xi. Relaciones con los Proveedores: seguridad de la información en las relaciones con los proveedores.
xii. Gestión de Incidencias que afectan a la Seguridad de la Información

xiii. Aspectos de Seguridad de la Información para la Gestión de la Continuidad del Negocio

xiv. Conformidad

1.5.1.1.3. Seguridad de las Operaciones

Este dominio describe las mejores prácticas para la seguridad de operaciones, contiene controles para registro de eventos de usuarios, excepciones, fallas y eventos seguridad de la información que deben ser protegidos contra la manipulación y acceso no autorizado. Además, controles para la evolución de vulnerabilidades y la implementación de medidas adecuadas para hacer frente a los riesgos asociados.

1) Procedimientos y responsabilidades operativas*:*
   Objetivo. - Asegurar operaciones correctas y seguras de instalaciones de procesamiento de información.
   a) Procedimientos operativos documentados
      Control: Los procedimientos operativos deben documentarse y ponerse a disposición de todos los usuarios que los necesiten.
   b) Gestión del cambio
      Control: Deben controlarse los cambios en la organización, los procesos empresariales, las instalaciones de procesamiento de la información y los sistemas que afectan a la seguridad de la información.
   c) Gestión de la capacidad
      Control: El uso de los recursos debe ser monitoreado, sintonizado y proyecciones hechas de los requerimientos futuros de capacidad para asegurar el desempeño requerido del sistema.
   d) Separación de entornos de desarrollo, prueba y operación
      Control: Los entornos de desarrollo, pruebas y operacionales deben estar separados para reducir los riesgos de acceso no autorizado o cambios en el entorno operativo.
2) Protección contra el malware:

Objetivo. - Asegurar que el procesamiento de la información y la información de las instalaciones están protegidos contra el malware.

a) Controles contra el malware

Control: Los controles de detección, prevención y recuperación para proteger contra el malware deben ser implementados, combinados con la conciencia apropiada del usuario.

3) Respaldo:

Objetivo. - Proteger contra la pérdida de datos.

a) Respaldo de información

Control: Copias de seguridad de información, software e imágenes del sistema deben ser tomadas y probadas regularmente de acuerdo con una política de respaldo acordada.

4) Registro y seguimiento:

Objetivo. - Registrar eventos y generar pruebas.

a) Registro de sucesos

Control: Los registros de eventos que recopilan las actividades del usuario, las excepciones, los fallos y los eventos de seguridad de la información deben ser producidos, mantenidos y revisados regularmente.

b) Protección de la información del registro

Control: Las instalaciones de registro y la información de registro deben estar protegidas contra la manipulación y el acceso no autorizado.

c) Registros del administrador y del operador

Control: Las actividades del administrador del sistema y del operador del sistema deben ser registradas y los registros protegidos y revisados regularmente.

d) Sincronización del reloj

Control: Los relojes de todos los sistemas de procesamiento de información relevantes dentro de una organización o dominio de seguridad deben sincronizarse con una única fuente de tiempo de referencia.

5) Control de software operacional

Objetivo. - Garantizar la integridad de los sistemas operativos.

a) Instalación de software en sistemas operacionales

Control: Deben implementarse procedimientos para controlar la instalación de software en los sistemas operacionales.

6) Gestión técnica de la vulnerabilidad

Objetivo. - Evitar la explotación de vulnerabilidades técnicas.

a) Gestión de vulnerabilidades técnicas

Control: La información sobre las vulnerabilidades técnicas de los sistemas de información que se están utilizando debe obtenerse de manera oportuna, se debe evaluar la exposición de la organización a tales vulnerabilidades para definir las medidas apropiadas para abordar el riesgo asociado.

b) Restricciones en la instalación del software

Control: Deben establecerse e implementarse reglas que rijan la instalación de software por parte de los usuarios.

7) Sistemas de información consideraciones de auditoría

Objetivo. - Minimizar el impacto de las actividades de auditoría en los sistemas operativos.

a) Controles de auditoría de sistemas de información

Control: Los requisitos de auditoría y las actividades que impliquen la verificación de los sistemas operacionales deben planearse cuidadosamente y acordarse para minimizar las interrupciones en los procesos empresariales.

1.5.1.1.4. Seguridad de las Comunicaciones

Este dominio describe las mejores prácticas para la seguridad de comunicaciones, contiene controles entorno a la gestión y protección de la información en los sistemas informáticos y aplicaciones, además políticas y procedimientos para proteger la transferencia de información a través del uso de todo tipo de comunicación.

1) Gestión de la seguridad de redes

Objetivo. - Garantizar la protección de la información en las redes y sus instalaciones de procesamiento de información de apoyo.

a) Controles de red

Control: Las redes deben ser gestionadas y controladas para proteger la información en sistemas y aplicaciones.

b) Seguridad de los servicios de red

Control: Los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red deben identificarse e incluirse en los acuerdos de servicios de red.

c) Segregación en redes

Control: Grupos de servicios de información, usuarios y sistemas de información deben ser segregados en redes.

2) Transferencia de información

Objetivo. - Mantener de información transferida dentro de una organización y con cualquier entidad externa.

- Políticas y procedimientos de transferencia de información

  Control: Deben establecerse políticas, procedimientos y controles para proteger la transferencia de información mediante el uso de todo tipo de medios de comunicación.
- Acuerdos sobre transferencia de información

  Control: Los acuerdos deben abordar la transferencia segura de información comercial entre la organización y las partes externas.
- Mensajería electrónica

  Control: La información involucrada en la mensajería electrónica debe estar debidamente protegida.
- Acuerdos de confidencialidad o no divulgación

  Control: Los requisitos para los acuerdos de confidencialidad o no divulgación deben reflejar las necesidades de la organización para la protección de la información deben ser identificados, revisados y documentados periódicamente.

1.5.1.2. Norma INEN ISO/IEC 27005:2012

Esta norma contiene recomendaciones y directrices para la gestión de riesgos de la seguridad de la información en una organización. Es compatible con los conceptos especificados en la norma ISO/IEC 27001 y está diseñada como soporte para facilitar la implementación satisfactoria un sistema de gestión de seguridad de la información con base en el enfoque de gestión del riesgo.

La gestión de riesgo de la seguridad de la información es una actividad recurrente que se refiere al análisis, planificación, ejecución, control y seguimiento de las medidas implementadas y la política de seguridad impuesta. Los indicadores de riesgo muestran si la organización está sujeta o tiene una alta probabilidad de ser sometida a un riesgo que excede el riesgo permitido. La gestión el riesgo consta del establecimiento del establecimiento del contexto, valoración del riesgo, tratamiento del riesgo, aceptación del riesgo, comunicación del riesgo y monitoreo y revisión del riesgo.

1.5.1.3. Análisis del riesgo

- Identificación del riesgo

El propósito de la identificación del riesgo es determinar qué podría suceder que cause una pérdida potencial, y llegar a comprender el cómo, dónde y por qué podría ocurrir esta pérdida.

- Identificación de los activos

Un activo es todo aquello que tiene valor para la organización y que, por lo tanto, requiere de protección. Para la identificación de los activos se recomienda tener en cuenta que el sistema de información consta de más elementos que sólo hardware y software, teniendo un nivel adecuado de detalle, que proporcione información suficiente para la valoración del riesgo.

- Identificación de las amenazas

Una amenaza tiene el potencial de causar daños a activos tales como información, procesos y sistemas, por lo tanto, a las organizaciones. Las amenazas pueden ser de origen natural o humano y podrían ser accidentales o deliberadas. Es recomendable identificar tanto los orígenes de las amenazas accidentales como de las deliberadas. Una amenaza puede tener su origen dentro o fuera de la organización, se debe tomar en cuenta cualquier tipo de amenaza que pueda provocar pérdida de información.

- Identificación de los controles existentes

Se debería realizar la identificación de los controles existentes para evitar trabajo o costos innecesarios. Además, mientras se identifican los controles existentes es recomendable hacer una verificación para garantizar que los controles funcionan correctamente, si el control no funciona como se espera, puede causar vulnerabilidades.

- Identificación de las vulnerabilidades

Se pueden identificar vulnerabilidades en las áreas de organización, procesos y procedimientos, rutinas de gestión, personal, ambiente físico, configuración del sistema de información, hardware, software o equipo de comunicaciones, dependencia de partes externas. La sola presencia de una vulnerabilidad no causa daño por sí misma, dado que es necesario que haya una amenaza presente para explotarla. Una vulnerabilidad que no tiene una amenaza correspondiente puede no requerir de la implementación de un control, pero es recomendable reconocerla y monitorearla para determinar los cambios.

1.5.1.4. Estimación del Riesgo

El análisis del riesgo se puede realizar con diferentes grados de detalle dependiendo de la criticidad de los activos, la amplitud de las vulnerabilidades conocidas y los incidentes anteriores que implicaron a la organización. Una metodología de estimación puede ser cualitativa o cuantitativa, o una

combinación de ellas, dependiendo de las circunstancias. En la práctica, con frecuencia se utiliza la estimación cualitativa en primer lugar para obtener una indicación general del nivel del riesgo y revelar los riesgos más importantes. Posteriormente puede ser necesario realizar un análisis más específico o cuantitativo de los riesgos importantes dado que es, por lo general, menos complejo y menos costoso realizar un análisis cualitativo que uno cuantitativo.

La estimación del riesgo asigna valores a la probabilidad y las consecuencias de un riesgo. Estos valores pueden ser cuantitativos o cualitativos. La estimación del riesgo se basa en las consecuencias evaluadas y la probabilidad. Además, la estimación puede considerar el beneficio de los costos, los intereses de las partes involucradas y otras variables, según correspondan para la evaluación del riesgo. El riesgo estimado es una combinación de la probabilidad de un escenario de incidente y sus consecuencias.

1.5.1.5. Evaluación del riesgo

Los criterios de evaluación del riesgo utilizados para tomar decisiones deberían ser consistentes con el contexto definido para la gestión del riesgo en la seguridad de la información externa e interna y deberían tomar en consideración los objetivos de la organización, los puntos de vista de las partes interesadas, etc. Las decisiones, tal como se toman en la actividad de evaluación del riesgo, se basan principalmente en el nivel aceptable de riesgo. Sin embargo, también es recomendable considerar las consecuencias, la probabilidad y el grado de confianza en la identificación y el análisis del riesgo. La agrupación de múltiples riesgos bajos o medios puede dar como resultado riesgos globales mucho más altos y es necesario tratarlos según corresponda.

1.5.1.6. Tratamiento del riesgo

Existen cuatro opciones disponibles para el tratamiento del riesgo: reducción del Figura 5 ilustra la actividad del tratamiento del riesgo dentro de los procesos de gestión del riesgo de la seguridad de la información.

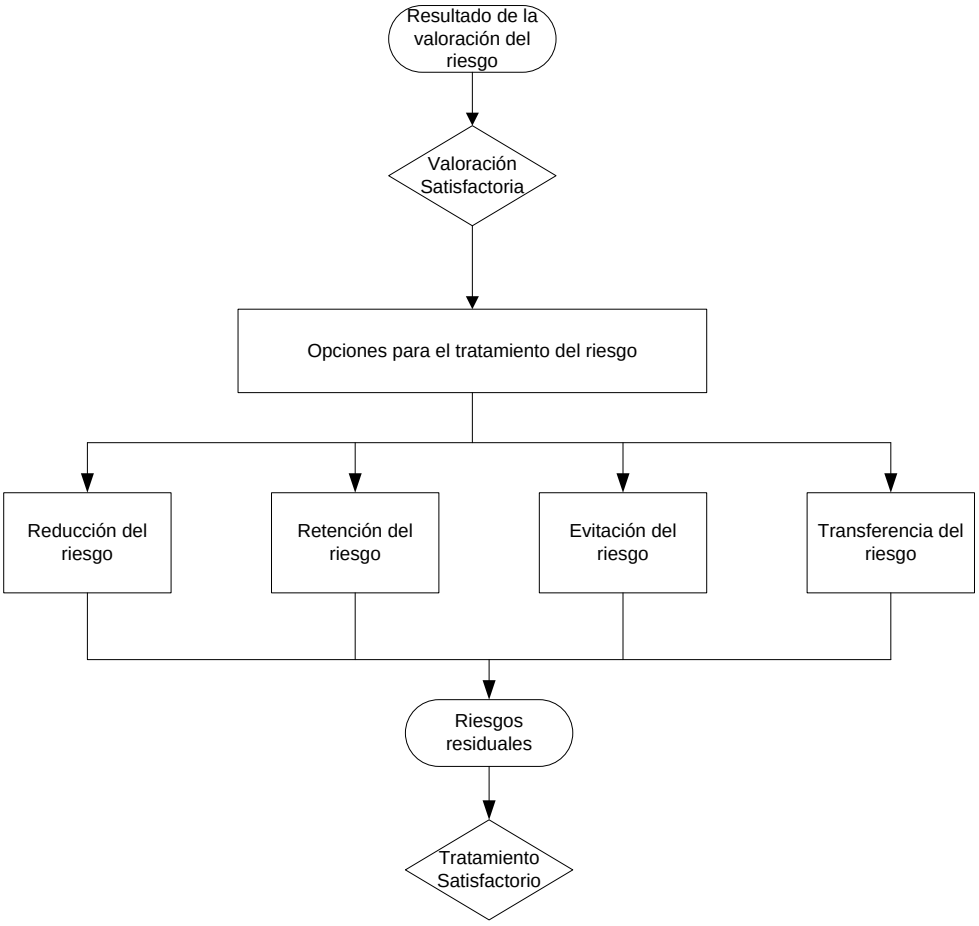


Figura 5 Actividad para el tratamiento del riesgo.

Fuente: (ISO/IEC, 27001:2005)

- Reducción del riesgo

El nivel del riesgo se debería reducir mediante la selección de controles, de manera tal que el riesgo residual se pueda reevaluar como aceptable. Se recomienda seleccionar controles adecuados y justificados que satisfagan los requisitos identificados en la valoración y el tratamiento del riesgo.

- Retención del riesgo

Si el nivel del riesgo satisface los criterios para su aceptación, no es necesario implementar controles adicionales y el riesgo se puede retener.

- Evitación del riesgo

Cuando los riesgos identificados se consideran muy altos, o si los costos para implementar otras opciones de tratamiento del riesgo exceden los beneficios, se puede tomar una decisión para evitar por completo el riesgo, mediante el retiro de una actividad o un conjunto de actividades planificadas o existentes, o mediante el cambio en las condiciones bajo las cuales se efectúa tal actividad.

- Transferencia del riesgo

El riesgo se debería transferir a otra parte que pueda gestionar de manera más eficaz el riesgo particular dependiendo de la evaluación del riesgo. La transferencia del riesgo involucra una decisión para compartir algunos riesgos con las partes externas. Puede crear riesgos nuevos o modificar los riesgos identificados existentes. Por lo tanto, puede ser necesario el tratamiento adicional para el riesgo.

1.5.1.7. Aceptación del riesgo de la seguridad de la información

Se debería tomar la decisión de aceptar los riesgos y las responsabilidades de la decisión, y registrarla de manera formal. Los planes para el tratamiento del riesgo deberían describir la forma en que los riesgos valorados se deben tratar, con el fin de satisfacer los criterios de aceptación del riesgo. Es importante que los directores responsables revisen y aprueben los planes propuestos para el tratamiento del riesgo y los riesgos residuales resultantes, y que registren todas las condiciones asociadas a tal aprobación.

1.5.1.8. Riesgo de TI

Los riesgos de Tecnologías de Información (TI) que pueden presentarse para cometer fraudes son los siguientes:

- Fallas en el hardware y/o software
- Falta de seguridades lógicas y físicas
- Indisponibilidad e integridad dudosa de los datos
- Acceso no autorizado a la información y a los sistemas
- Fallas en las telecomunicaciones

- Interrupciones de los sistemas
- Software malicioso

1.6. Mecanismos de Protección

Un sistema de gestión de seguridad de la información establece un conjunto de controles o mecanismos de seguridad orientados a minimizar las probabilidades del riesgo debido a las vulnerabilidades propias del sistema de la organización y le permitan ser más eficiente y seguro. Los mecanismos de protección de seguridad informática son técnicas o herramientas físicas y/o lógicas que permiten fortalecer la disponibilidad, integridad y confidencialidad del sistema informático. Los mecanismos son también controles que indican la forma en la cual se deben ejecutar las acciones que permitan mitigar las amenazas, vulnerabilidades y sus riesgos en los sistemas. Existen varios mecanismos de seguridad informática, su selección depende del tipo de sistema, función y factores de riesgo que lo amenazan; principalmente se dividen en tres grupos de acuerdo al nivel de madurez de la organización frente al concepto de seguridad de la información y la importancia atribuida a la implementación de procesos sistémicos y controles para resguardar la seguridad, se los puede definir como mecanismos preventivos, detectivos y de gestión.

1.6.1. Mecanismo Preventivos

Los mecanismos preventivos como su nombre lo indica actúan antes de que un incidente de seguridad ocurra, tienen como finalidad prevenir la ocurrencia de un ataque informático durante el funcionamiento normal del sistema. Los mecanismos aplicables varían desde una habitación con una cerradura y llave hasta equipos más sofisticados para monitoreo de la información, encriptación de código, cifrado de comunicaciones, control de activos, accesos y autenticación, cámaras de video vigilancia y sistemas de alimentación ininterrumpida (UPS).

Los mecanismos preventivos representan un primer paso en la implementación de un SGSI, las organizaciones inicialmente muestran su interés por proteger su información e invierten en equipos de bajo costo que les permitan algún nivel de seguridad, equipos de seguridad perimetral, soluciones de antivirus, de anti spam, sistemas de autenticación. A continuación, una descripción rápida de cada uno de ellos:

- *Soluciones de Antivirus:*

Son programas informáticos cuya función principal es detectar y eliminar virus y otros códigos maliciosos antes o después de que ingresen a los equipos informáticos. Utilizan varios mecanismos de detección para analizar continuamente el sistema y evitar robo y pérdida de información, alteración del funcionamiento, disrupción del sistema y propagación hacia otros equipos.

- *Cortafuegos (Firewall):*

Es un dispositivo de hardware o un software que nos permite gestionar y filtrar tráfico de red entrante y saliente. Configurados para permitir, limitar, cifrar y descifrar, el tráfico en base a un conjunto criterios y normas de seguridad. Permiten a las organizaciones tener un monitoreo de seguridad en tiempo real, las 24 horas del día, y un análisis de registros, lo que ayuda a detectar y responder ante intrusiones no deseadas o cualquier tipo de ataque informático.

- *Anti-spam:*

Son mecanismos o herramientas que permiten detectar y eliminar correos basura o no deseados. El principal objetivo de una herramienta anti spam, es lograr un buen porcentaje de filtrado de correo no deseado, para evitar que el buzón de correo se sature y provoque una pérdida de información total o parcial de correos que no pueden ingresar al sistema o ya se encuentran en él. Algunos antivirus y firewalls poseen incorporadas herramientas anti spam que permiten migar los riesgos y prevenir que las organizaciones ingresen al listado de listas negras.

1.6.2. Mecanismos Detectivos

Los preventivos representan una primera línea de defensa evitando muchos problemas y ataques externos contra la red, pero no garantizan estar libre de riesgos o daños. Es por ello que se hace casi indispensable el uso de mecanismos detectivos que tienen como objetivo detectar todo aquello que pueda ser una amenaza o violación para el sistema informático monitoreando constantemente la red en busca de comportamientos sospechosos. Denominados también sistemas de detección de intrusos (IDS) permiten detectar tanto las acciones de atacantes externos como las actividades anormales de usuarios internos que pueden producir daños en el sistema.

Se pueden considerar como intrusiones esencialmente tres actividades, como son las actividades de reconocimiento en las que el atacante realiza exploraciones de red para identificar direcciones IP, puertos, servicios activos y vulnerabilidades; actividades de explotación en las que se ataca el puerto o servicio detectado como vulnerable y para finalmente provocar la denegación de servicio dejando inactivos a los equipos de red. En el mercado podemos encontrar dos tipos de IDS basados en red y basados en host.

- *Sistemas de Detección de Intrusos basados en Red (NIDS):*

Son aplicaciones que permiten analizar todo el tráfico de paquetes, cada paquete es examinado y se comprueba su contenido en base a una base de datos de firmas de ataques y detectar así algún tipo de anomalía.

- *Sistemas de Detección de Intrusos basados en Host (HIDS):*

Son aplicaciones que residen dentro del host que monitorizan, se encargan de analizar registros de actividad, logs de registro, accesos a ficheros, configuraciones de las aplicaciones instaladas, etc., para detectar actividades anormales del host y ataques dentro de la red.

1.6.3. Mecanismos de Gestión

Los sistemas de red están expuestos a un número cada vez mayor de amenazas, que pueden provocar daños irreparables en los elementos activos de la información, muchas de las organizaciones a pesar de contar con soluciones o dispositivos de prevención y detección se siguen viendo expuestas a ataques informáticos, debido a que no se realiza una administración y procesamiento adecuado de los logs registrados por los equipos anteriores y no se toma las medidas de control eficaces que eliminen o disminuyan su exposición al riesgo. Es frecuente encontrar que los dispositivos de seguridad son administrados individualmente y cada uno contiene una fuente de registros aislada, todo esto hace necesario implementar adicionalmente sistemas de gestión centralizados que permitan almacenar, analizar y correlacionar los registros o eventos generados por los distintos equipos de red.

Estas herramientas de correlación de eventos permiten llevar a cabo una gestión más eficiente de todos los activos de la organización, mediante un monitoreo constante en tiempo real que facilita la detección de vulnerabilidades y amenazas, y reduce el tiempo de reacción y toma de decisiones de medidas correctivas ante posibles intrusiones. Dentro de las herramientas de gestión información y correlación de eventos se distinguen tres tipos de sistemas como se puede observar en la Figura 6.

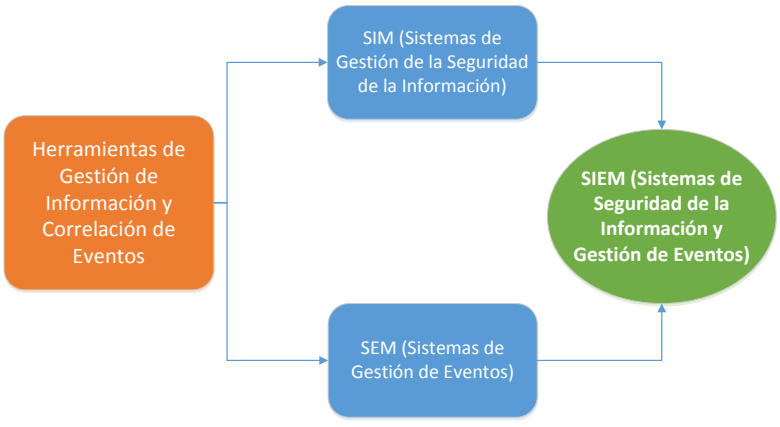


Figura 6 Herramientas de Gestión de la Información y Correlación de Eventos

- **SIM (Sistema de Gestión de la Seguridad de la Información)**

Las herramientas de gestión de seguridad de la información son sistemas de supervisión que se encargan de recolectar, correlacionar y analizar la información de seguridad de forma histórica, están optimizadas para captar grandes volúmenes de información y almacenarlas con una gran compresión para disminuir el espacio usado. Ayudan a centralizar y administrar la información de seguridad mediante reportes y archivos de registro.

- **SEM (Sistema de Gestión de Eventos)**

Las herramientas de gestión de eventos se encargan de monitorizar y gestionar los eventos producidos en la red en tiempo real. Su función principal consiste en recoger los datos de los eventos de seguridad producidos por los equipos de la red para realizar un análisis y correlación para brindar reportes en el menor tiempo posible Permiten la visualización, monitoreo y gestión de eventos que detecten situaciones anormales generando y automaticen las respuestas y medidas correctivas en caso de aparición de incidentes de seguridad. (Tejada, 2014)

- **SIEM (Sistema de Gestión de la Seguridad de la Información y Gestión de Eventos)**

Los sistemas de seguridad de la información y gestión de eventos es un híbrido de elementos SIM y SEM. Se encargan de monitorear, recolectar, analizar, correlacionar y presentar la información de eventos generados por los dispositivos de red, en tiempo real. La solución SIEM realizan un análisis y correlación de eventos detectando anomalías y amenazas que normalmente pasarían desapercibidas por un sistema IDS.

Estos sistemas permiten aplicar procedimientos de control y administración, que buscan atenuar las amenazas y mantener un bajo nivel de exposición de riesgo de la organización, asegurando la disponibilidad, integridad y confiabilidad del sistema. En el siguiente capítulo se realizará un análisis más detallado sobre este tipo de herramientas.

CAPITULO 2: ESTUDIO DE SOLUCIONES SIEM

2.1. Análisis SIEM (Sistema de Gestión de la Seguridad de la Información y Gestión de Eventos)

Hoy en día los ataques informáticos son cada vez más sofisticados e inmunes a la detección por parte de dispositivos convencionales. Los posibles ataques o amenazas pueden ser difíciles de detectar y pueden llegar a pasar desapercibidas, por lo que se hace necesario implementar soluciones completas que permitan una fácil administración y monitoreo de eventos, que nos lleven a la posibilidad real de detectar una posible intrusión en nuestros sistemas, como SIEM.

SIEM (Seguridad de la Información y Correlación de Eventos) proviene de una combinación de SEM y SIM. SEM (Gestión de Eventos de Seguridad) proporciona monitorización en tiempo real, recopilación de eventos, agregación y correlación en tiempo real, y una consola dinámica para gestión de eventos; y SIM (Gestión de Seguridad de la Información) muestra un análisis histórico y la presentación de informes de datos de eventos de seguridad.

En definitiva, las plataformas SIEM están formadas por una colección compleja de tecnologías diseñadas para realizar el monitoreo completo de la red, mediante la recopilación y correlación en tiempo real de eventos de login, acceso a bases de datos, logs de firewall, proxy, IPS, logs de aplicaciones, etc., y en base a ello predecir el comportamiento del sistema de tal forma que ante un comportamiento inusual del sistema informático puede generar una alerta y/o realizar una acción determinada.

2.1.1. Capacidades SIEM

Las soluciones SIEM se encargan de monitorear, recolectar, analizar, y presentar la información de eventos generados por los dispositivos de red, en tiempo real; permitiendo la gestión de vulnerabilidades y cumplimiento de

políticas. En la figura 7. Se pueden observar algunas de las capacidades de estas soluciones:

Figura 7 Capacidades SIEM

- *Agregación de datos:* Realizan un escaneo de la red para verificar la topología e identificar sus elementos activos, además de un continuo monitoreo y recolección de datos generados por los dispositivos, consolidando toda la información en una base de datos para su análisis.
- *Correlación:* Realiza la vinculación de eventos a través de atributos comunes, que permitan integrar varias fuentes con el fin de convertir los datos en información útil para la prevención de ataques.
- *Alertas:* Presenta alertas o notificaciones automatizadas en base al análisis y correlación de eventos generados en el sistema.
- *Dashboards:* Presentan informes o cartas informativas, en base a la recolección de eventos para ayudar a identificar patrones, o comportamientos anormales.
- *Retención:* Mantienen un almacenamiento de los datos históricos generados para facilitar la correlación de eventos pasados, y proporcionar una base de cumplimiento de normas.

2.1.2. Productos SIEM

En el mercado actual se presentan una gran cantidad de soluciones SIEM, que buscan solventar las diferentes necesidades de las organizaciones, de forma general la capacidad presentada por cada producto varía en forma proporcional a su costo y escalabilidad, teniendo como eje básico el monitoreo, recopilación y administración de eventos generados en la red. A continuación, en la Tabla 3 se muestran algunas de las soluciones SIEM que se puede encontrar en el mercado.

Tabla 3
Productos SIEM

PRODUCTOS SIEM			
	LogLogic		Splunk
	AlienVault (USM) / (OSSIM free)		LogRhythm
	McAfee Enterprise Security Manager		HP ArcSight
	Trustwave SIEM		IBM Security QRadar SIEM
	SenSage SIEM		SolarWinds LEM
	FileAudit		Accelops
	Cybereason		RSA Security Analytics
	Hyperic HQ (Free)		Securia SGSI (Free)

2.1.3. Comparación de Sistemas SIEM

En el mercado existen varias soluciones y marcas que permiten llevar a cabo la gestión y correlación de eventos de seguridad, sin embargo es importante seleccionar aquellas que tengan una respuesta rápida ante problemas, fácil despliegue, integración con la mayoria de sistemas y equipos de varias soluciones, y que puedan integrarse a varias fuentes. Para implementar cualquier tipo de solución de los diversos fabricantes es imperativo realizar una análisis de necesidades específicas para cada organización, pues en base a los objetivos de negocio se debe buscar la opcíon más adecuada.

Un fuente información o punto de partida de las organizaciones, para la busqueda de las mejores soluciones SIEM que existen en el mercado es el Cuadrante Mágico de Gartner, elaborado por la firma de consultoría e investigación Gartner, que se enfoca en el análisis de mercado de las nuevas tecnologías. Este cuadrante es una representación gráfica de la situación de un producto tecnológico específico en un momento determinado. En la Figura 8 se puede observar el cudrante mágico correspondiente a productos SIEM.

Figura 8 "Cuadrante Mágico" de Gartner para SIEM 2016.

Fuente: (Kavanagh & Rochford, 2016)

Para entender el Cuadrante se debe tomar en cuenta que el eje horizontal “Integridad de Visión” representa cuántas características puede tener un producto y las mejora innovadoras que se están realizando; el eje vertical “Capacidad de Ejecución” que determina la capacidad de venta del producto y la calidad de sus revendedores y distribuidoes. Con ello nos indica que a pesar de que un producto se encuentre en el lugar más alto de dentro del cuadro de líderes no siempre implica que tenga un mejor desarrollo tecnológico.

Cabe recalcar que la versión analizada por Gartner de AlienVault corresponde a la versión comercial (pagada) USM y tiene como versión gratuita OSSIM; está verión es más limitada en sus capacidades y soporte, sin embargo presenta un alto despliegue de componentes, y es una solución muy conveniente para aquellas organizaciones pequeñas y medianas que buscan implementar un sistema de gestión de seguridad informática. A continuación en la Tabla 4 Se muestra un comparativo con los aspectos más reelevantes:

Tabla 4
Comparativo USM vs OSSIM

USM **(Gestión de Seguridad Unificada)**	**OSSIM**
Comercial	Código Abierto
Inteligencia de amenaza **Apoyado por la Comunidad**	Inteligencia de amenaza semanal Actualizaciones desarrolladas por el Equipo de Investigación de Laboratorios AlienVault
Robusta gestión y búsqueda de registros& Retención de registro a largo plazo	Limitada colección de eventos &Retención de registro sólo para eventos SIEM →

+ 150 informes personalizable, incluyendoInforme de cumplimiento específico	3 Informes Plantillasde Alto Nivel
Arquitectura Multi-Tier Federada Varios servidores a través de geografías o un servidor con múltiples sensores	Las implementaciones planas de servidores individuales
Multi-usuario, control de acceso basado en roles con plantillas de permisos	Único Usuario
Administración y Configuración Centralizada	Gestión de componentes individuales
Soporte Profesional	Apoyo de la Comunidad

Garnert en su informe indica de Alien Vault que: “Referencias de clientes indican que las ofertas de software y equipamiento son mucho menoscaros que los conjuntos de productos correspondientes de la mayoría de los competidores en elespacio SIEM. La media de las puntuaciones de satisfacción del cliente AlienVault de referencia para las reglaspredefinidas de correlación e informes, y la capacidad de crear reglas de correlación personalizada, esmás alta que las puntuaciones medias para todos los clientes de referencia en esas áreas.” (Kavanagh & Rochford, 2016)

En base al Cuadrante Mágico de Gartner 2016, presentado en la Figura 8, se seleccionaron tres productos *IBM QRadar* del cuadrante de líderes, *EMC RSA* aspirante y *Alient Vault USM (OSSIM)* que es el único visionario de todas las soluciones, además el producto *Hyperic HQ* con licenciamiento gratuito para realizar una comparación con la herramienta que será implementada OSSIM presentado en la Tabla 5.

Tabla 5
Comparativo Productos SIEM

Característica	IBM QRADAR	EMC RSA	OSSIM	HYPERIC HQ
Costo de Licencia	Muy Alto	Muy Alto	Gratuita	Gratuita
Exploración de redes	√	√	√	X
Detección de intrusos	√	√	√	√
Deteccnión de vulnerabilidades	√	√	√	X
Monitorización de equipos Host	X	√	√	√
Plugins gratuitos	X	X	√	√
Notificaciones automáticas	√	√	√	√
Network IDS	√	√	√	X
Interface de usuario Web	√	√	√	X
Cantidad de usuarios	Múltiples	Múltiples	Uno	Uno
Registros a largo plazo	√	√	√	X
Soporte	Profesional	Profesional	Comunitario	Comunitario

2.2. OSSIM (Open Source Security Information Management)

En español OSSIM se traduce como una Herramienta de código abierto para la gestión de seguridad de la información; es una colección de herramientas en código abierto, desarrollado para gestionar la información de seguridad de una red, a través de una plataforma potente y centralizada que integra soluciones para detección y monitoreo de eventos de seguridad de una organización. Permite recolectar eventos generados por equipos de TI, para que el Administrador o Responsable de seguridad informática de la

organización pueda interpretarlos, analizarlos y monitorearlos, a través de una estructura completamente centralizada; con el fin de detectar posibles comportamientos anormales o eventos relevantes que podrían generar incidentes de seguridad.

La capacidad de la consola OSSIM para obtener información completa y selecta, de los miles de eventos que reportan otras herramientas, le permite ser una herramienta muy útil. A los administradores de red, les permite elegir el procedimiento que regirá la seguridad en el sistema de información, pudiendo así, detectar amenazas rápidamente y disponer de un nivel adecuado de protección para la información y equipos que permiten la comunicación dentro de la red. (Torres & Villegas, 2010). Para gestionar la red de forma eficiente y centralizada cuenta con un conjunto de características entre las cuales podemos mencionar:

- Gratuito. .
- Monitoreo centralizado de eventos y tráfico excesivo.
- Análisis de los posibles riesgos y anomalías en la red.
- Controla de posibles ataques en la red.
- Interfaz web gráfica amigable con Administrador de TI.
- Recolección de logs.
- Test de vulnerabilidad.
- Notificaciones automáticas mediante alertas y presentación de informes técnicos. Las notificaciones pueden ser:
    - Falso supuesto
    - Duplicidad de MAC
    - Clave incorrecta
    - Alerta de intruso
    - Posible ataque
    - Trafico excesivo... etc.

2.2.1. Capas de OSSIM

OSSIM se presenta como un sistema personalizado para las necesidades de cada organización por tres capas como se muestra en la Figura 9:

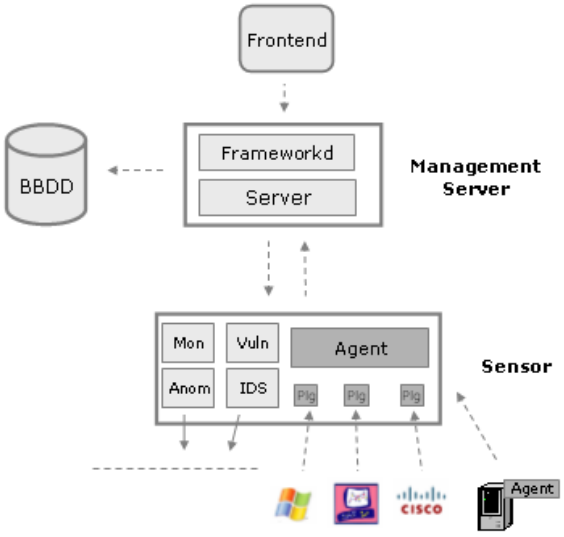


Figura 9 Capas del Herramienta OSSIM

- **Capa Inferior**

  También llamada nivel de "Preprocesador", se encarga de la recolección de datos a través de un conjunto de sensores y monitores, que se encargan de realizar la detección de los eventos que suceden en el sistema informático y posteriormente envían al sistema central para el análisis y correlación de los diferentes eventos. Entre algunos de los sensores dispersos en la red se tiene: IDS (detectores de patrones), detectores de intrusos y anomalías, Firewalls y varios tipos de Monitores.

- **Capa Intermedia**

  También llamada nivel de "Post procesado", se encarga de realizar el procesamiento y análisis de los datos recolectados por los sensores, utilizando la correlación de eventos para dar nivel de prioridad y valorar el riesgo que pueden producir para el sistema; aumentando la

sensibilidad y la fiabilidad de la red. En esta capa se realizan tareas de normalización, correlación, priorización y valoración de Riesgos. En esta capa se distinguen tres elementos importantes:

- ***Base de Datos de Eventos (EDB)***
  Almacena todos los datos (logs) generados por los sensores dispersos en la red, estos datos son normalizados y mostrados al administrador de alarmas y reportes.
- ***Base de Datos de Framework (KDB)***
  Almacena las configuraciones de las políticas de seguridad aplicadas para poder identificar el tipo de información que se genera en los distintos dispositivos de red.
- ***Base de Datos de los Perfiles (UDB)***
  Almacena todos los datos aprendidos en el constante monitoreo de la red, discriminarlos y tomar las precauciones necesarias a futuro.

- **Capa Superior**
  Esta capa corresponde al framework o “Front-end”, corresponde a la consola web de administración, permite configurar y visualizar todos los módulos que constituyen el sistema de seguridad; en esta consola se definen topologías, inventario de activos, políticas de seguridad, reglas de correlación y enlazar las diferentes herramientas integradas.

2.2.2. Componentes OSSIM

La arquitectura de OSSIM nos muestra que está formado básicamente por tres componentes esenciales como son el servidor, sensor y agentes.

- **Servidor OSSIM**

Es un programa esencial de la herramienta de gestión OSSIM se encarga de recolectar en una base de datos los eventos generados por los distintos

sensores y de agregar y correlacionar los mismos en tiempo casi real, facilitando la gestión a través de una única pantalla de control y administración, y disminuyendo el tiempo y complejidad de análisis que requieren los incidentes de seguridad. Utiliza la información de los activos instalados, así como sus vulnerabilidades y amenazas, para ofrecer un análisis exhaustivo y preciso sobre los posibles ataques de seguridad. El servidor se encarga de varias funciones como:

- Recolectar datos de los agentes y otros servidores
- Priorizar los eventos recibidos
- Correlacionar los eventos recibidos de diferentes fuentes
- Realizar la evaluación de riesgos y disparar alarmas
- Almacenar eventos en la base de datos
- Reenviar eventos o alarmas a otros servidores

- **Sensores**

Los sensores se hallan desplegados en la red para censar y detectar la actividad de los diferentes dispositivos de red, se encarga de generar los registros de logs se luego son enviados al servidor para ser analizados y mostrados al administrador de red. Inspeccionan todo el tráfico y recopilan información sin afectar el rendimiento de la red. Estos sensores utilizan más de diez sistemas expertos que identifican ataques a lo largo de cinco ejes diferentes:

- Detección de intrusiones
- Detección de anomalías
- Detección de Vulnerabilidad
- Descubrimiento y perfiles de red
- Sistemas de Inventario

Todos estos sistemas localizan en tiempo casi real tanto ataques conocidos como desconocidos a través de informes de aprendizaje y

anomalías. Identificando vulnerabilidades y amenazas de red latentes que pueden ser corregidas antes de que se produzca un ataque.

- **Agentes**

Los agentes son instalados en cada los equipos o dispositivos de red que vayan a ser monitoreados. Realizan un seguimiento de las configuraciones de hardware y software de los equipos, así como de actividades anormales que puedan comprometer la integridad del equipo. Los agentes se encargan de recolectar todos los datos enviados por los diferentes dispositivos estandarizar estos datos para que los sensores pueda entenderlos, y luego enviarlos al servidor. Estos agentes funcionan en cualquier sistema Unix, Linux, Mac y Windows y brindan gran detalle de los distintos eventos que se puedan suscitar en la red.

2.2.3. Arquitectura OSSIM

OSSIM tiene una arquitectura abierta, basada en tres capas analizadas anteriormente, cada una de ellas está formada por niveles como se muestra en la Figura 10, los cuales describen el funcionamiento de la herramienta.

Figura 10 Arquitectura de Herramienta OSSIM

1) El primer nivel corresponde a los *detectores de patrones,* que corresponden a aplicaciones que analizan el tráfico de red en busca de patrones malignos definidos a través de firmas o reglas; en caso de detectar un patrón envían alertas al sistema de seguridad. Tantos

dispositivos específicos para detección (por ejemplo: IDS) como cualquier otro dispositivo de la red, como switch, firewall, o el mismo sistema operativo de los hosts, tienen la capacidad de detectar patrones y alertar al sistema a través de log de seguridad.

2) Los *detectores de anomalías* presentan capacidades más avanzadas que en el caso anterior, en este caso no es necesario especificar al sistema, mediante reglas que es un comportamiento bueno o malo, sino que es capaz de "aprender" por sí solo y emitir alertas cuando un comportamiento difiere de lo normal.

3) La *normalización* se encarga de agrupar todos los eventos de seguridad generados por los diferentes detectores en un solo lugar y con un mismo formato.

4) La *priorización* permite definir la importancia de un evento de seguridad dependiendo de la topología de la red, inventario de cada máquina y del rol que estas desempeñan en la organización; en base a esto se aplicaran las políticas de seguridad necesarias en cada dispositivo.

5) Luego de priorizar los eventos, se procede a*valorar el riesgo*, en base a tres aspectos; el valor del activo al que el evento se refiere, la amenaza que representa y la probabilidad de que este ocurra. OSSIM calculará el Riesgo Instantáneo de cada evento, "producido por la recepción de una alerta, valorada de forma instantánea como la medida ponderada entre el daño que produciría el ataque y la fiabilidad del detector que lo reporta." (Muñoz, 2003)

6) La *correlación* es una función mediante la cual se relacionan diferentes eventos que pueden estar involucrados en el mismo ataque, "el motor de correlación se encarga de comprobar cada uno de los eventos y

busca evidencias o síntomas que prueben la veracidad de un ataque o si se trata de un falso positivo.” (Puchades & Peñalver, 2003)

7) Los *monitores* realizan un escaneo permanente de la red para detectar eventos anormales y dar una visualización al administrador del estado del sistema; indicando el nivel de riesgo de un proceso después de efectuada la correlación, y datos de sesiones de un host.

8) La *consola forense* permite analizar de forma centralizada todos los eventos que han sido recolectados y guardados por el sistema; muestra detalles sobre todos los riesgos detectados en la red.

9) Finalmente, el *cuadro de mandos* permite configurar una visión del estado de la red, a través de indicadores que miden el estado de seguridad de la organización, definiendo umbrales mínimos de cumplimiento.

2.2.4. Proceso de Detección

El principal objetivo del proyecto OSSIM es *aumentar la capacidad de detección* ofrecida por los productos hasta hoy desarrollados. Dicha capacidad de detección conlleva dos aspectos importantes, mostrados en la Tabla 6.

Tabla 6

Capacidad de Detección

Propiedad	Descripción	Efecto ante su ausencia
Fiabilidad	Grado de certeza que nos ofrece el detector ante el aviso de un posible evento.	*Falsos Positivos*
Sensibilidad	Capacidad de análisis que posee el detector a la hora de localizar un posible ataque.	*Falsos Negativos*

En la actualidad muchas de las soluciones carecen de estas propiedades provocando en su capacidad de detección dos principales problemas:

- Falsos Positivos, debido a la falta de confiabilidad o fiabilidad se detectan posibles ataques que realmente corresponden con ataques reales.
- Falsos Negativos, debido a la falta de sensibilidad no se detecta un posible ataque real.

El Proceso de Detección consiste en el descubrimiento de alertas y anomalías en la red, a través de la recopilación de datos originados por los detectores y monitores dispersos en la red; implica normalmente tres fases:

- **Pre proceso:** Implica la generación de alertas por los detectores y la consolidación previa al envío de información.

- **Colección:** Abarca el envío y recepción de toda la información de los detectores a un punto centralizado.

- **Post proceso:** Corresponde al tratamiento dado a la información a través de mecanismos de priorización valoración de riesgos y correlación, que mejoran la sensibilidad y fiabilidad de la detección, disminuyendo los falsos positivos y los falsos negativos.

2.2.4.1. Post proceso

Dentro del proceso de detección la colección y el pre proceso son capacidades comunes que no agregan valor transcendente en el sistema SIEM, sin embargo, en el post proceso, se pueden implementar mecanismos para mejorar la sensibilidad y fiabilidad de la detección. Elevando la complejidad del tratamiento de los eventos incluyendo métodos que se encargarán de descartar falsos positivos o al contrario descubrir patrones más complejos que los sensores y agentes han pasado por alto. Para ello se agregarán tres métodos en el post proceso:

1. *Priorización:* Donde se priorizan las alertas recibidas mediante un proceso de contextualización desarrollado a través de la definición de una Política de Seguridad y el Inventariado de activos.

2. *Valoración de Riesgo:* Cada evento será valorado respecto del Riesgo que implica, es decir, de una forma proporcional entre el activo al que aplica, la amenaza que supone y la probabilidad del evento.

3. *Correlación:* Donde se analizan un conjunto de eventos para obtener una información de mayor valor.

2.2.5. Herramientas OSSIM

OSSIM también está basado en una arquitectura de Distribución cuyo objetivo es integrar un conjunto herramientas OpenSource a través de una única consola de administración. Las aplicaciones propias y desarrolladas por terceros que se pueden integrar gracias a plugins específicos y genéricos configurables.

Tabla 7
IDS integrados en sistema OSSIM

IDS	
Herramienta	**Función**
Snort	Sistema de detección de intrusos en una Red (NIDS).
Osiris	Sistema de detección de intrusos a nivel de Host (HIDS).
OSSEC	Sistema de detección de intrusos basado en los logs (LIDS).

Tabla 8
Detectores integrados en sistema OSSIM

DETECTORES	
Herramienta	**Función**
Pads	Detección de anomalías en servicios.
Spade	Detección de anomalías en paquetes.
Arpwatch	Detección de anomalías en direcciones MAC.
P0f	Detección del sistema operativo y la versión de las maquinas conectadas en la red.

Tabla 9
Monitores integrados en sistema OSSIM

MONITORES	
Herramienta	**Función**
Ntop	Monitorización del tráfico de red.
Tcptrack	Sniffer utilizado para conocer información de las sesiones.
Nagios	Monitorización de la disponibilidad de host y servicios.

Tabla 10
Scanners integrados en sistema OSSIM

SCANNERS	
Herramienta	**Función**
Nessus	Scanner de vulnerabilidades en la red.
Nmap	Inventario de sistemas activos.

Tabla 11
SysLogs integrados en sistema OSSIM

SYSLOGS	
Herramienta	**Función**
Ntsyslog	Analizador de logs para Windows.
Syslog	Analizador de logs en Linux
Snarewindows	Trabaja como un manejador de logs y reporte de incidentes.

Tabla 12
Firewall integrados en sistema OSSIM

FIREWALL	
Herramienta	**Función**
Cisco PIX	Controla el tráfico entre la red interna y externa.
IPTables	Filtra el tráfico, recolecta los eventos de las iptables.

Tabla 13
Servidores Web integrados en sistema OSSIM

SERVIDORES WEB	
Herramienta	**Función**
IIS Colector	Servidor de páginas Web de Microsoft, registra los eventos del servidor, peticiones y errores.
Apache Colector	Servidor HTTP de código abierto, registra la actividad, rendimiento y los problemas que puedan ocurrir en el servidor HTTP.

CAPITULO 3: DISEÑO E IMPLEMENTACIÓN DEL PROTOTIPO

3.1. Introducción

La tecnología SIEM en la actualidad es una de las líneas de investigación más importantes en el ámbito de la seguridad informática. La esencia de esta tecnología es proporcionar una colección ordenada de registros de seguridad a partir de una variedad de fuentes, y almacenamiento en un repositorio centralizado de datos en un formato común para el modelado y análisis para detectar y predecir los ataques, y el desarrollo de contramedidas. (Kotenko, Polubelova, Chechulin, & Saenk, 2013)

En este capítulo se definirán los principales elementos y componentes del prototipo que será implementado, se ha considerado una arquitectura de red y seguridad perimetral tradicional que se puede encontrar en la mayoría de esquemas de pequeñas y medianas organizaciones. La herramienta OSSIM puede ser implementada y desplegada dentro de la red interna de la organización con una conexión directa al equipo de seguridad perimetral.

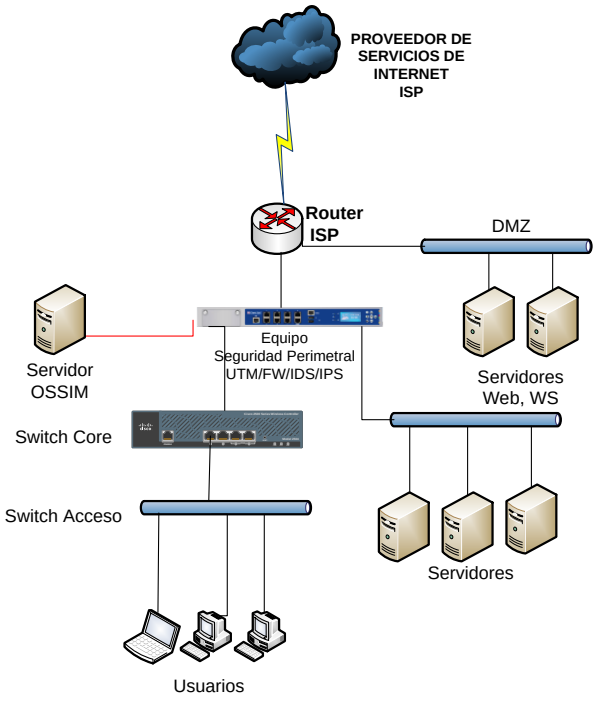


Figura 11 Arquitectura de red tradicional

Por seguridad de la red, OSSIM será considerado como un servidor y por tanto se deberá controlar sus conexiones internas y externas. Únicamente estarán habilitados los puertos que permitan la comunicación con los equipos considerados como fuente de registros a ser analizados. En la Figura 11, se puede apreciar la arquitectura de red tradicional que generalmente se maneja en cualquier organización, la cual será la base para definir la arquitectura de la solución OSSIM propuesta para el escenario de pruebas.

3.2. Arquitectura Propuesta para Herramienta OSSIM

La arquitectura mostrada en la Figura 12, indica el esquema de conexión del servidor OSSIM con equipos tecnológicos que son comúnmente utilizados en una infraestructura de red tradicional. El servidor OSSIM, así como todos los elementos se implementarán a través del software de virtualización Virtual Box, por sus prestaciones y rendimiento en comparación con otras soluciones de virtualización, además por su facilidad en el despliegue y administración de máquinas virtuales.

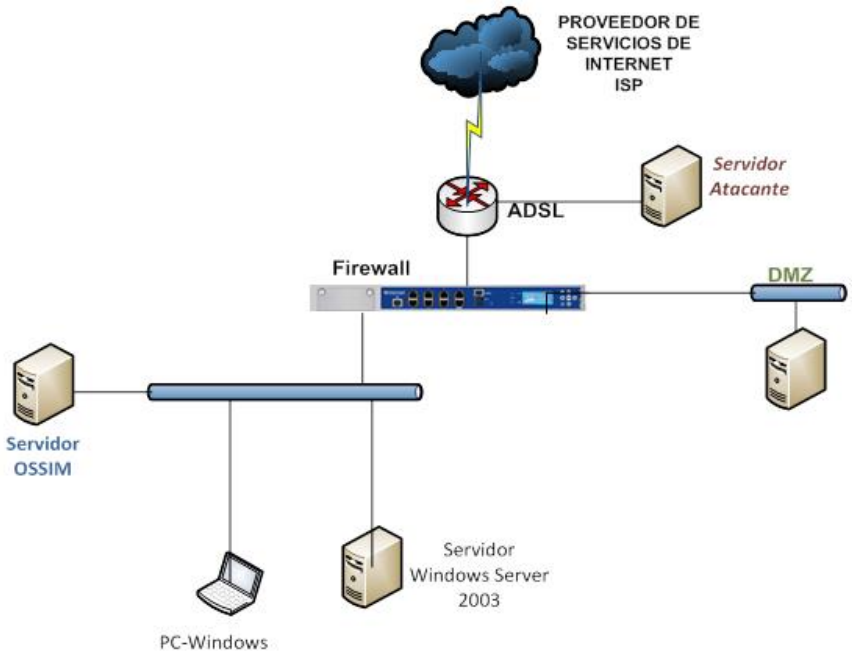


Figura 12 Topología de red

3.3. Selección de Fuentes de Eventos

Los equipos tecnológicos (Windows y Linux) que fueron seleccionados como Fuentes de Eventos responden a una arquitectura de red que es comúnmente implementada en pequeñas y medianas organizaciones. En las Tablas 14 y 15 se detalla el tipo de fuente, servicio o aplicativo a ser integrado en la solución propuesta para el escenario de pruebas.

Tabla 14
Descripción Nombres Identificadores de Fuentes de Eventos

Nombre del servidor o equipo	HostName Firewall	HostName OSSIM	HostName Virtual Box
Sistema de gestión de eventos de seguridad informática	OSSIM	OSSIM	OSSIM
Sistema de Seguridad Perimetral	Firewall	Firewall	FW
Servidor de autenticación	Windows-Server	Windows-Server	WS2008
Servidor de aplicación web	Ubuntu-Server	Ubuntu-Server	Ubuntu-Server
Equipo atacante	N/A	N/A	ATACANTE
PC-Windows	Windows-Cliente	Windows-Cliente	Windows-Cliente
PC-Ubuntu	Ubuntu-Cliente	Ubuntu-Cliente	Ubuntu-Cliente
PC-Administración	Windows-Administración	N/A	N/A

Tabla 15

Detalles de Fuentes de Eventos

Ítem	Servidor	Tipo Fuente	Dirección IP	Descripción
1	Sistema de gestión de eventos de seguridad informática.	Logs de seguridad	Eth0: 192.168.100.60	Servidor de sistema de gestión de eventos de seguridad informática.
2	Sistema de Seguridad Perimetral	Firewall de seguridad	Eth0: 192.168.100.1	Conexión a red interna de la empresa, aplicación de reglas de seguridad en intranet.
			Eth4: 192.168.200.3	Conexión a la red de servidores situados en el segmento de red DMZ.
			Eth1: 10.10.10.1	Administración y gestión de reglas de seguridad del sistema de seguridad perimetral.
			Eth2: 192.168.1.50	Conexión externa hacia Internet.
3	Equipo atacante	Escáner de Vulnerabilidades	192.168.2.1	Servidor externo para realizar pruebas de seguridad y análisis de vulnerabilidades hacia un cliente o servidor de la red interna.
4	Servidor de aplicación web.	Log de seguridad de acceso web. BDD MySQL.	Eth0: 192.168.200.3	Servidor ubicado en la DMZ, la base de datos que registrará las operaciones realizadas en una base de transaccional de negocio. →

				Además, activará los principales logs de seguridad, por ejemplo, los accesos al sistema.
5	Servidor de autenticación	Active Directory	Interfaz LAN: 192.168.100.10	Se registrarán los principales logs de seguridad del servidor, así como los accesos de los usuarios a la red.
6	PC-Ubuntu	Log de seguridad de acceso.	Eth0: 192.168.1.90	El agente instalado en el equipo cliente con sistema operativo Ubuntu recopilará información de los logs o registros de seguridad generados en el cliente.
7	PC-Windows	Log de seguridad de acceso.	Interfaz LAN: 192168100100	El agente instalado en el equipo cliente con sistema operativo Windows recopilará información de logs o registros de seguridad generados en el cliente.
PC-Admin	Windows-Administración	N/A	Interfaz LAN:10.10.10.2	No se registrarán los logs que genere este equipo.

3.4. Dimensión de Número de Eventos por Segundo (EPS)

El dimensionamiento del número de eventos por segundo (EPS) es una fase muy importante a la hora de implementar la solución integral de un

sistema de seguridad informática, un correcto dimensionamiento permitirá que la inversión esté acorde a las necesidades de la organización y requerimientos de seguridad. El dimensionamiento se lo realiza una vez identificado y seleccionado la fuente de datos, registros o logs a ser integrados en la solución, en base a dos criterios:

- Muestras en tiempo real: El primer método permite contar con un número bastante aproximado a la realidad, para ello es necesario instalar un recolector de logs que permita grabarlos en un archivo de texto plano, y posteriormente acceder al archivo y contar el número de líneas generadas en un lapso de tiempo. Dependiendo del sistema, aplicación o servicio de logs, se podría también contabilizar directamente en el módulo o administración de logs propio del equipo.

- Utilizando plantillas estándar: El segundo método es más eficiente y permite un cálculo aproximado de logs que se generan en equipos de red y servicios tradicionales, por lo general este método lo realizan las proveedores de las marcas reconocidas de equipos SIEM en la fase de levantamiento de información previo el dimensionamiento de la solución y posterior propuesta técnica económica a fin de que el cliente pueda analizarla, de ser el caso los proveedores ajustan los requerimientos del cliente de acuerdo a sus necesidades y presupuesto.

Debido a que el primer método es bastante complejo, tomaría demasiado tiempo en realizar, la integración al OSSIM de cada fuente de registros, a esto se suma la dificultad de realizarlo en horas pico lo que incidiría en el rendimiento del equipo censado. El método seleccionado para el prototipo fue mediante la utilización de una plantilla estándar, la cual considera de manera general que se tiene una ventana de generación de eventos diaria de 43200

segundos, es decir 12 horas, este criterio es adecuado por cuanto la mayor cantidad de logs que se genera son en horas laborables en el día.

En la Tabla 13, se resumen la cantidad de eventos por segundo (EPS), se puede apreciar los Bytes/log aproximados, que varían dependiendo de la complejidad e importancia de la fuente de registros; también se ha considerado la capacidad de almacenamiento diario en Mega Bytes (MB)/día, que se debe considerar para la retención de logs, que podrán ser útiles como evidencias frente alguna eventualidad de seguridad informática importante.

Tabla 16
Dimensionamiento de EPS

Tipo de Fuente	Cantidad	Logs al día	Logs/seg (EPS)	Bytes/log	EPS Totales	AnchoBanda Almacenamiento (bytes)	Almacenamiento Diario
Escanner Vulnerabilidades	1	80.000	1,85	500	2	926	38
Directorio Activo/LDAP / Radius	1	518.000	11,99	800	12	9.593	395
Controladores de Dominio	1	864.000	20,00	300	20	6.000	247
HIDS - Host IDS	2	43.000	1,00	400	2	796	33
Base de datos (Servidor Linux)	1	172.000	3,98	300	4	1.194	49
Servidores Unix / Linux (Log seguridades)	1	80.000	1,85	200	2	370	15
Servidores Windows	1	172.000	3,98	800	4	3.185	131
Ordenadores Personales	2	8.600	0,20	800	0	319	13
TOTALES	10			SUMA EPS	46	22.383	
				MEGAS GENERADOS POR SEGUNDO	MB	0,021	
				ALMACENAMIENTO DIARIO	GB		1

El almacenamiento diario mostrado en la Tabla 13 sugiere 1GB, sin embargo, para propósitos del prototipo propuesto será suficiente un almacenamiento de 500MB diarios. El sistema OSSIM debe contar con espacio en disco para al menos dos semanas con 5 días laborables da un total de 5GB para retención por dos semanas. El espacio de almacenamiento de disco duro para la máquina virtual del OSSIM en este caso será de 20 GB para mayor capacidad de tiempo.

3.5. Dimensionamiento del Hardware

Los requisitos de hardware para el despliegue del servidor OSSIM dependerán principalmente del número de eventos que tenga que procesar,

la cantidad de información de los registros que se quiera almacenar en la base de datos del OSSIM, y en general de la cantidad de clientes (agentes o host) en la red. De acuerdo al dimensionamiento de EPS y su respectivo almacenamiento, como requisito mínimo se consideró para el prototipo las características de una máquina virtual según la tabla 14:

Tabla 17
Requerimientos de Hardware para el Servidor OSSIM

Parámetro	Valor
Procesador	1 núcleo de 2,5 GHz o superior
Memoria	2 GB o superior
Disco Duro	20 GB o superior
Tarjeta de Red	100/1000 Mbps
Interfaces	Ópticas, lector USB.

3.6. Implementación y Configuración Servidor OSSIM

La implementación del prototipo del sistema de gestión de eventos de seguridad informática, contará con un entorno virtual, con ayuda del software Virtual Box; previo a la creación de la máquina virtual para el servidor OSSIM, se detalla brevemente, en la siguiente sección, las características y requerimientos del servidor OSSIM, así como el equipo físico sobre el cual se va a montar.

3.6.1. Requerimientos del Servidor Virtual OSSIM

Desde la versión OSSIM 4.0 no se cuenta con versiones de 32 bits del producto, y debido a que se encuentra en constante evaluación, cambios y mejoras por ser un software de libre distribución, la tendencia es mejorar la eficiencia de las prestaciones por cuanto OSSIM integra una gran variedad de herramientas de monitoreo, análisis de vulnerabilidades, entre otros, por lo que actualmente solo se podrá encontrar versiones para 64 bits.

Es importante mencionar, para referencia de interés, que OSSIM de 64 bits se intentó instalar en un equipo con CPU de arquitectura de 32 bits, en Virtual Box y VMware, presentando inconvenientes en la instalación, como se indica en las Figuras 14 y 15; se muestra el siguiente mensaje "*This kernel requires an x86-64 CPU, but only detected an i686 CPU. Unable to boot – please use a kernel appropiate for your CPU*".

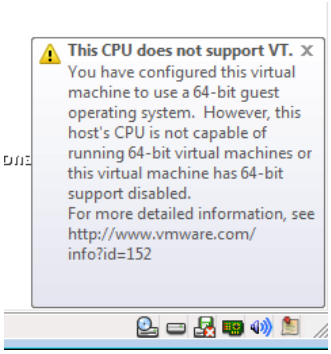


Figura 13 Mensaje VMware requiere tecnología VT

En la Figura 13, el software VMware muestra un mensaje de advertencia que indica que el CPU no soporta la opción VT (*Tecnología de Virtualización*), y se necesita una infraestructura de 64 bits para instalar el sistema operativo, en algunos casos la tecnología VT no viene habilitada en los computadores por lo que es necesario ingresar al BIOS del computador para activar la opción. Para mayor referencia se recomienda ingresar a la página del fabricante del procesador a fin de verificar la compatibilidad. Para procesadores Intel se recomienda utilizar la utilidad de identificación del procesador en el siguiente enlace: http://www.intel.com/support/processors/tools/piu/.

La tecnología Intel Virtualization Technology (Intel VT) asistida por el hardware en combinación con el software de virtualización adecuado, permiten la máxima la utilización de recursos del sistema consolidando varios entornos en un único servidor o computador. Intel VT logra esto eliminando cualquier tipo de dependencia de software del hardware subyacente, lo que a su vez ayuda a reducir costos, aumentar la eficiencia de la gestión, fortalecer

la seguridad, y hacer que la infraestructura informática más resistente en caso de un desastre. (Soporte_Sony, 2015)

Intel VT requiere una computadora con un procesador, un chipset, software o sistema operativo que active el BIOS, controladores de dispositivos y aplicaciones diseñadas para aprovechar las características de VT. Debido a esto, el rendimiento de las características VT variará dependiendo de la configuración de la computadora. (Soporte_Sony, 2015)

Figura 14 Mensaje de VMware OSSIM requiere CPU 64 bit

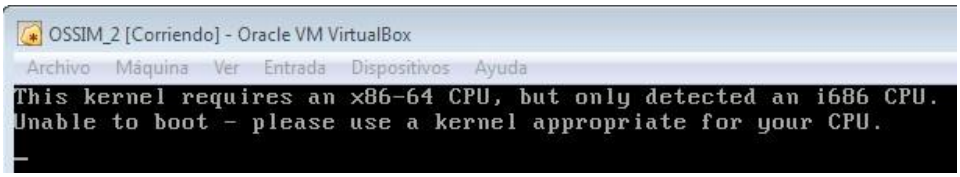


Figura 15 Mensaje de Virtual box OSSIM requiere CPU 64 bit

Por lo general las pequeñas y medianas organizaciones a fin de abaratar sus costos de operaciones tienden a utilizar computadores PC de 32 bit que no soportan la tecnología VT, por tanto, se recomienda verificar este requerimiento, así como realizar la actualización respectiva del BIOS, con el fin de no tener inconvenientes. Cabe señalar que en computadores modernos si se cuenta con procesadores de 64 bits o con la tecnología VT, es recomendable que las organizaciones manejen como estándar una infraestructura de 64 bits a pesar de que implique una pequeña inversión adicional en este sentido. La documentación de ayuda de Virtual Box indica que soporta sistemas operativos de 64 bits para virtualización, incluso con el sistema operativo host de 32 bits, si se cumple las siguientes condiciones:

- Es necesario un procesador de 64 bits con soporte de virtualización por hardware.

- Se debe habilitar la virtualización por hardware para máquinas virtuales en particular que se requiera que soporte 64 bits; la virtualización por software no soporta máquinas virtuales de 64 bits.

3.6.2. Requisitos Previos a la Instalación de OSSIM

Además de los requerimientos técnicos de hardware y software descritos anteriormente, es importante indicar que el personal técnico o administrador del equipo OSSIM tenga los conocimientos básicos necesarios para poder interpretar, analizar y manejar adecuadamente OSSIM y en general la solución integral de seguridad que se desee implementar en la organización, los conocimientos mínimos son:

- Poseer conocimientos básicos de Redes TCP/IP
- Tener conocimientos básicos de Administración de Redes
- Tener un conocimiento medio-avanzado de Seguridad Informática
- Demostrar conocimiento medio en Sistemas Windows y Linux (Desktop y Server)
- Conocer e interpretar a nivel medio-avanzado los registros o logs de seguridad
- Tener un conocimiento medio en seguridad de la información y normas ISO/IEC 27000.

3.6.3. Instalación de Máquina Virtual y Sistema Operativo del Servidor OSSIM

A continuación, se detalla los pasos para la instalación y configuración de la máquina virtual del Servidor OSSIM, realizado sobre una máquina con arquitectura de 64 bits. De acuerdo a lo indicado en la sección 3.6.1, en la Figura 16, se muestra la habilitación en el BIOS de la tecnología VT para permitir la virtualización de OSSIM de 64 bits.

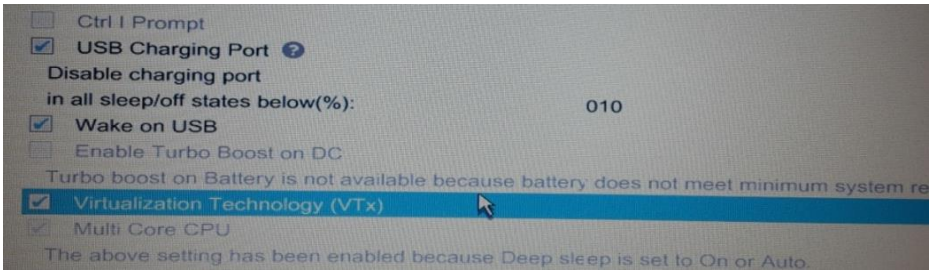


Figura 16 Habilitación de VT para servidor OSSIM

Una vez habilitada la opción, Virtual Box permitirá crear máquinas virtuales de 64bit. En las Figuras 17 a 31 se muestra la asignación de capacidades de hardware y despliegue de la máquina virtual del servidor OSSIM.

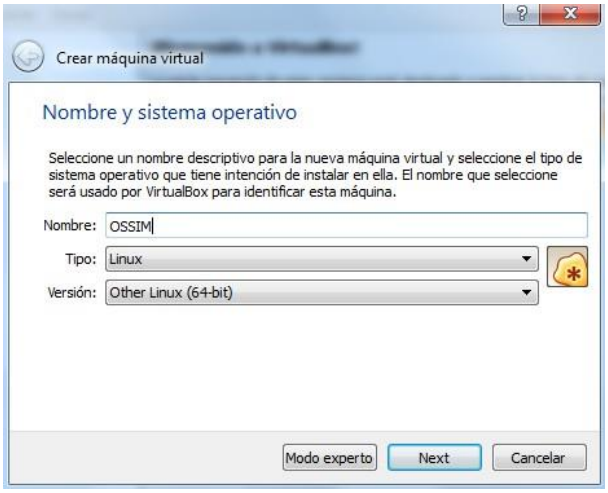


Figura 17 Máquina Virtual OSSIM - selección del sistema operativo

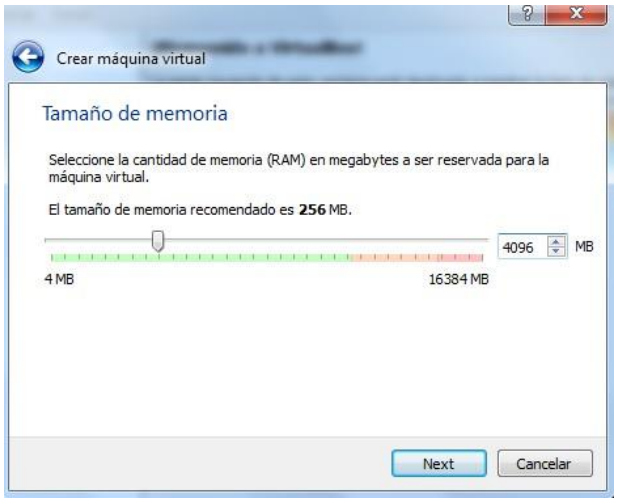


Figura 18 Máquina Virtual OSSIM – Selección de la memoria RAM

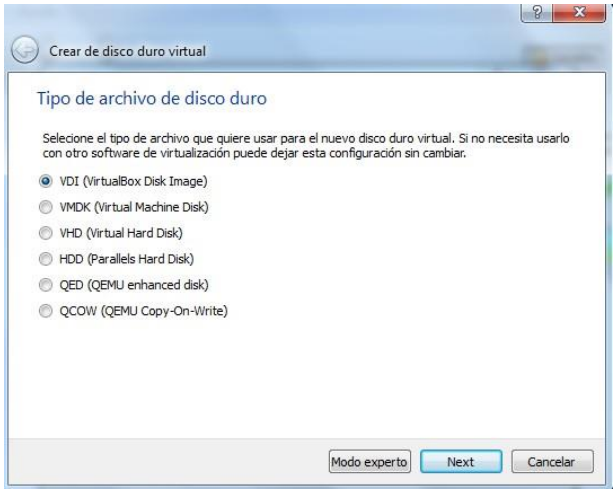


Figura 19 Máquina Virtual OSSIM – Selección del tipo de disco duro

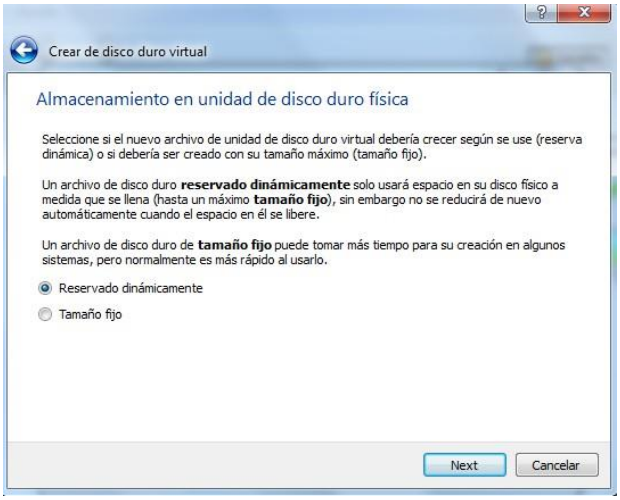


Figura 20 Máquina Virtual OSSIM – Tipo de almacenamiento dinámico

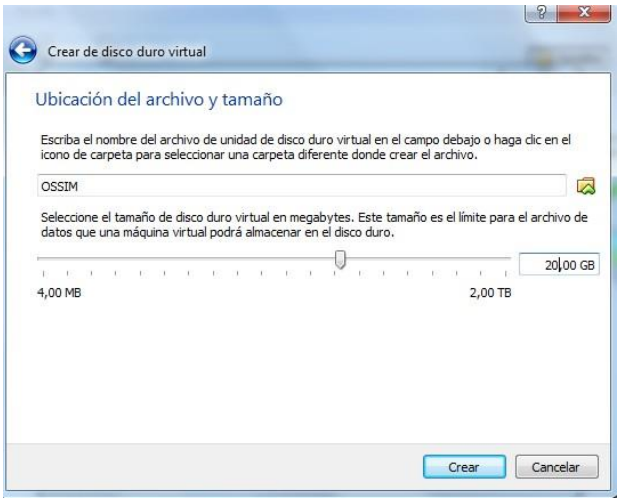


Figura 21 Máquina Virtual OSSIM – Capacidad del disco duro

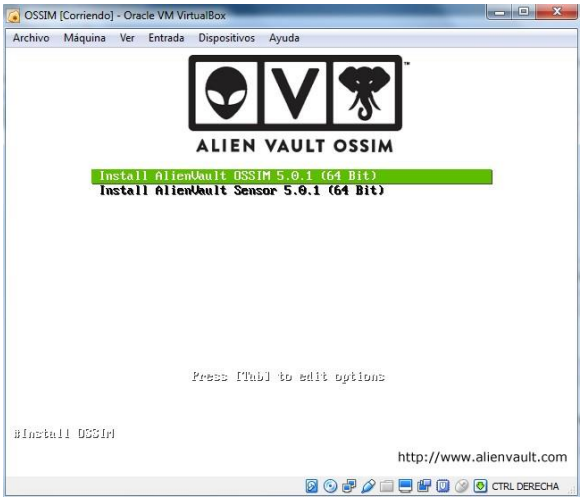


Figura 22 Máquina Virtual OSSIM – Pantalla inicial de instalación

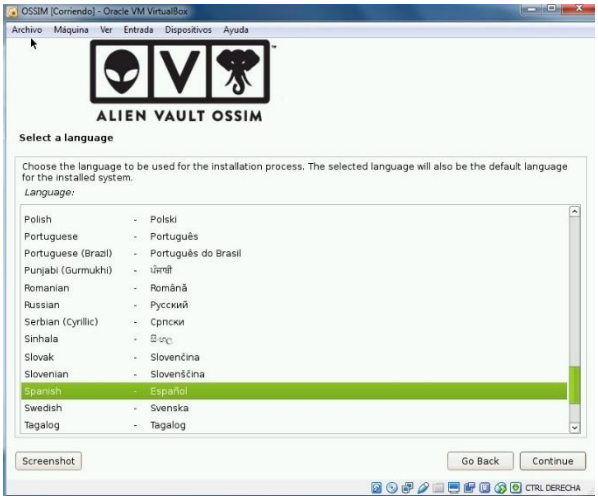


Figura 23 Máquina Virtual OSSIM – Selección del idioma

Figura 24 Máquina Virtual OSSIM - Selección de la ubicación

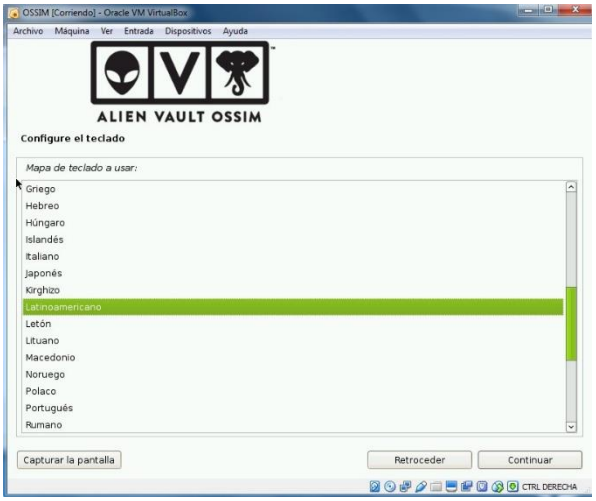


Figura 25 Máquina Virtual OSSIM - Configuración del teclado

Figura 26 Máquina Virtual OSSIM – Configuración de la IP

Figura 27 Máquina Virtual OSSIM – Configuración de la máscara de red

Figura 28 Máquina Virtual OSSIM - Configuración puerta de enlace

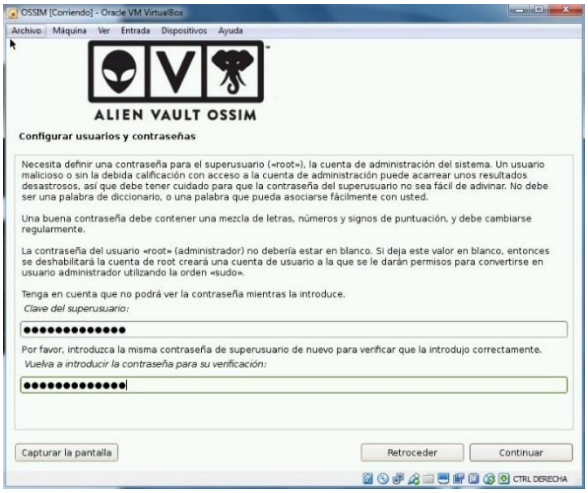


Figura 29 Máquina Virtual OSSIM - Establecimiento de la contraseña de súper usuario

Figura 30 Máquina Virtual OSSIM – Configuración de la zona horaria

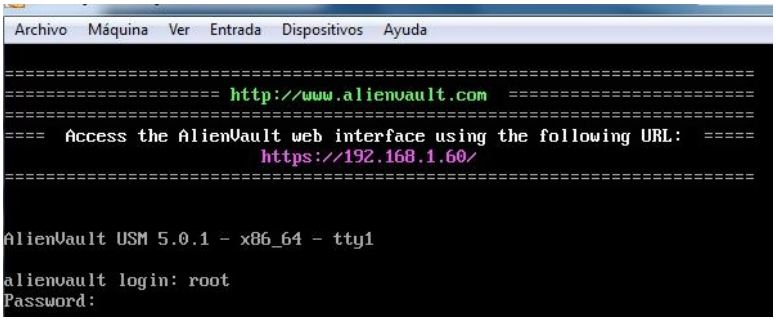


Figura 31 Máquina Virtual OSSIM – Pantalla de login al sistema

3.6.4. Configuración de Servidor OSSIM

En esta sección se detalla la configuración de los principales componentes de OSSIM, posterior a la instalación, se puede ingresar a la interfaz web con la siguiente dirección URL: https://192.168.100.60, donde nos solicitará el usuario y contraseña; la herramienta nos permite utilizar el asistente para realizar un descubrimiento y recolección de logs de los equipos a ser monitoreados.

Figura 32 OSSIM Asistente para el descubrimiento en la red

Como ejemplo se utilizó la opción de descubrimiento de equipos, posteriormente se podrá realizar la configuración y recolección de logs de acuerdo a las necesidades; luego del escaneo en la red interna se detectó a dos equipos en la red.

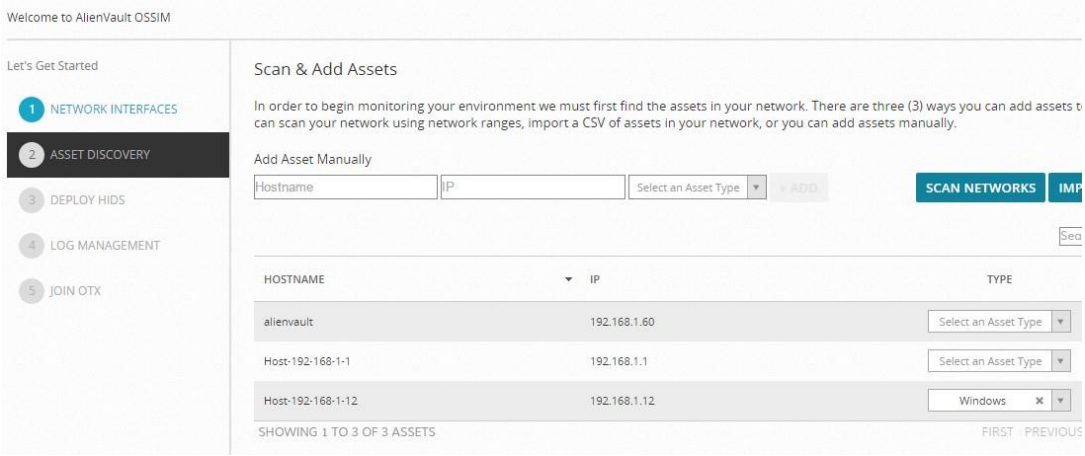


Figura 33 OSSIM – Escaneo y descubrimiento de equipos en red interna

Luego de realizar el descubrimiento como muestra la Figura 34, el sistema OSSIM refleja su pantalla principal que maneja cinco opciones principales Dashboard, Analisys, Enviroment, Reports y Configuration. En el *Dashboard*, se puede tener una visualización global del estado del sistema de gestión, el cual permite contar con un control general de los eventos, riesgos, análisis, despliegue, reportes, configuración, entre otras opciones, para una administración integral de la herramienta.

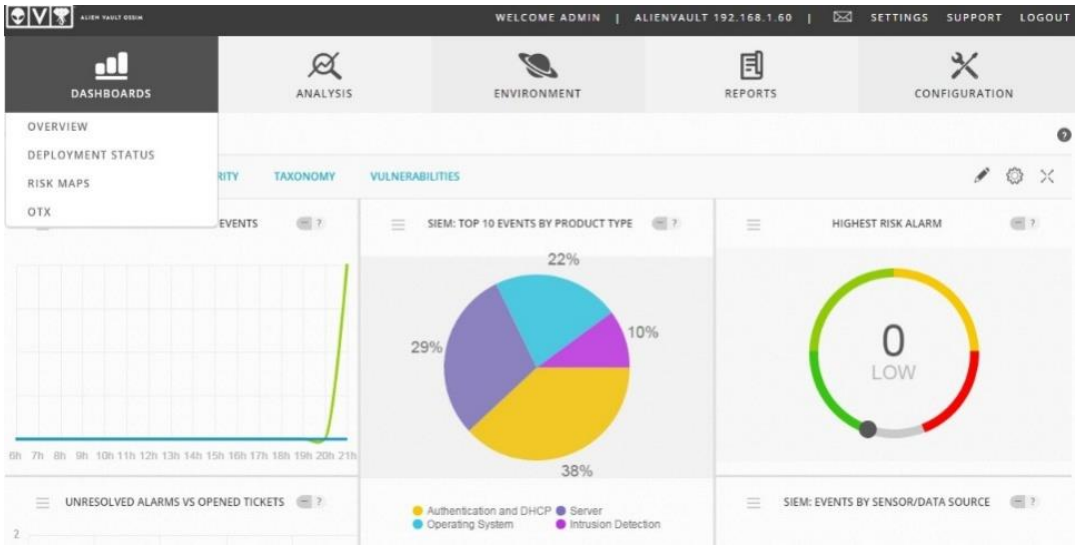


Figura 34 OSSIM – Dashboard del sistema de gestión de eventos

3.6.5. Instalación y Configuración de Fuentes de Eventos

Para realizar la configuración de las fuentes de eventos, registro o logs de seguridad, en primer lugar, se detallará los pasos de instalación de los servidores y clientes, es decir las máquinas virtuales. Posteriormente se detallarán los pasos para la recolección e integración de dichas fuentes con el servidor OSSIM.

3.6.5.1. Instalación y Configuración de Equipo Firewall

3.6.5.1.1. Instalación de Máquina Virtual y Sistema Operativo del Firewall

A continuación, en las Figuras 35 a 61 se detalla la instalación de la máquina virtual y el sistema operativo de la versión gratuita del Firewall Checkpoint versión R77.20.

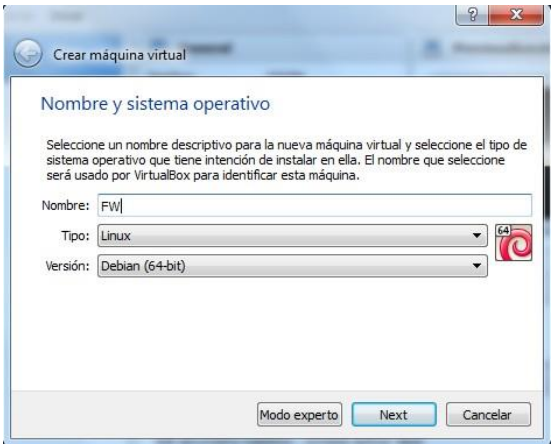


Figura 35 Máquina Virtual Firewall – selección del sistema operativo

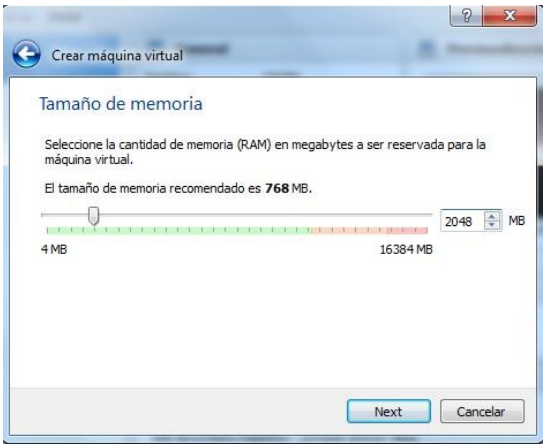


Figura 36 Máquina Virtual Firewall – Selección de la memoria RAM

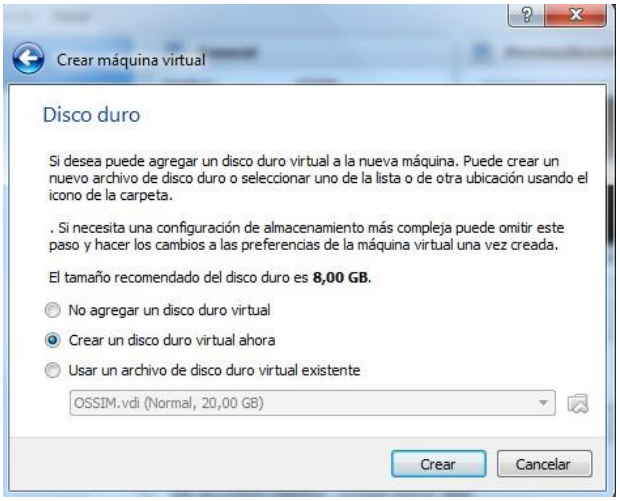


Figura 37 Máquina Virtual Firewall – Creación del disco virtual

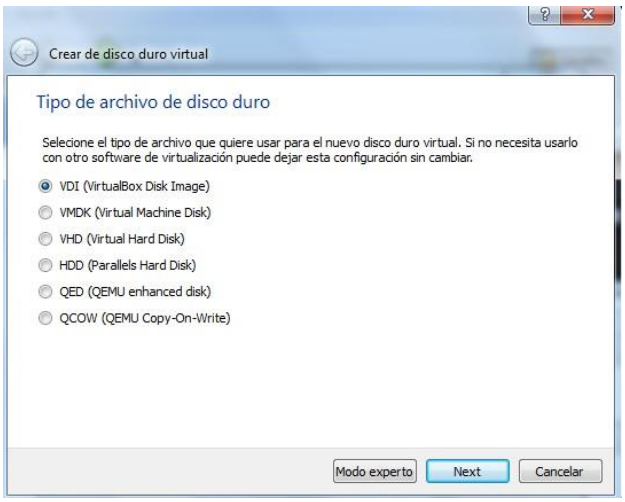


Figura 38 Máquina Virtual Firewall - Selección del tipo de disco duro

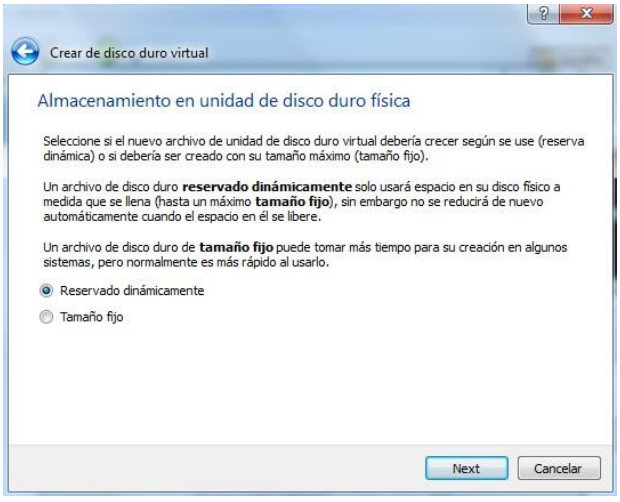


Figura 39 Máquina Virtual Firewall – Selección del tipo de disco duro

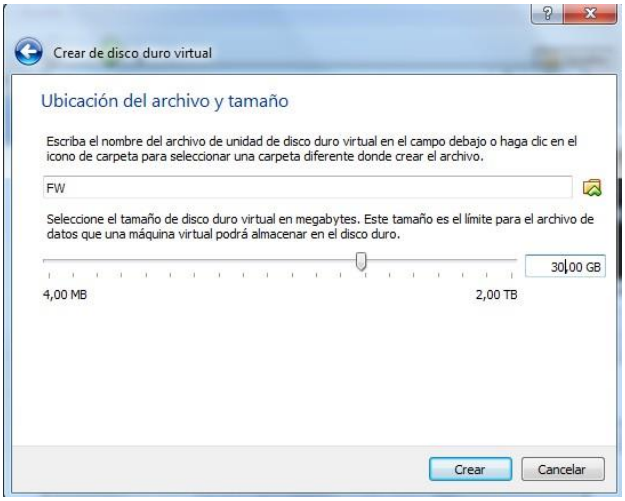


Figura 40 Máquina Virtual Firewall –Selección capacidad del disco duro

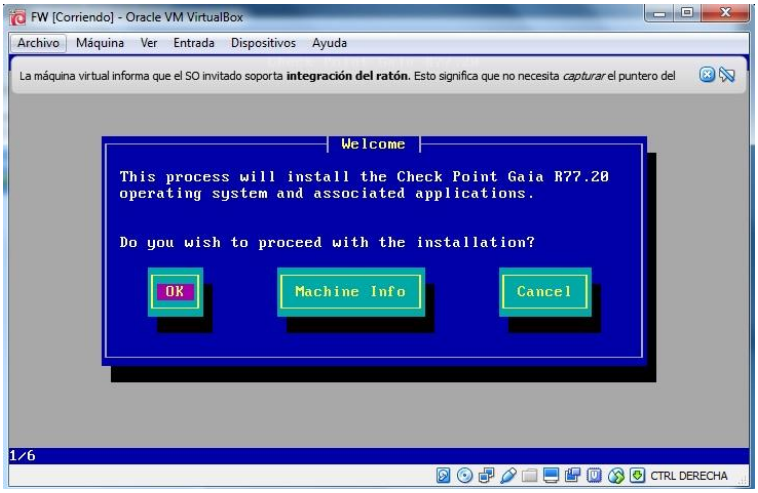


Figura 41 Máquina Virtual Firewall – Inicio de instalación de sistema

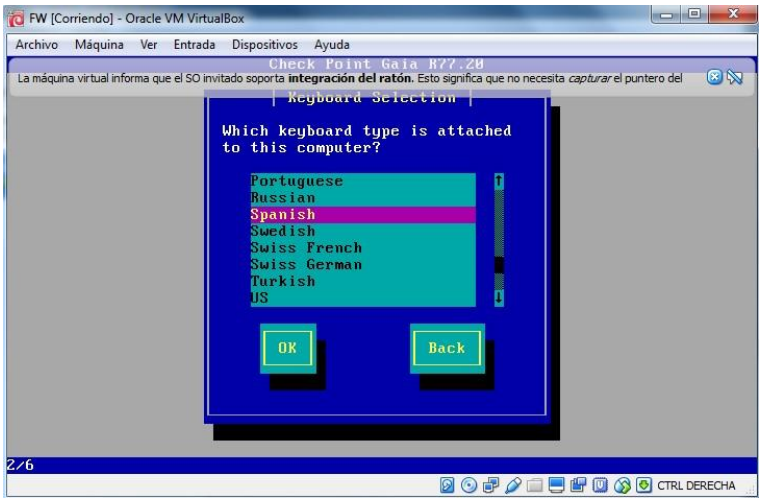


Figura 42 Máquina Virtual Firewall – Selección de idioma

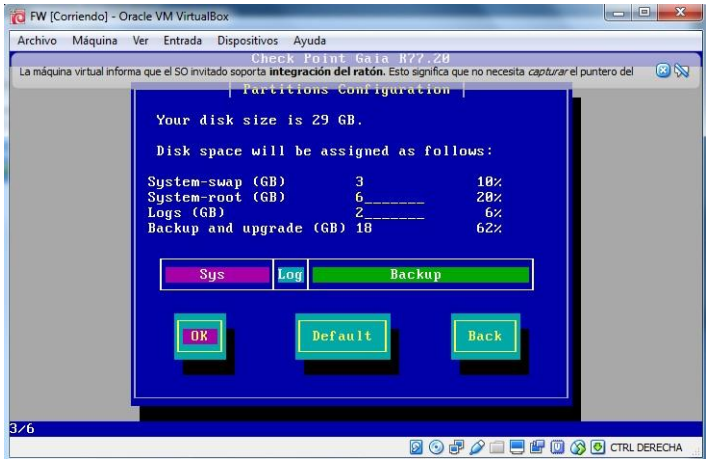


Figura 43 Máquina Virtual Firewall – Configuración de particiones automática generada por Checkpoint

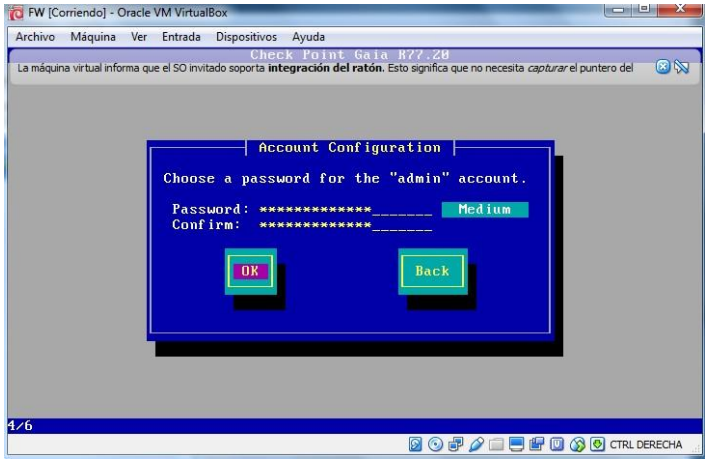


Figura 44 Máquina Virtual Firewall – Definición de clave para usuario administrador

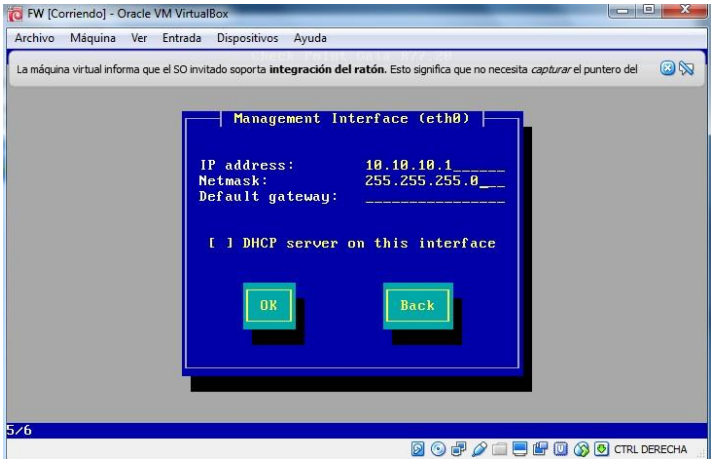


Figura 45 Máquina Virtual Firewall - Definición de Dirección IP para red de administración

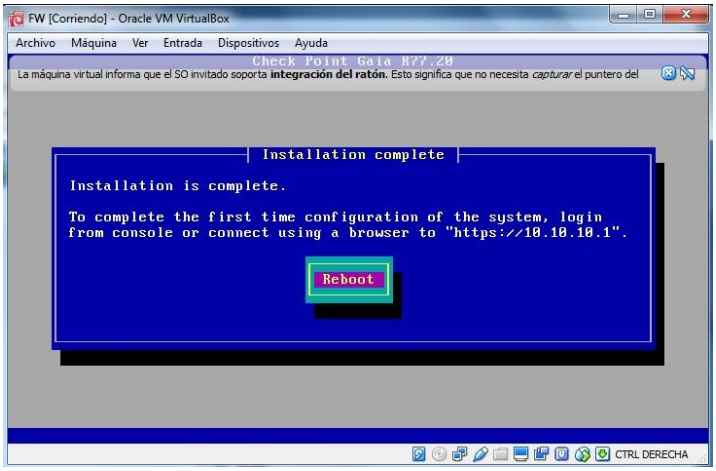


Figura 46 Máquina Virtual Firewall – Pantalla de Instalación completa

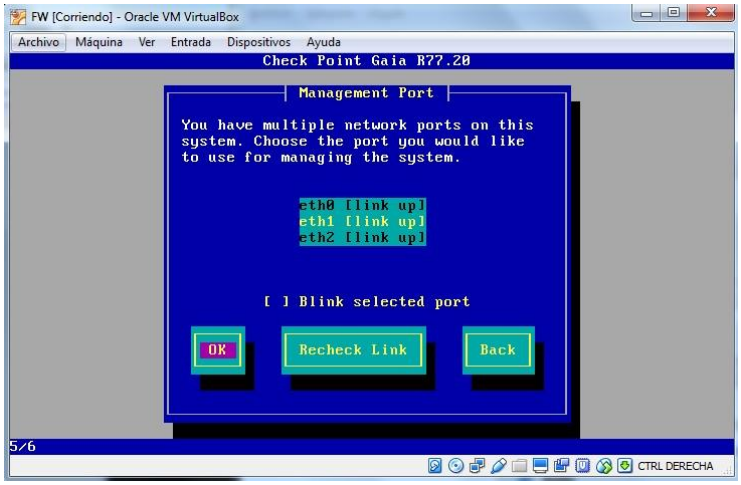


Figura 47 Máquina Virtual Firewall – Selección de interfaz de administración

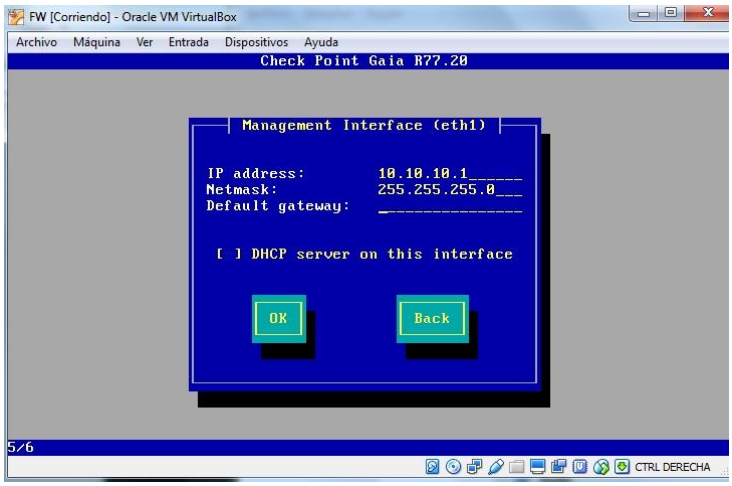


Figura 48 Máquina Virtual Firewall – Definición de interfaz Eth1 de administración

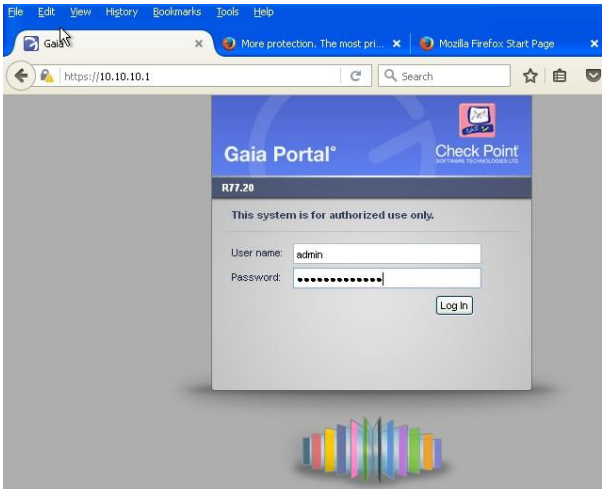


Figura 49 Máquina Virtual Firewall - Ingreso a Portal Gaia para administración web

Figura 50 Máquina Virtual Firewall – Pantalla de Inicio de administrador web

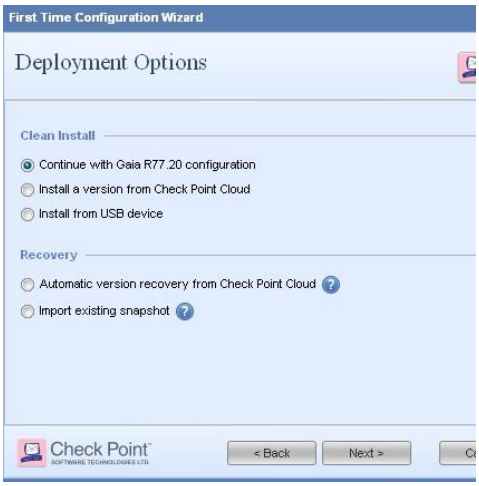


Figura 51 Máquina Virtual Firewall - Selección de administrador

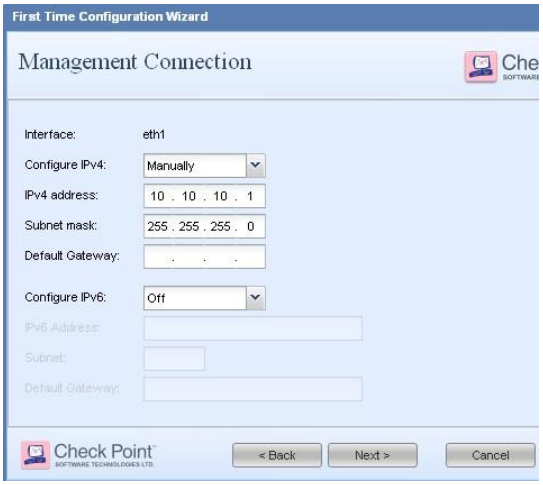


Figura 52 Máquina Virtual Firewall - Configuración de Dirección IP eth1

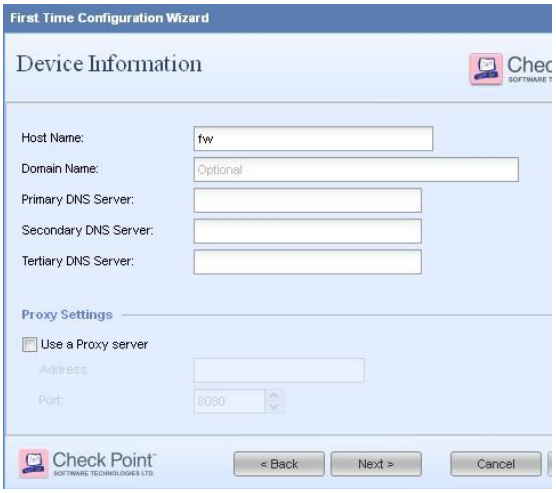


Figura 53 Máquina Virtual Firewall - Selección de nombre de equipo

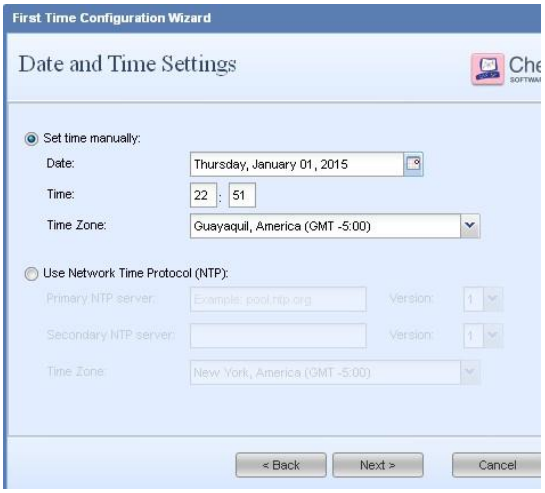


Figura 54 Máquina Virtual Firewall - Definición de Fecha

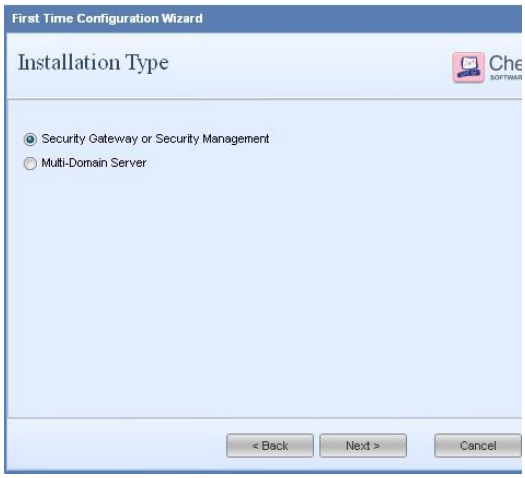


Figura 55 Máquina Virtual Firewall - Selección tipo de configuración

Figura 56 Máquina Virtual Firewall - Selección de productos del sistema firewall

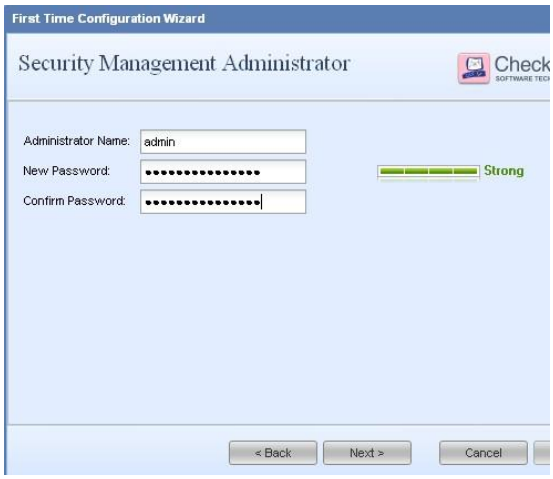


Figura 57 Máquina Virtual Firewall - Definición d Usuario y clave de administración

Figura 58 Máquina Virtual Firewall - Definición de dirección IP de equipo de administración

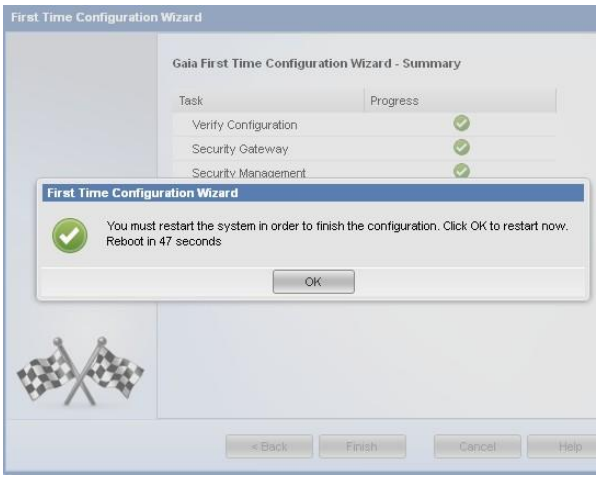


Figura 59 Máquina Virtual Firewall - Finalización de instalación - reinicio de sistema

Figura 60 Máquina Virtual Firewall - Ingreso a sistema de administración

Figura 61 Máquina Virtual Firewall - Pantalla de inicio de configuración

3.6.5.1.2. Integración Firewall – OSSIM

Posterior a la instalación de la máquina virtual del Firewall, se procederá a la configuración de envío de los eventos de seguridad del Firewall al Servidor OSSIM, mediante el protocolo Syslog que utiliza el puerto UDP 514.

- **Firewall:**

Primero se realizará la configuración de eventos en el Firewall, se ingresará desde línea de comando a modo Experto, para modificar el archivo de configuración */etc/syslog.conf*, como se muestra en las Figuras 62 a 67; para finalmente realizar un reinicio del servicio syslog.

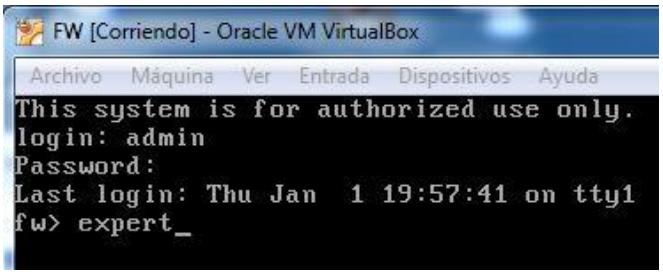


Figura 62 Ingreso a modo Experto Firewall

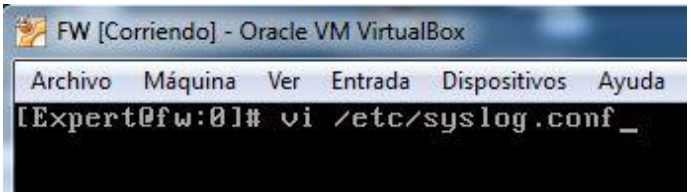


Figura 63 Ingreso al archivo syslog.conf

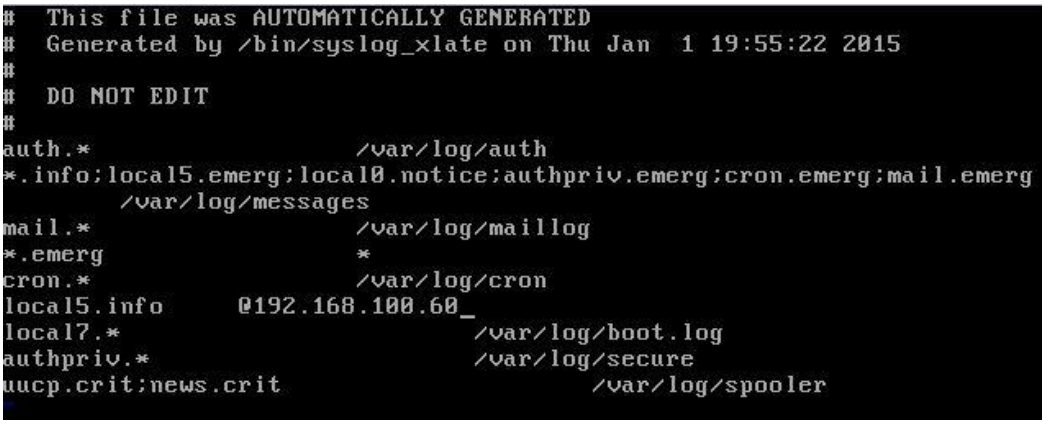


Figura 64 Modificación Archivo Syslog.conf

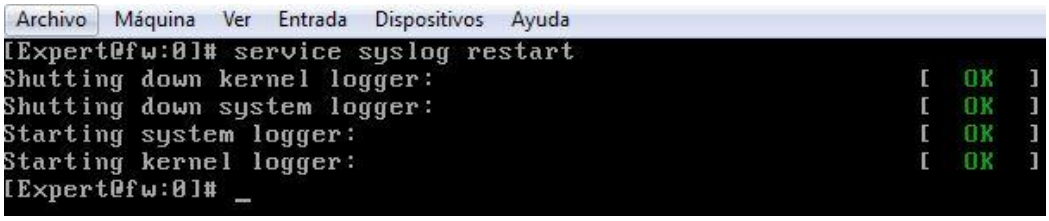


Figura 65 Reinicio de servicio syslog

Figura 66 Configuración del archivo /etc/rc.d/init.d/cpboot

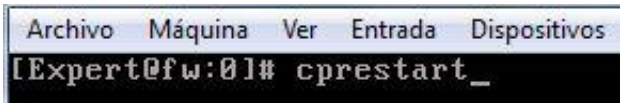


Figura 67 Reinicio de máquina virtual

- **OSSIM:**

Para lograr una integración y visualización de los syslog enviados por el Firewall se procederá a la configuración de recepción y almacenamiento de los eventos en el servidor OSSIM, como se muestra en las Figuras 68 a 73.

Figura 68 Ingreso a línea de comando de OSSIM

Figura 69 Configuración del archivo rsyslog.conf

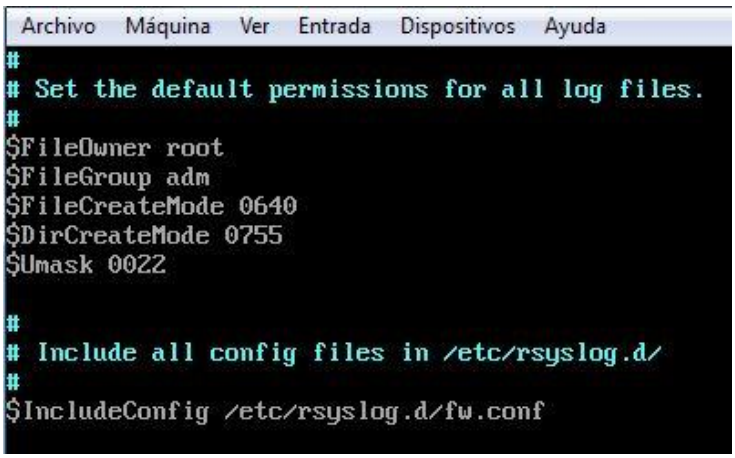


Figura 70 Agregación de archivo /etc/rsyslog.d/fw.conf

Figura 71 Actualización el archivo de configuración /etc/rsyslog.d/fw.conf

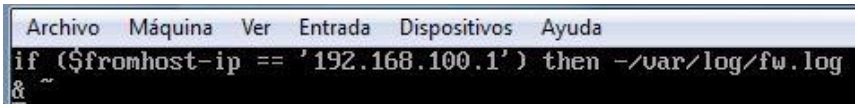


Figura 72 Definición de IP desde la cual se receptan los eventos (Firewall)

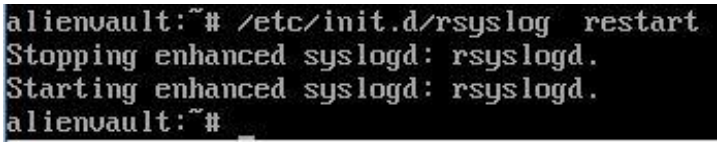


Figura 73 Reinicio del archivo rsyslog

Para comprobar que se están recibiendo los logs desde el firewall (IP 192.168.100.1) hacia el servidor OSSIM (192.168.100.60), se puede utilizar el comando tail como se muestra en la Figura 74:

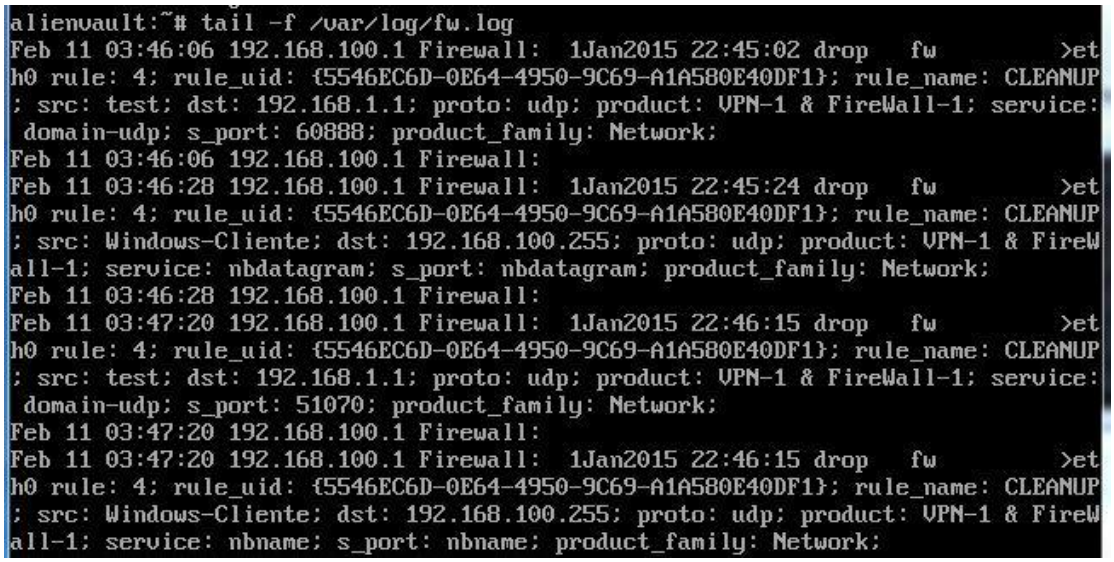


Figura 74 Verificación de recepción de logs

Adicionalmente para que exista conexión con el protocolo syslog entre el Firewall y el Servidor OSSIM, es importante establecer una regla en el firewall habilitando el puerto de destino UDP 514, por lo que desde la consola gráfica Gaia Checkpoint se habita la comunicación por el protocolo Syslog, como se muestra en la Figura 75:

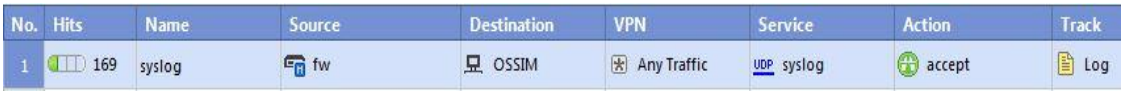


Figura 75 Creación de regla syslog para comunicación entre firewall y OSSIM

Luego de esto se debe configurar los archivos .cfg y .sql para el agente del equipo Firewall Checkpoint, como se muestra en las Figuras 76 a 87.

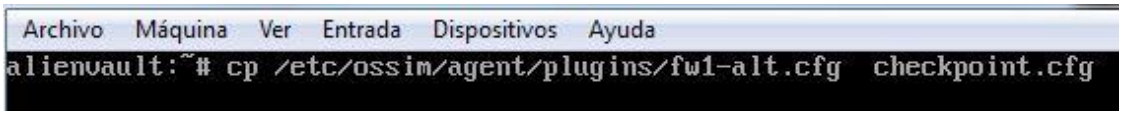


Figura 76 Copia del archivo de configuración fw1-alt.cfg para el equipo Checkpoint

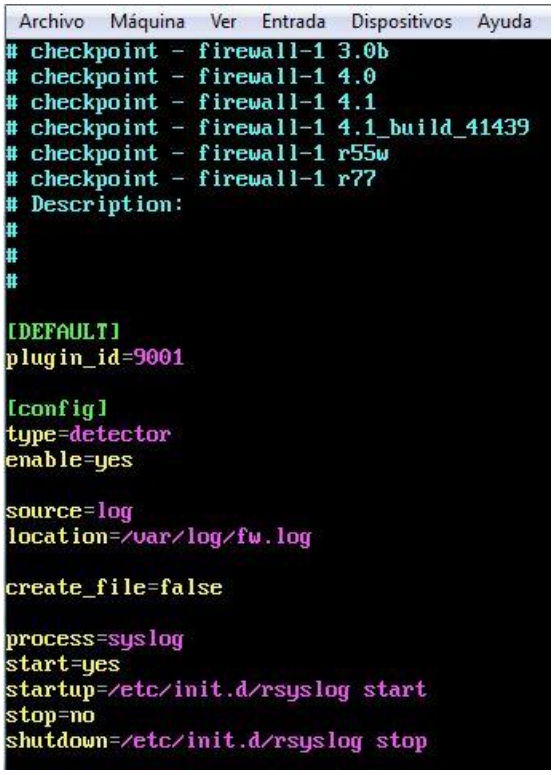


Figura 77 Modificación archivo checkpoint.cfg

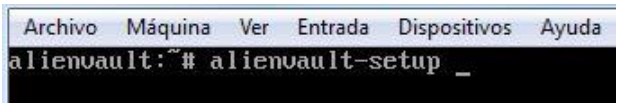


Figura 78 Activación del plugin checkpoint creado, mediante el comando: alienvault-setup

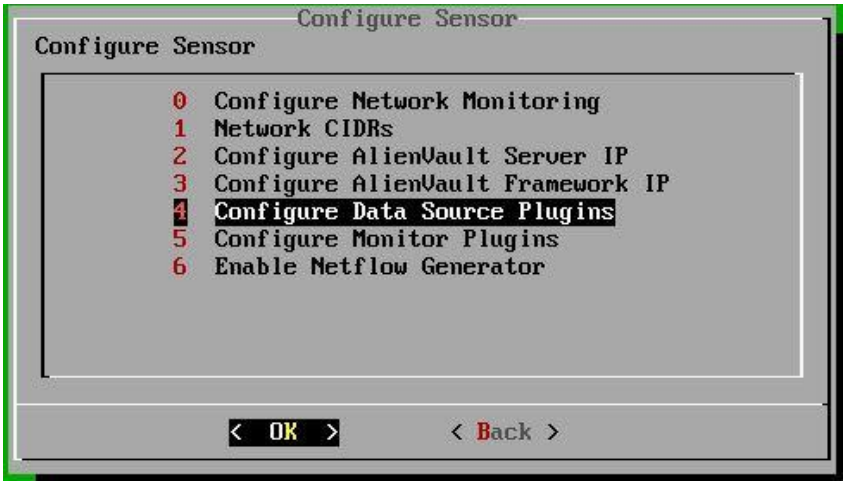


Figura 79 Configuración de Sensores OSSIM se activa el plugin para el Firewall

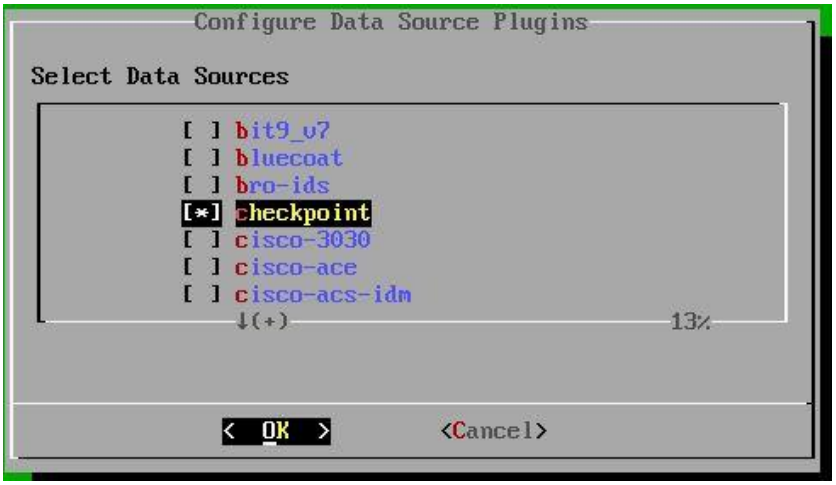


Figura 80 Selección del plugin Checkpoint

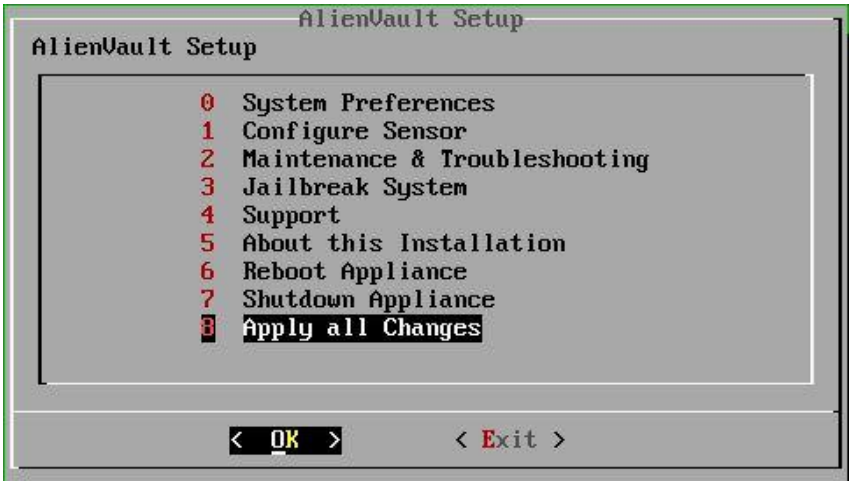


Figura 81 Aplicación de cambios

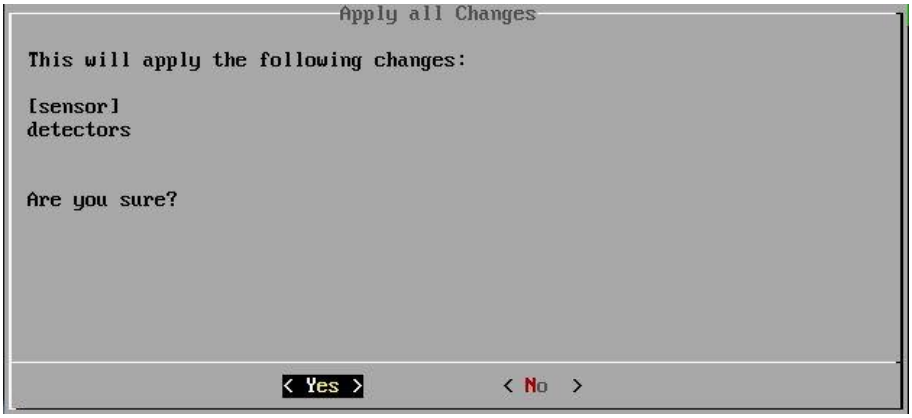


Figura 82 Confirmación de aplicación de cambios

```
alienvault:~# cp /usr/share/doc/ossim-mysql/contrib/plugins/fw1-alt.sql checkpo
nt.sql
```

Figura 83 Configuración de la base de datos, copiamos el plugin fw1-alt.sql

```
DELETE FROM plugin WHERE id = "9001";
DELETE FROM plugin_sid where plugin_id = "9001";

INSERT IGNORE INTO plugin (id, type, name, description) VALUES (9001, 1, 'chec
oint', 'Checkpoint R77');

INSERT IGNORE INTO plugin_sid (plugin_id, sid, category_id, class_id, name) VA
ES (9001, 1, NULL, NULL, 'checkpoint: drop');
INSERT IGNORE INTO plugin_sid (plugin_id, sid, category_id, class_id, name) VA
ES (9001, 2, NULL, NULL, 'checkpoint: authorize');
INSERT IGNORE INTO plugin_sid (plugin_id, sid, category_id, class_id, name) VA
ES (9001, 3, NULL, NULL, 'checkpoint: deauthorize');
INSERT IGNORE INTO plugin_sid (plugin_id, sid, category_id, class_id, name) VA
ES (9001, 4, NULL, NULL, 'checkpoint: reject');
INSERT IGNORE INTO plugin_sid (plugin_id, sid, category_id, class_id, name) VA
ES (9001, 5, NULL, NULL, 'checkpoint: ctl');
INSERT IGNORE INTO plugin_sid (plugin_id, sid, category_id, class_id, name) VA
ES (9001, 6, NULL, NULL, 'checkpoint: alert');
INSERT IGNORE INTO plugin_sid (plugin_id, sid, category_id, class_id, name) VA
ES (9001, 7, NULL, NULL, 'checkpoint: accept');
INSERT IGNORE INTO plugin_sid (plugin_id, sid, category_id, class_id, name) VA
ES (9001, 8, NULL, NULL, 'checkpoint: allow');
INSERT IGNORE INTO plugin_sid (plugin_id, sid, category_id, class_id, name) VA
ES (9001, 9, NULL, NULL, 'checkpoint: monitor');
INSERT IGNORE INTO plugin_sid (plugin_id, sid, category_id, class_id, name) VA
ES (9001, 10, NULL, NULL, 'checkpoint: encrypt');
INSERT IGNORE INTO plugin_sid (plugin_id, sid, category_id, class_id, name) VA
ES (9001, 11, NULL, NULL, 'checkpoint: decrypt');
@
<sim-mysql/contrib/plugins/checkpoint.sql" [noeol] 19L, 2009C 1,1           To
```

Figura 84 Colocación de ID definido para plugin Checkpoint '9001'

```
alienvault:/usr/share/doc/ossim-mysql/contrib/plugins# ossim-db <checkpoint.
```

Figura 85 Ingreso a la base de datos

```
alienvault:/usr/share/doc/ossim-mysql/contrib/plugins# ossim-db
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 1705
Server version: 5.6.23-72.1 Percona Server (GPL), Release 72.1, Revision 0503478

Copyright (c) 2009-2015 Percona LLC and/or its affiliates
Copyright (c) 2000, 2015, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> select * from plugin where id = 9001;
+------------------+------+------+------------+-----------------+--------------+-
--------+
| ctx              | id   | type | name       | description     | product_type |
vendor |
+------------------+------+------+------------+-----------------+--------------+-
--------+
|                  | 9001 |    1 | checkpoint | Checkpoint R77 |            0 |
NULL   |
+------------------+------+------+------------+-----------------+--------------+-
--------+
1 row in set (0.00 sec)

mysql>
```

Figura 86 Consulta a base de datos

```
rchivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
alienvault:/usr/share/doc/ossim-mysql/contrib/plugins# alienvault-reconfig
```

Figura 87 Reconfiguración de OSSIM

Luego de la configuración de transmisión de logs, se realizó una prueba para la verificación de visualización de eventos, para lo que se creó una regla que permita el tráfico icmp (ping), desde el cliente "Windows-Cliente" a la interfaz del Firewall:

Figura 88 Ingreso web a servidor OSSIM

52	Prueba	Windows-Cliente OSSIM	fw	Any Traffic	icmp-requests	accept	Log

Figura 89 Creación de regla en Firewall

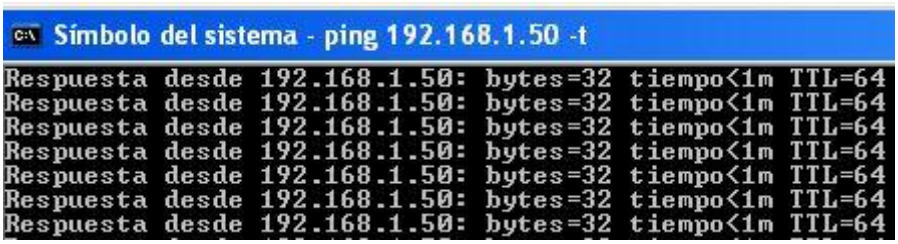


Figura 90 Envío de ping desde Windows-Cliente" a la ip 192.168.1.50 de la interfaz eth2 Firewall

EVENT NAME	RISK	GENERATOR	SENSOR	SOURCE IP
checkpoint: accept	0	checkpoint	alienvault	0.0.0.0:514
checkpoint: accept	0	checkpoint	alienvault	Windows-Cliente
checkpoint: accept	0	checkpoint	alienvault	Windows-Cliente

Figura 91 Verificación de recepción de los logs en la sección Análisis -> SIEM -> Real Time

EVENT DETAIL

NORMALIZED EVENT	DATE		ALIENVAULT SENSOR	DEVICE IP	INTERFACE
	2015-01-01 21:50:32 GMT-5:00		alienvault [192.168.100.60]	192.168.100.60	eth0
	TRIGGERED SIGNATURE		EVENT TYPE ID	CATEGORY	SUB-CATEGORY
	checkpoint: accept		7		
	DATA SOURCE NAME		PRODUCT TYPE		DATA SOURCE ID
	checkpoint		Unknown type		9001
	SOURCE ADDRESS	SOURCE PORT	DESTINATION ADDRESS	DESTINATION PORT	PROTOCOL
	Windows-Cliente	0	0.0.0.0	0	ICMP

Figura 92 Detalle de logs almacenados

3.6.5.2. Instalación y Configuración del Servidor Windows

3.6.5.2.1. Instalación de Máquina Virtual y Sistema Operativo de Windows Server 2008

En las Figuras 93 a 103 se muestra el despliegue de la máquina virtual Windows Server y la configuración del sistema operativo.

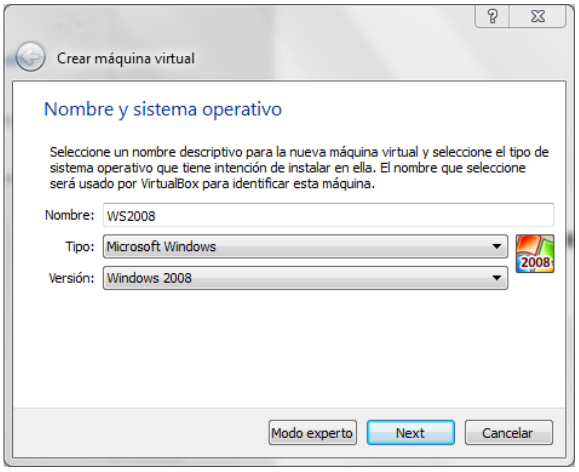


Figura 93 Máquina Virtual Windows Server 2008 – Selección del sistema operativo

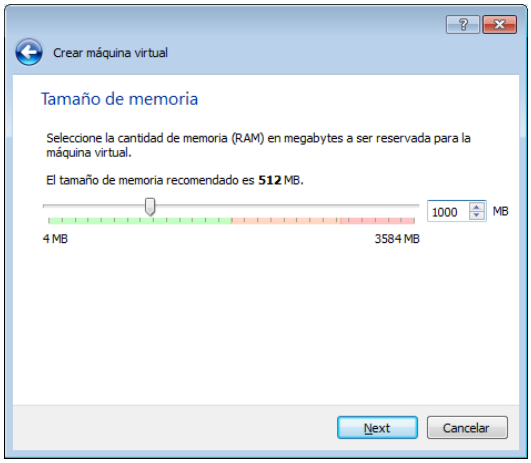


Figura 94 Máquina Virtual Windows Server 2008 – Selección de memoria RAM

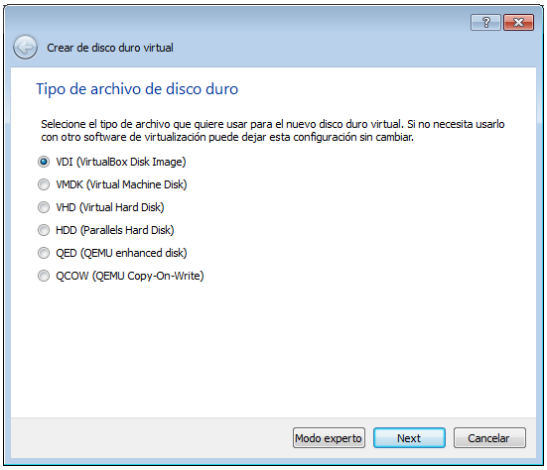


Figura 95 Máquina Virtual Windows Server 2008 – Selección del tipo de disco duro

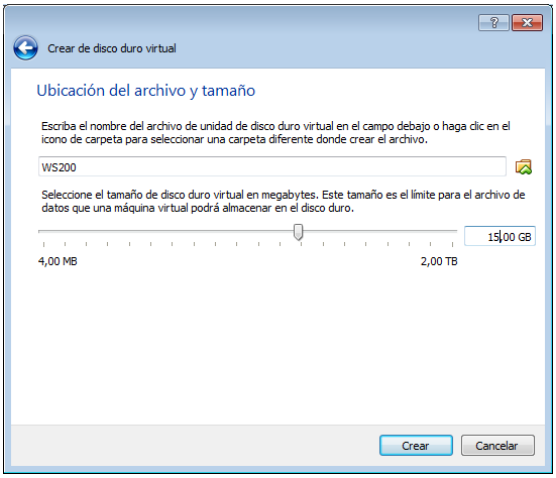


Figura 96 Máquina Virtual Windows Server 2008 – Selección espacio en disco duro

Figura 97 Máquina Virtual Windows Server 2008 – Selección de Idioma, Horario y Teclado

Figura 98 Máquina Virtual Windows Server 2008 – Inicio de Instalación

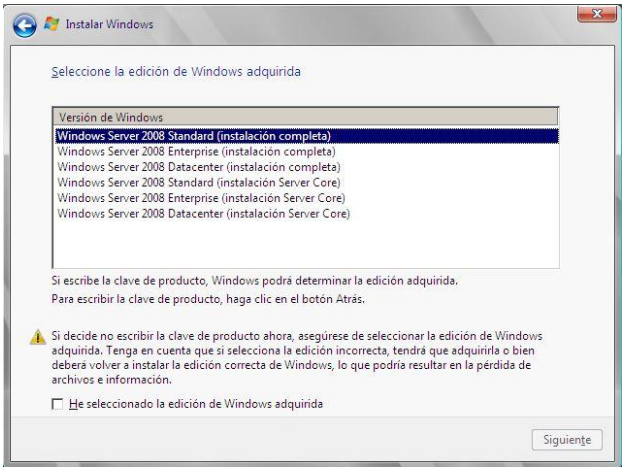


Figura 99 Máquina Virtual Windows Server 2008 – Selección de Versión de sistema operativo

Figura 100 Máquina Virtual Windows Server 2008 – Aceptación de términos de Licencia

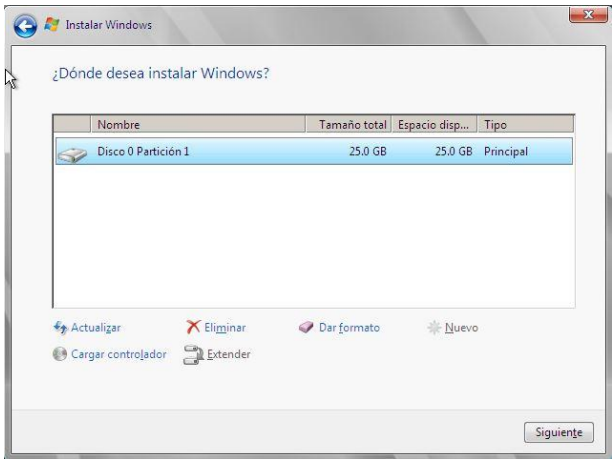


Figura 101 Máquina Virtual Windows Server 2008 – Selección de disco para instalación de sistema operativo

Figura 102 Máquina Virtual Windows Server 2008 – Proceso de instalación

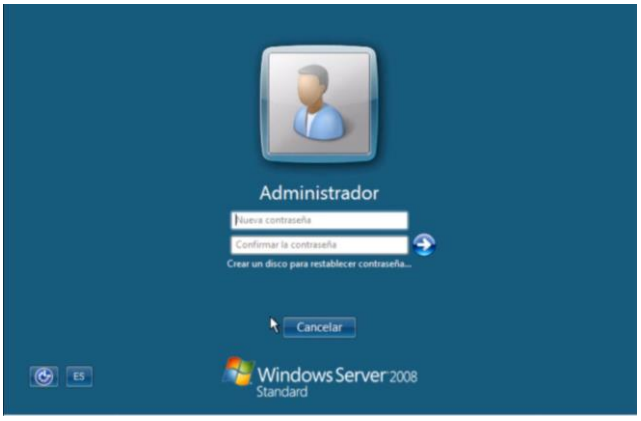


Figura 103 Máquina Virtual Windows Server 2008 – Instalación Finalizada - Inicio de Sesión

3.6.5.2.2. Configuración Controlador de Dominio Active Directory Windows Server 2008

A continuación, en la Figuras 104 a 117 se describe brevemente la configuración del Controlador de Dominio uno de los servicios sobre los cuales se realizará el monitoreo.

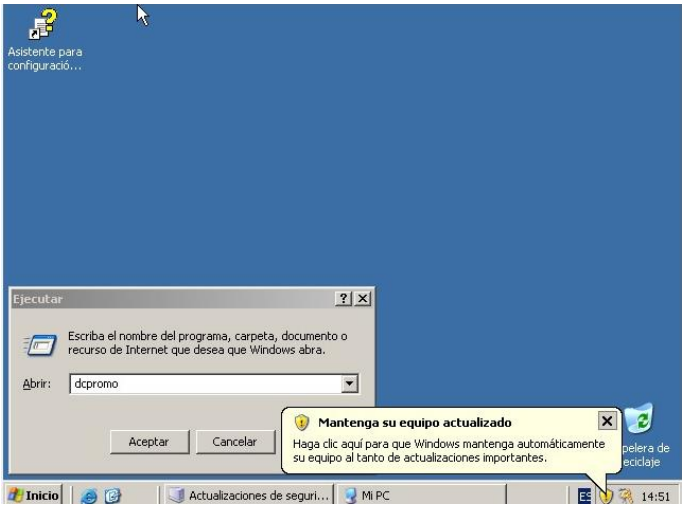


Figura 104 Windows Server 2008 – Promoción del Controlador de Dominio

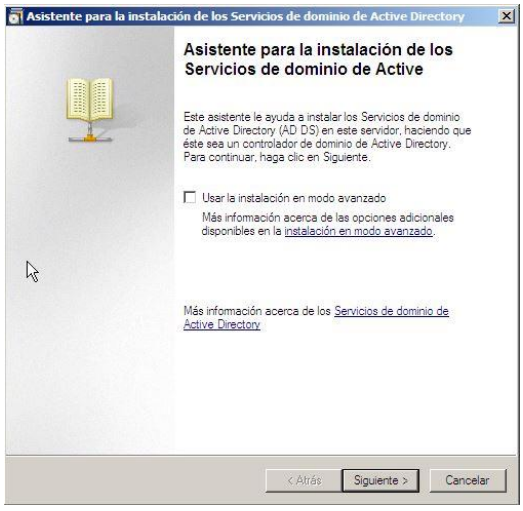


Figura 105 Windows Server 2008 – Configuración de Active Directory

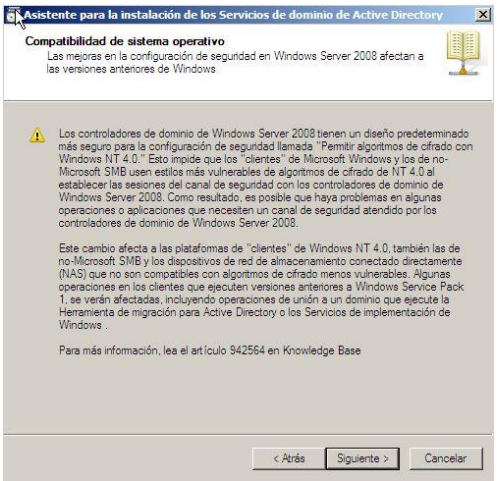


Figura 106 Windows Server 2008 – Creación del controlador de dominio

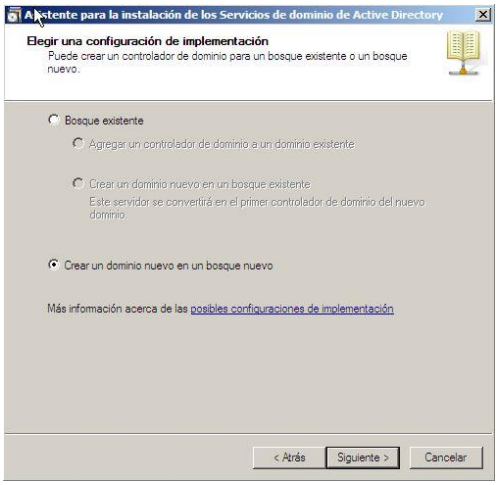


Figura 107 Windows Server 2008 – Nuevo Dominio

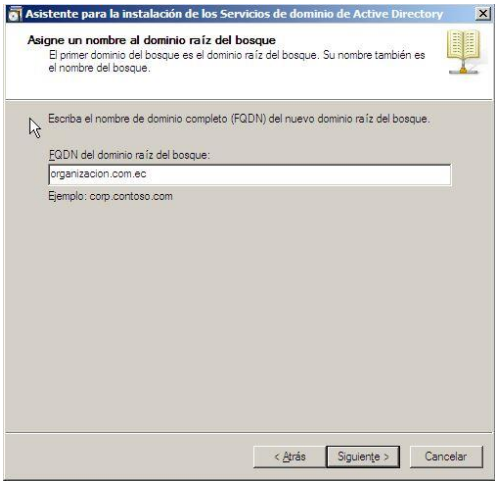


Figura 108 Windows Server 2008 – Nombre del Dominio

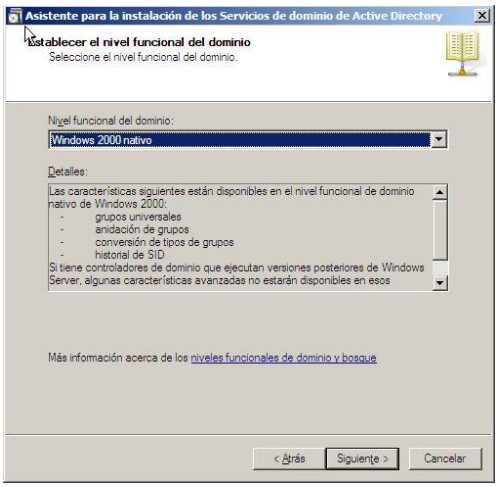


Figura 109 Windows Server 2008 – Selección de Dominio

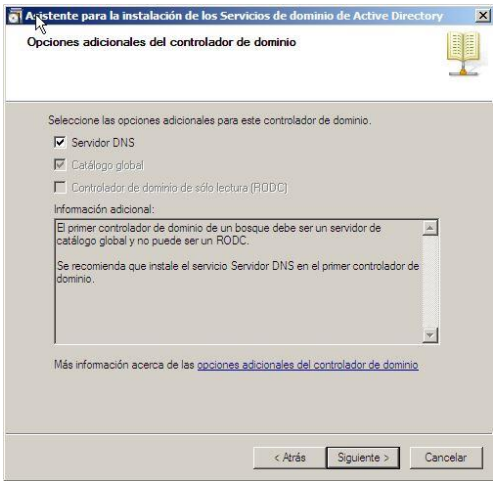


Figura 110 Windows Server 2008 – Selección de Servidor DNS

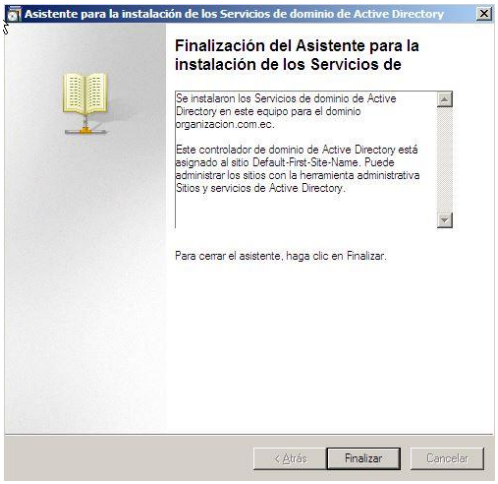


Figura 111 Windows Server 2008 – Instalación de Active Directory Finalizada

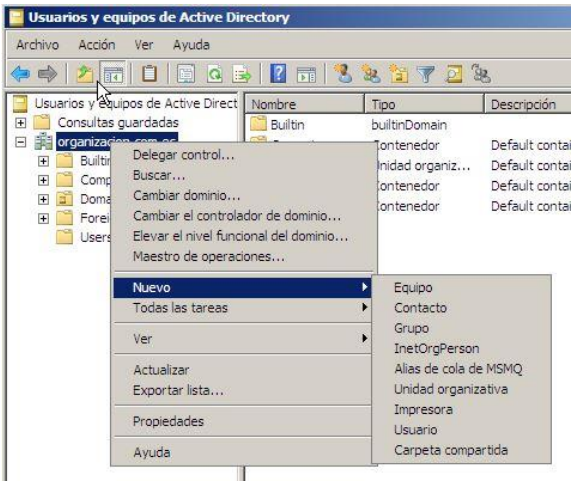


Figura 112 Windows Server 2008 – Creación de Nueva Unidad Organizativa

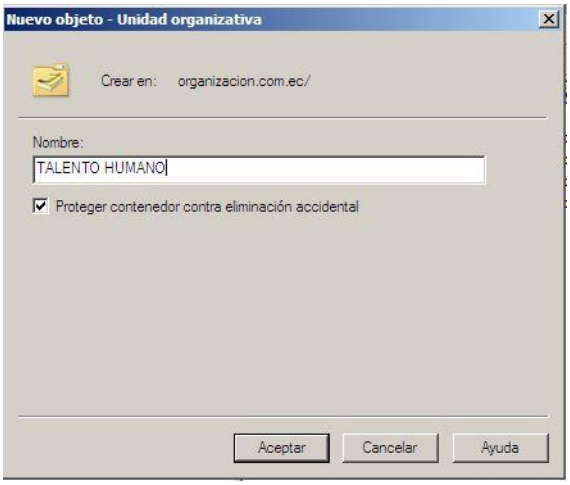


Figura 113 Windows Server 2008 – Nombre de Objeto

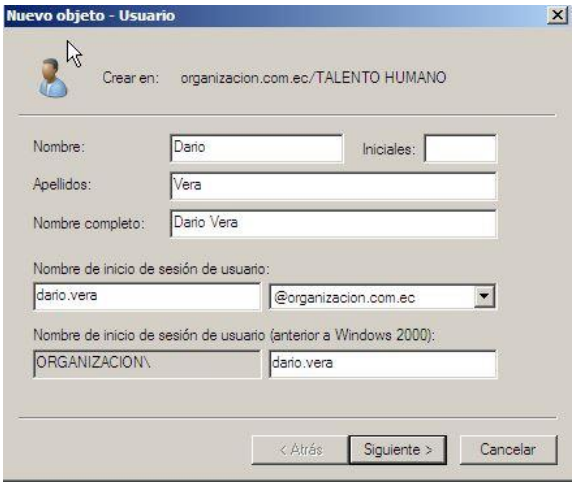


Figura 114 Windows Server 2008 – Creación de Nuevo Usuario

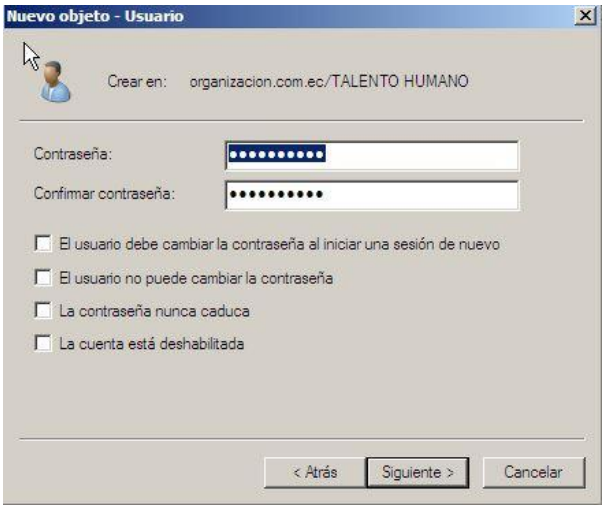


Figura 115 Windows Server 2008 – Asignación de Contraseña

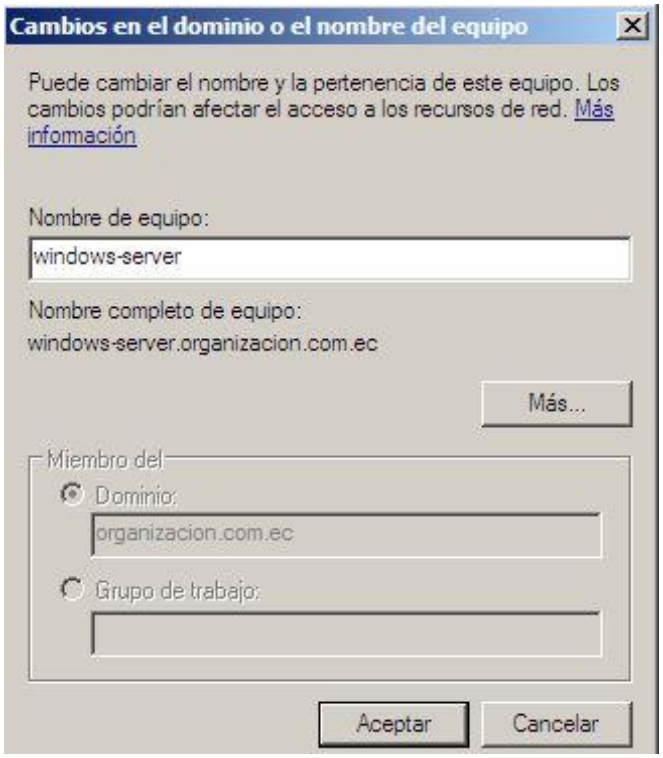


Figura 116 Windows Server 2008 – Selección Nombre del Equipo

Figura 117 Windows Server 2008 – Inicio de Sesión

3.6.5.2.3. Integración Windows Server 2008 - OSSIM

Posterior a la instalación y configuración del Controlador de Dominio, se procederá a la configuración de envío de los eventos de seguridad del Windows Server 2008 al Servidor OSSIM, a través del Agente OSSEC.

- **Windows Server 2008:**

En el servidor Windows 2008 se realiza la instalación del agente OSSEC, este agente se encarga de recolectar y enviar los registros o logs al servidor OSSIM a través de su dirección IP, en las Figuras 118 a 120 se muestra la instalación del agente como un programa común:

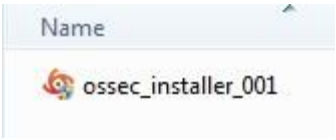


Figura 118 Agente a ser instalado en el Servidor Windows.

Figura 119 Configuración del agente hacia servidor OSSIM

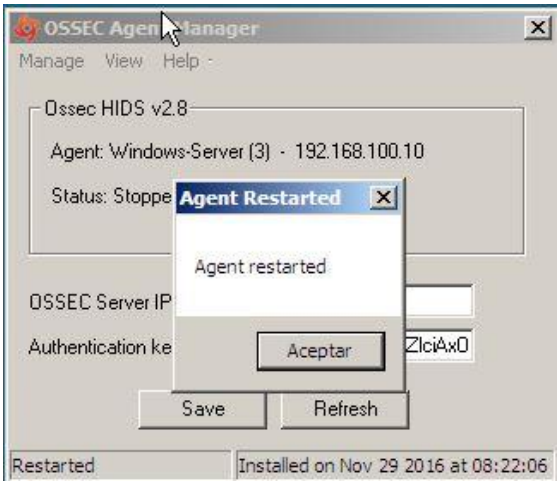


Figura 120 Inicio de Agente OSSEC

- **OSSIM:**

Para finalizar la integración del servidor Windows Server 2008 con OSSIM, se crea un nuevo agente dentro del módulo “Enviroment”->“Detection. El status del agente cambiará al activar el agente en la sección “Actions”. En las Figura 121 se muestra el agente activado.

Figura 121 Creación agente Windows Server y activación

Para verificar el correcto funcionamiento del agente OSSEC con el servidor Windows Server 2008, se reinició la sesión del servidor Windows, en la Figura 122 se visualiza los resultados.

EVENT NAME	RISK	GENERATOR	SENSOR	SOURCE IP
ossec: Windows Logon Success.	0	ossec-authentication_success	alienvault	Windows-Server
ossec: Windows Logon Success.	0	ossec-authentication_success	alienvault	Windows-Server

Figura 122 Recolección en tiempo real de logs Agente Windows Server

3.6.5.3. Instalación y Configuración Servidor Linux

3.6.5.3.1. Instalación de Máquina Virtual y Sistema Operativo Ubuntu Server

En las Figuras 123 a 133 se muestra el despliegue de la máquina virtual Ubuntu Server y la configuración del sistema operativo.

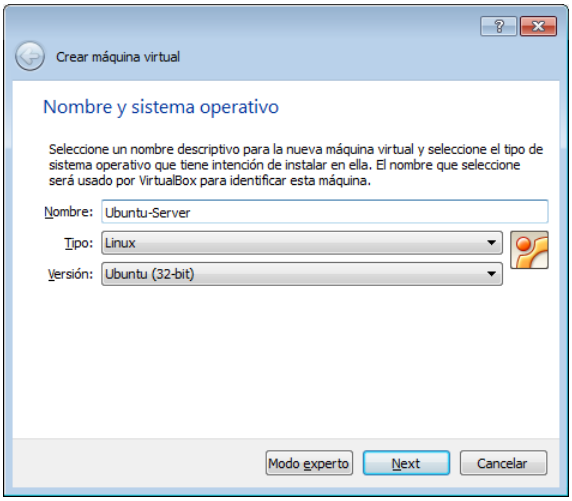


Figura 123 Máquina Virtual Ubuntu Server- Selección del sistema operativo

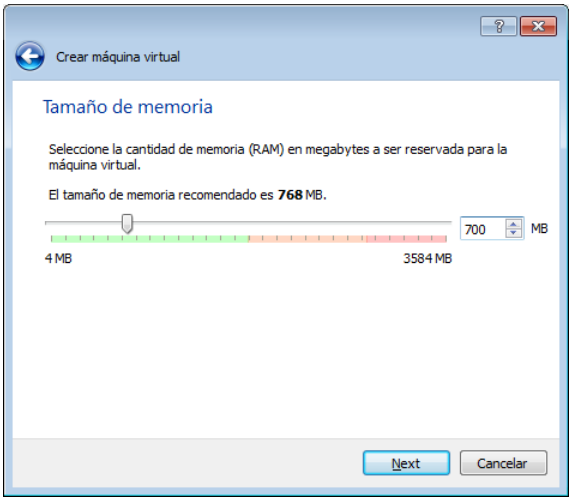


Figura 124 Máquina Virtual Ubuntu Server- Selección de la memoria RAM

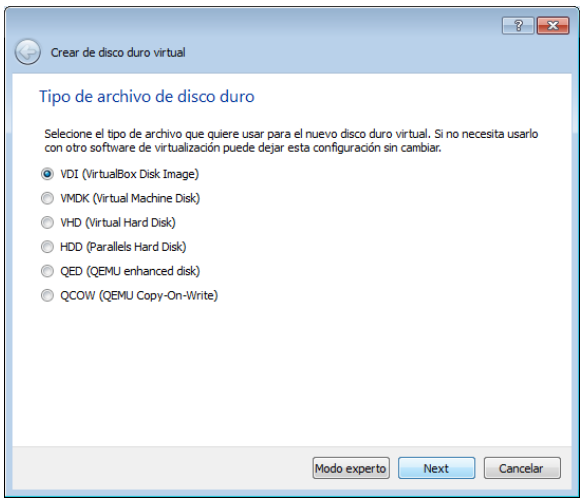


Figura 125 Máquina Virtual Ubuntu Server- Tipo de disco duro

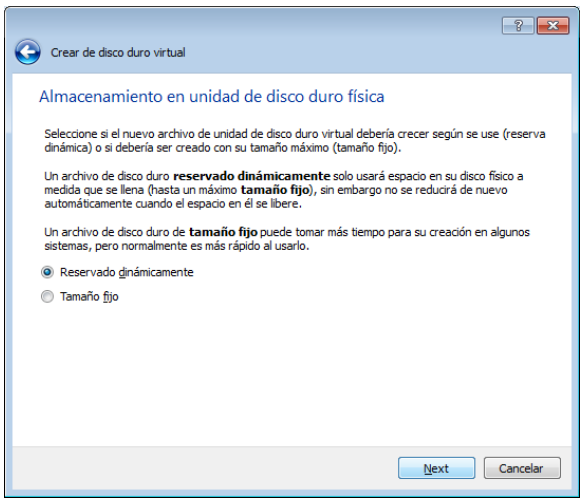


Figura 126 Máquina Virtual Ubuntu Server- Disco duro dinámico

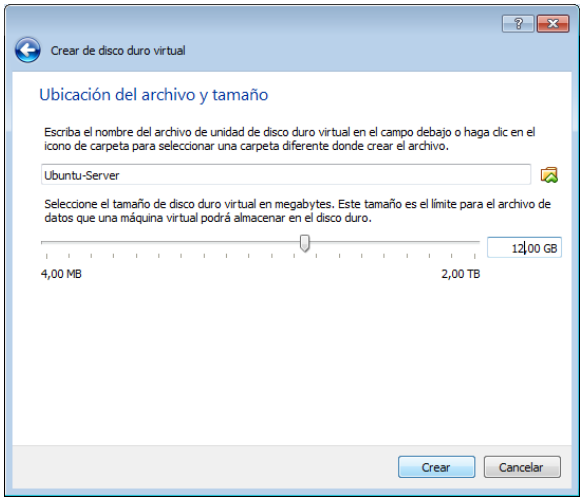


Figura 127 Máquina Virtual Ubuntu Server- Tamaño del disco duro

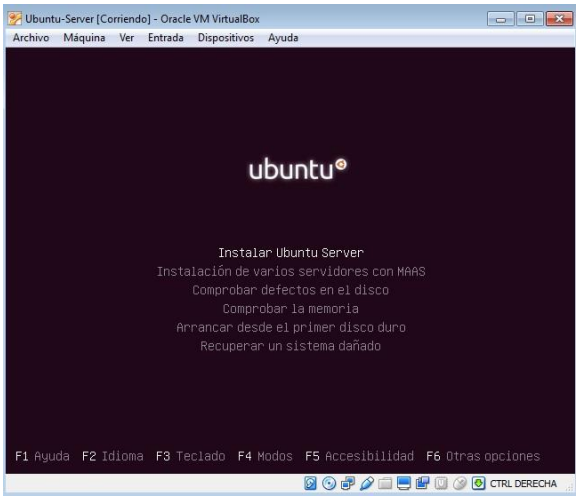


Figura 128 Máquina Virtual Ubuntu Server- Pantalla de inicio de instalación

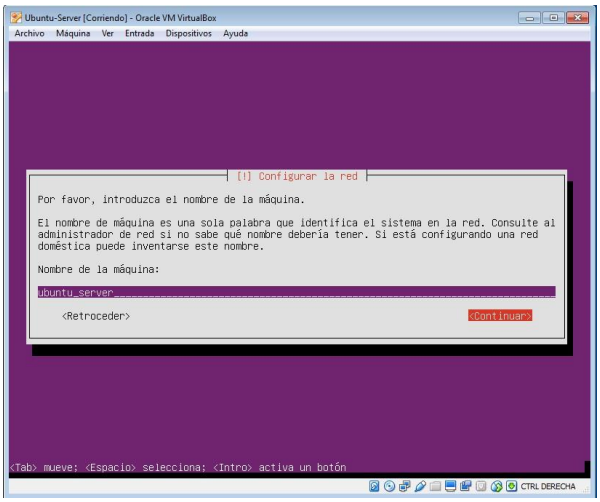


Figura 129 Máquina Virtual Ubuntu Server- Configuración de la red

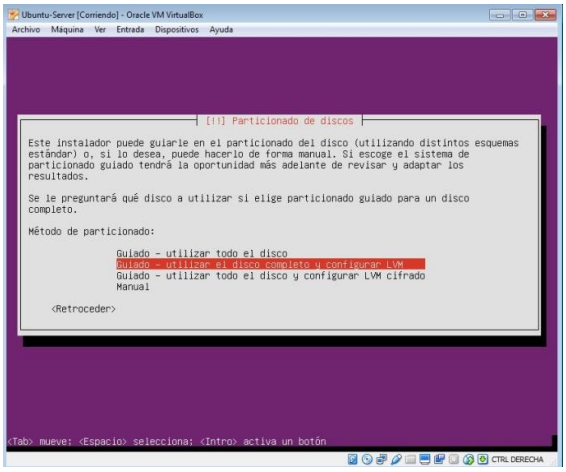


Figura 130 Máquina Virtual Ubuntu Server- Configuración de partición de discos

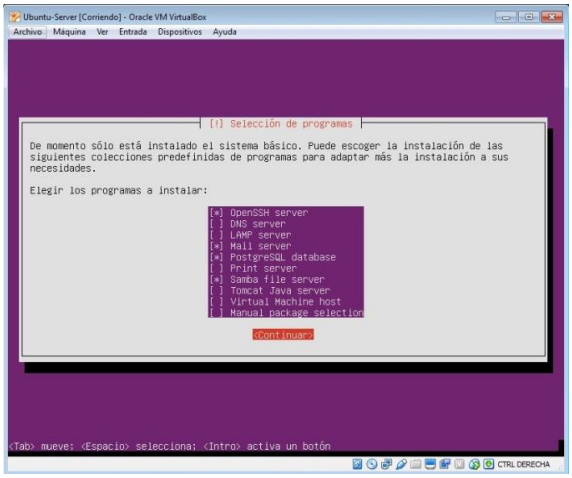


Figura 131 Máquina Virtual Ubuntu Server- Selección de programas predefinidas

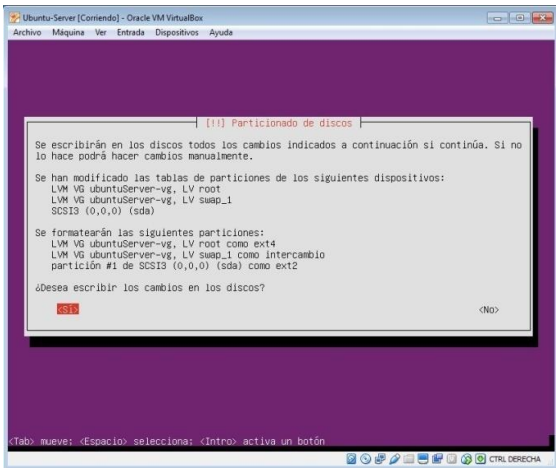


Figura 132 Máquina Virtual Ubuntu Server- Particionado del disco

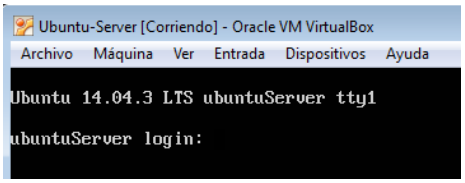


Figura 133 Máquina Virtual Ubuntu Server- Pantalla inicial de login

3.6.5.3.2. Instalación y configuración Servidor Base de Datos MySQL

Previo a la instalación del servidor de Base de Datos MySql, es necesario realizar una actualización de los paquetes del sistema operativo y de la versión del kernel, como se indica en las Figuras 134 y 135.

Figura 134 Ubuntu Server - Actualización de los paquetes de software

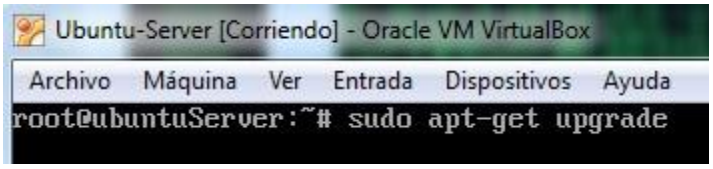


Figura 135 Ubuntu Server - Actualización del kernel

Posterior a la actualización del software, se iniciará la instalación del paquete MySQL-Server y se definirá la contraseña del usuario root, como se muestra en las Figuras 136 y 137. Con el fin de facilitar la creación y administración de la base de datos, se instalará el paquete phpmyadmin como indican la Figuras 136 a 140.

Figura 136 Ubuntu Server - Instalación del paquete MySQL

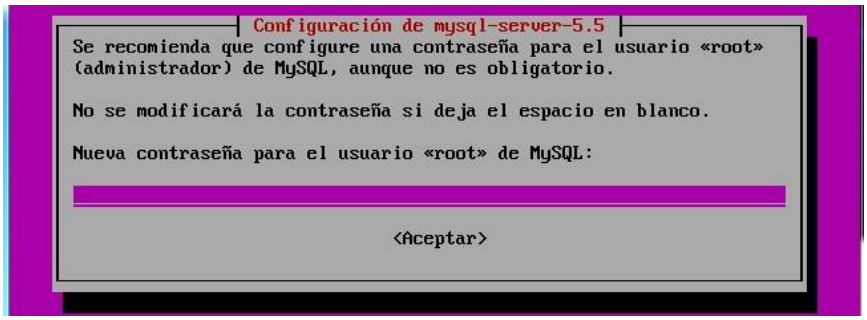


Figura 137 Ubuntu Server - Establecer contraseña root

Figura 138 Ubuntu Server - Instalación del paquete phpmyadmin

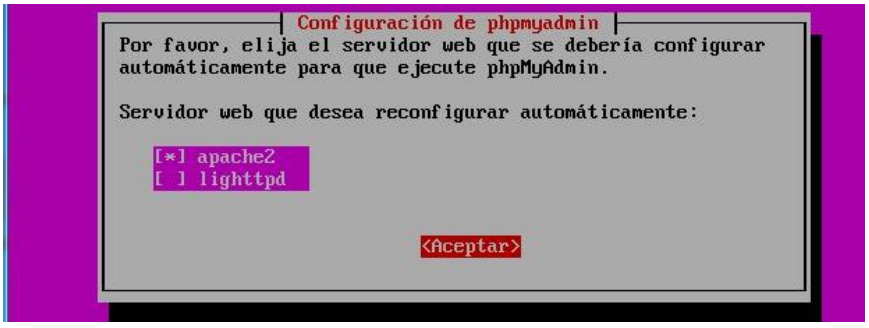


Figura 139 Ubuntu Server - Configuración del servidor web de phpmyadmin

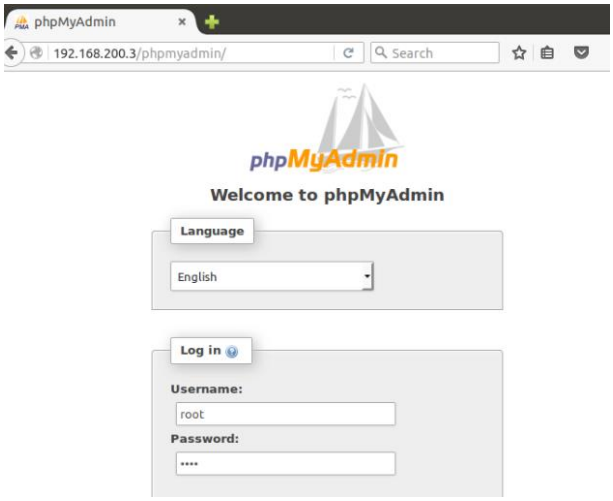


Figura 140 Ubuntu Server - Pantalla de login a phpmyadmin

A continuación, se creará la base de datos Ejemplo con tres tablas para el registro de Usuarios, Usuario_Sistema y Auditoría, como se muestra en las Figuras 141 a 144.

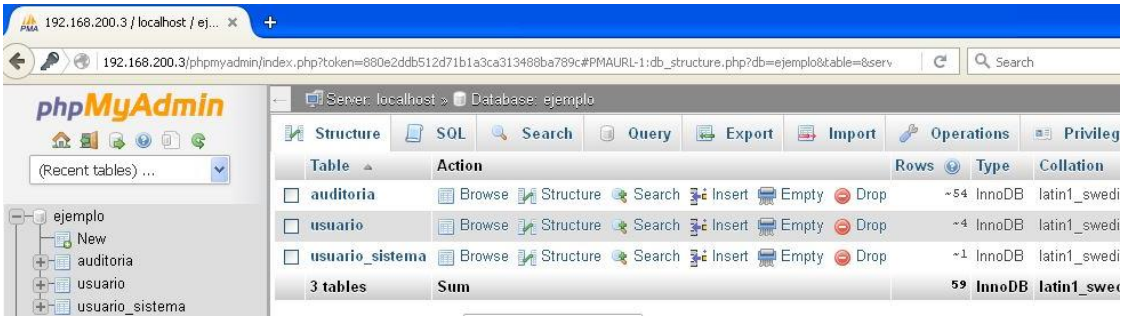


Figura 141 Ubuntu Server - Creación de la base de datos Ejemplo y sus tablas

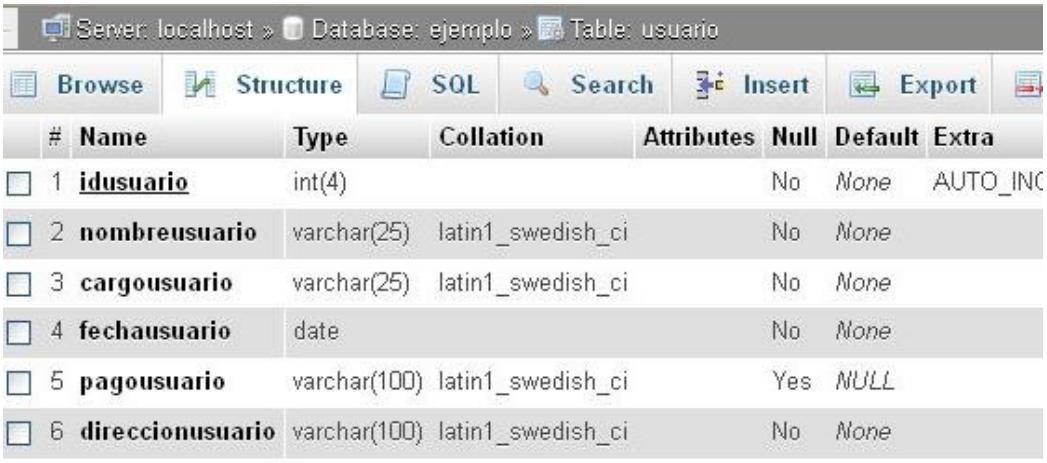


Figura 142 Ubuntu Server - Creación de la tabla Usuario

Figura 143 Ubuntu Server - Creación de la tabla Usuario_Sistema

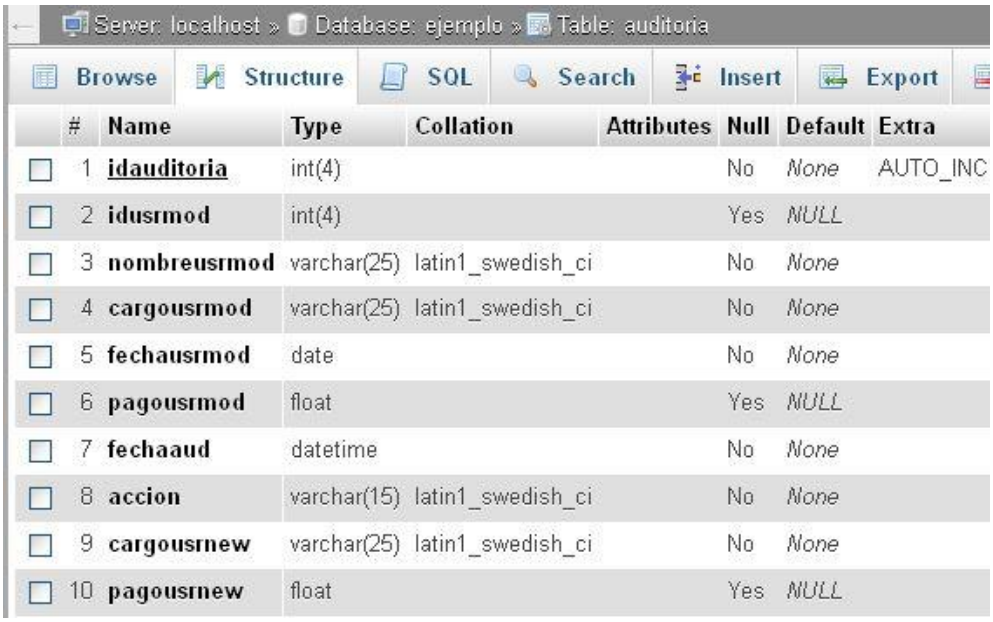


Figura 144 Ubuntu Server - Creación de tabla Auditoria

Los datos registrados en la tabla Auditoría se almacenarán automáticamente al realizarse modificaciones en la tabla Usuario, para esto

se ha realizado la creación de Triggers o disparadores en la tabla Usuario, que permiten captar los cambios realizados. En las Figuras 145 a 148 se muestra el detalle de los Triggers creados.

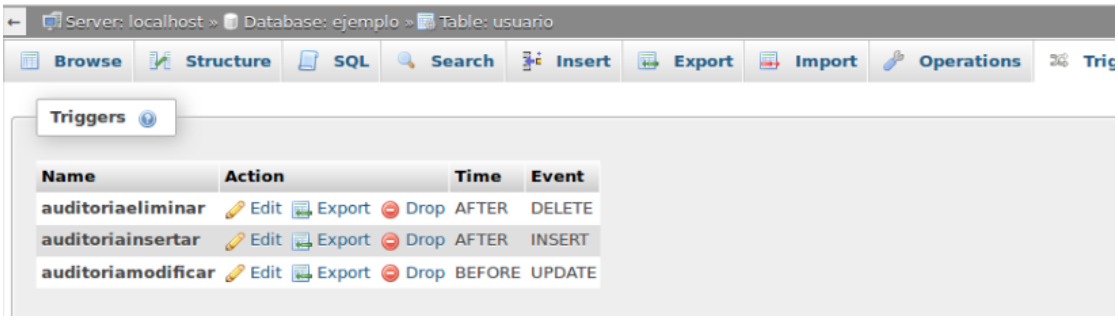


Figura 145 Ubuntu Server - Triggers en la tabla Usuario

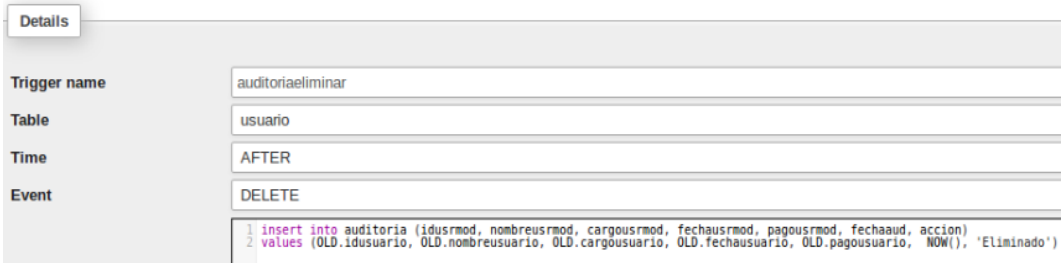


Figura 146 Ubuntu Server - Creación Trigger "Eliminar"

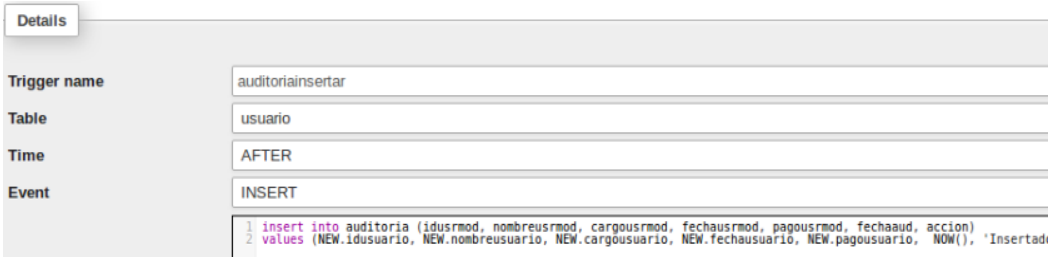


Figura 147 Ubuntu Server - Creación Trigger "Editar"

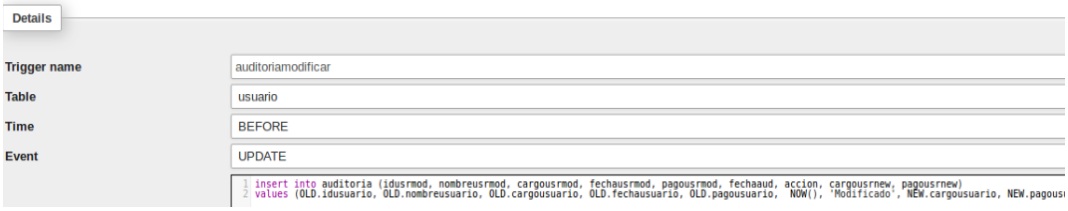


Figura 148 Ubuntu Server - Creación Trigger "Modificar"

Finalmente, para un manejo fácil de la Base de Datos anteriormente creada, se configuró una página Html que permita Agregar, Modificar o

Eliminar los Usuarios. En las Figuras 139 y 140 se muestra la página configurada.

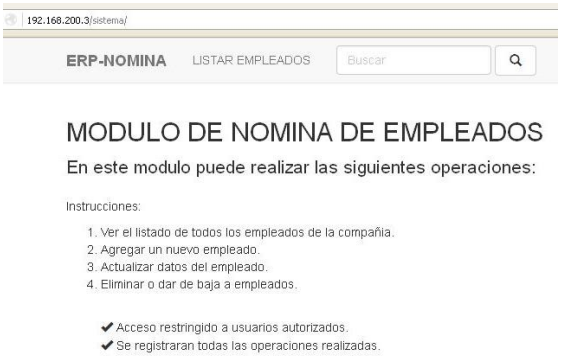


Figura 149 Ubuntu Server - Página de Inicio HTML para Base de Datos

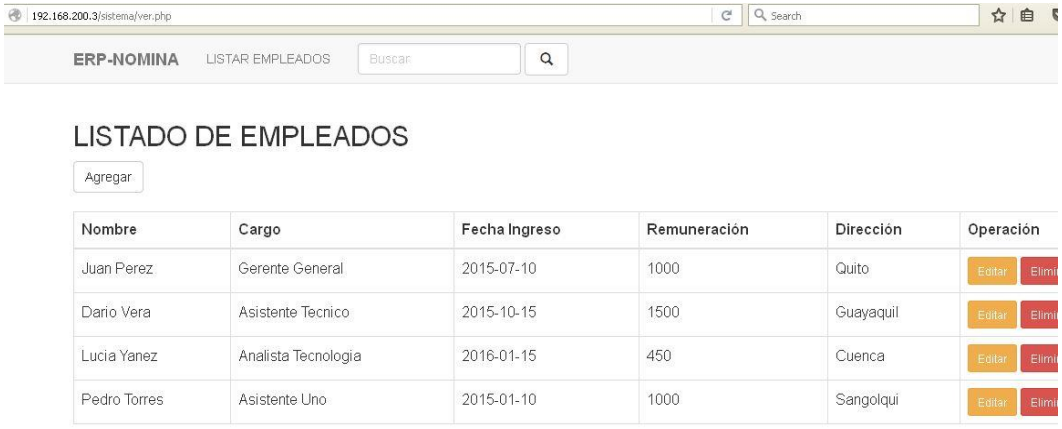


Figura 150 Ubuntu Server - Página HTML para Administración de Usuarios de Base de Datos

3.6.5.3.3. Integración Ubuntu Server- OSSIM

Posterior a la instalación y configuración de la Base de datos se procederá a la configuración de envío de los eventos de seguridad del Servidor Ubuntu al Servidor OSSIM, a través del Agente OSSEC.

- **Servidor Ubuntu:**

En el Ubuntu Server se realiza la instalación del agente OSSEC, este agente se encarga de recolectar y enviar los registros al servidor OSSIM a través de su dirección IP, en las Figuras 151 a 154 se muestra la instalación del agente a través del terminal del equipo:

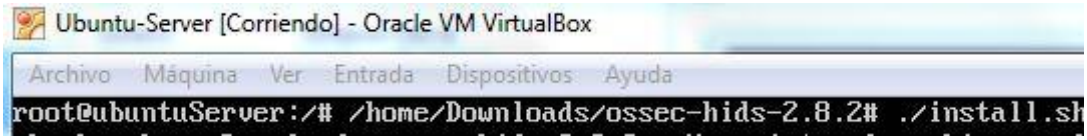


Figura 151 Instalación del paquete ossec-hids 2.8.2

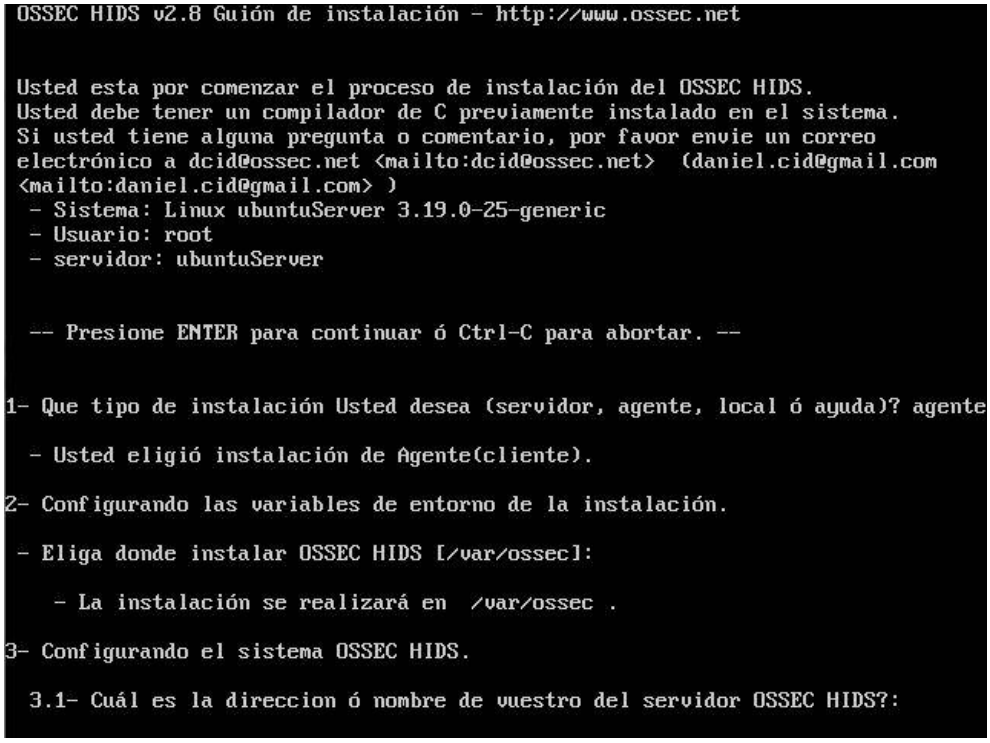


Figura 152 Proceso de instalación agente ossec

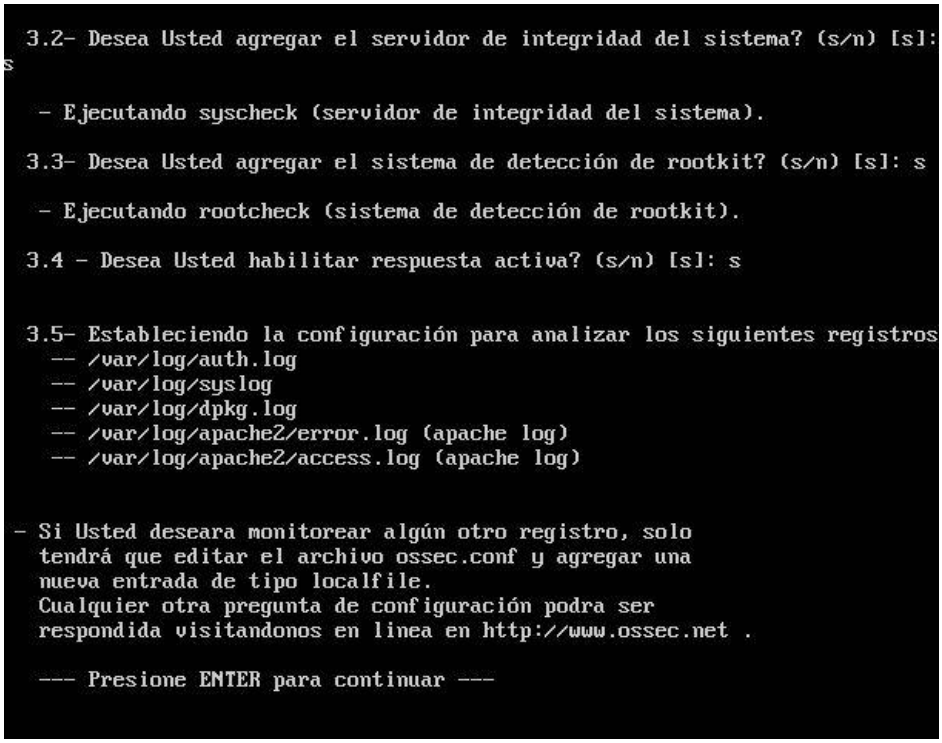


Figura 153 Selección de opciones para agente ossec

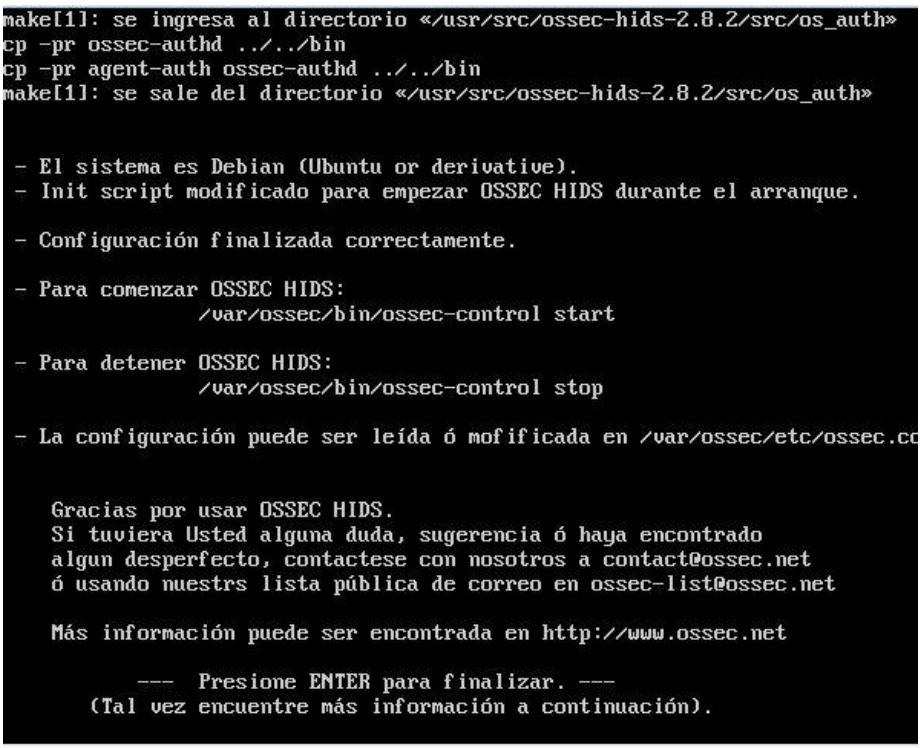


Figura 154 Instalación Finalizada

- **OSSIM:**

Para finalizar la integración del servidor Ubuntu con OSSIM, se crea un nuevo agente dentro del módulo “Enviroment”->“Detection. El status del agente cambiará al activar el agente en la sección “Actions”. En las Figuras 155 y 156 se muestra el agente activado.

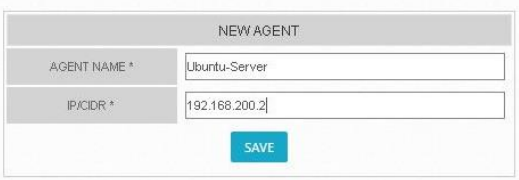


Figura 155 Creación agente Ubuntu Server

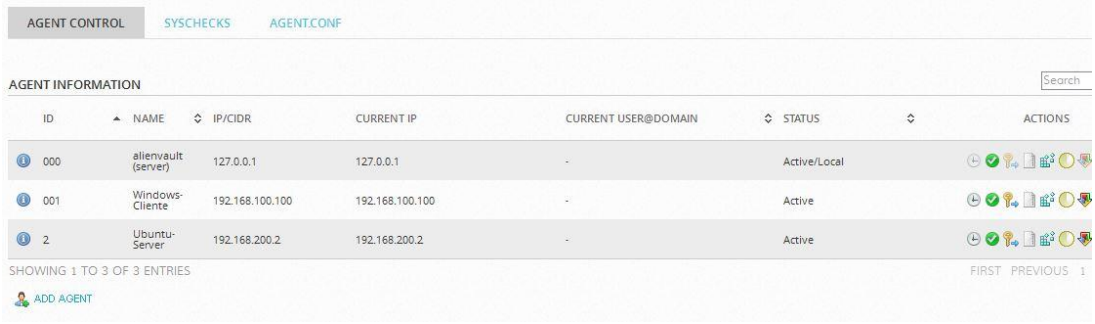


Figura 156 Agente Ubuntu Server Activado

Para verificar el correcto funcionamiento del agente OSSEC con el servidor Ubuntu, se reinició la sesión del servidor Ubuntu, en la Figura 157 se visualiza los resultados.

EVENT NAME	RISK	GENERATOR	SENSOR	SOURCE IP
ossec: Login session opened.	0	ossec-authentication_success	alienvault	Ubuntu-Server
ossec: SSHD authentication success.	0	ossec-authentication_success	alienvault	192.168.200.1:39818
ossec: SSHD authentication failed.	0	ossec-authentication_failed	alienvault	192.168.200.1:39816
ossec: User login failed.	0	ossec-authentication_failed	alienvault	Ubuntu-Server

Figura 157 Recolección en tiempo real de logs Agente Windows Server

3.6.5.4. Instalación y Configuración Cliente Windows

3.6.5.4.1. Instalación y Configuración de máquina virtual y Sistema Operativo Windows XP

Posterior a la instalación y configuración de la Base de datos se procederá a la configuración de envío de los eventos, en las Figuras 158 a 164 se muestra el procedimiento para la instalación de la máquina virtual y configuración del sistema operativo Windows XP.

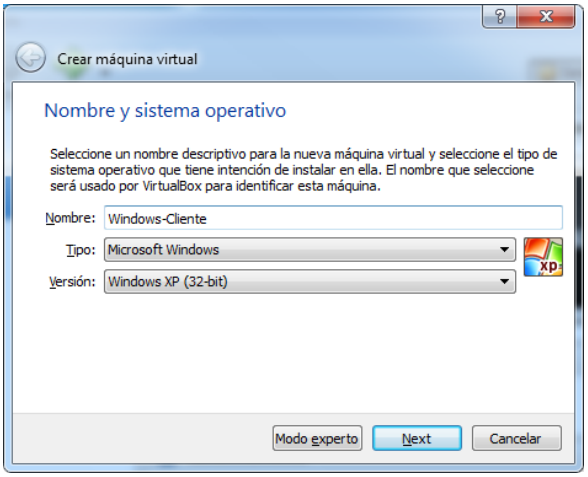


Figura 158 Máquina Virtual Cliente Windows – Selección del Sistema Operativo

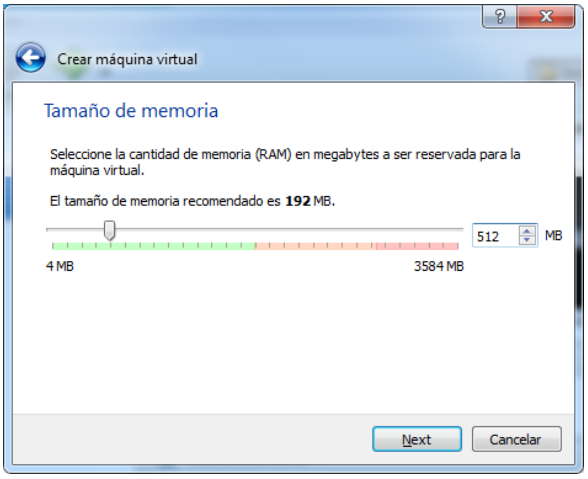


Figura 159 Máquina Virtual Cliente Windows –Selección memoria RAM

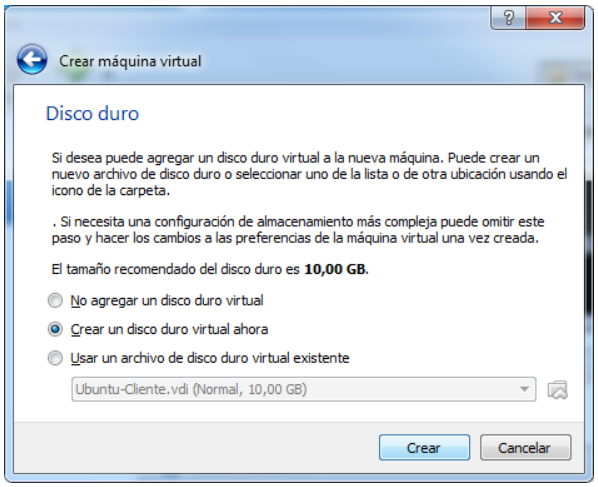


Figura 160 Máquina Virtual Cliente Windows – Creación del disco virtual

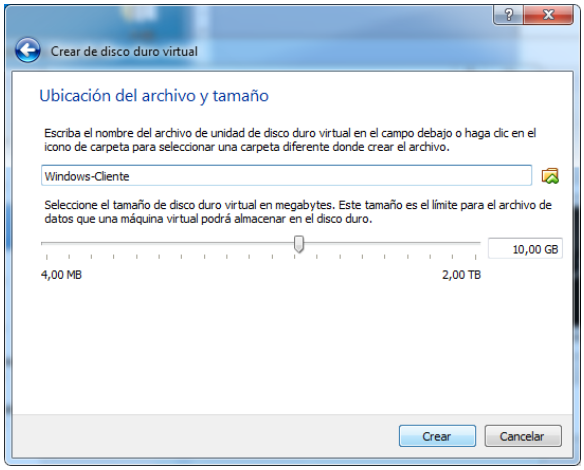


Figura 161 Máquina Virtual Cliente Windows – Configuración capacidad disco duro

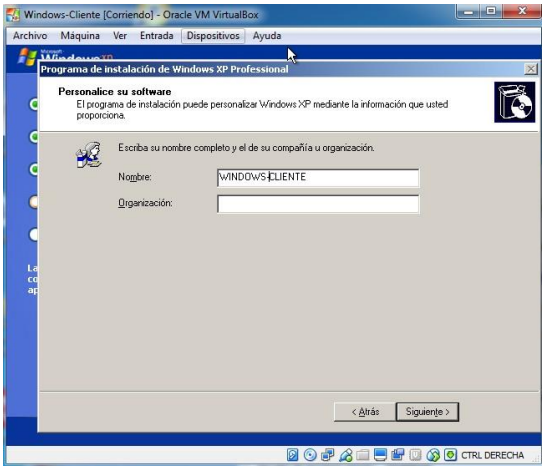


Figura 162 Máquina Virtual Cliente Windows – Configuración nombre de la organización

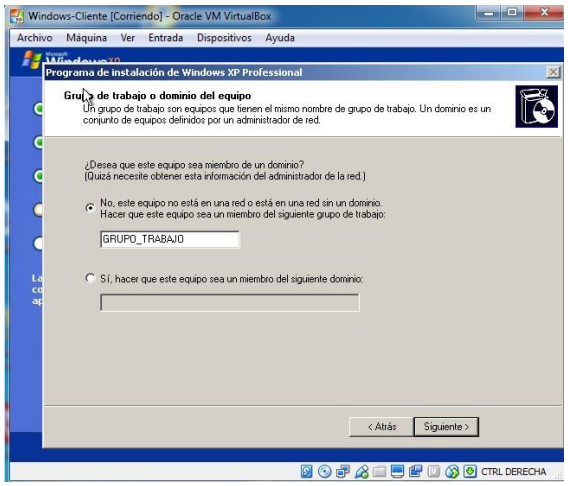


Figura 163 Máquina Virtual Cliente Windows – Grupo de trabajo

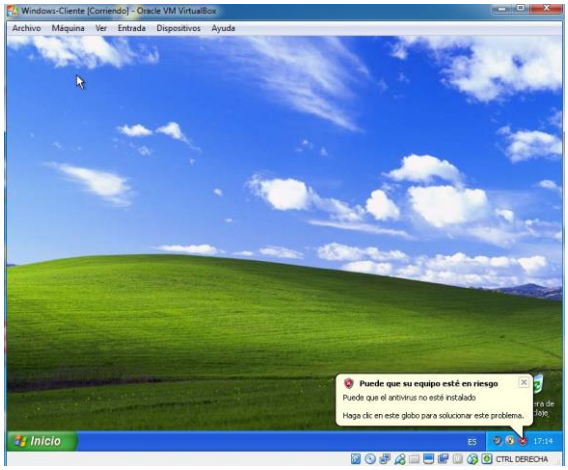


Figura 164 Máquina Virtual Cliente Windows – Pantalla de inicio de Windows

3.6.5.4.2. Configuración de Controlador de Dominio

Posterior a la instalación del cliente Windows, se procederá a la vinculación del mismo con el Dominio del servidor Windows Server 2008 como se muestra en las Figuras 165 y 166.

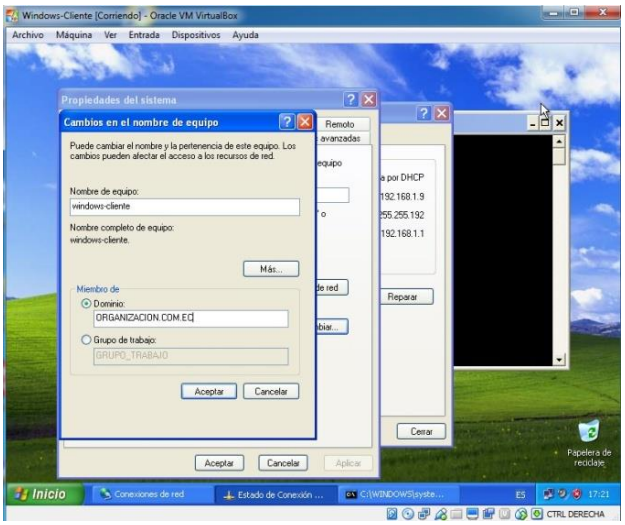


Figura 165 Máquina Virtual Cliente Windows – Agregar el cliente al Dominio

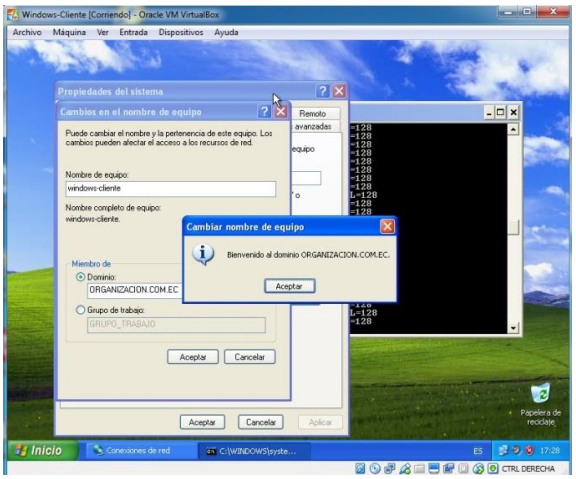


Figura 166 Máquina Virtual Cliente Windows – Vinculación al Dominio

A continuación, se crea un usuario de Active Directory, por seguridad se ha habilitado la opción que las contraseñas deben cumplir los requerimientos de complejidad, establecidas en la Directiva de Seguridad del Dominio, como se indica en la Figura 167 y 168. Para comprobar el funcionamiento ingresamos con el usuario creado desde el Windows-Cliente XP, como se indica en la Figura 169.

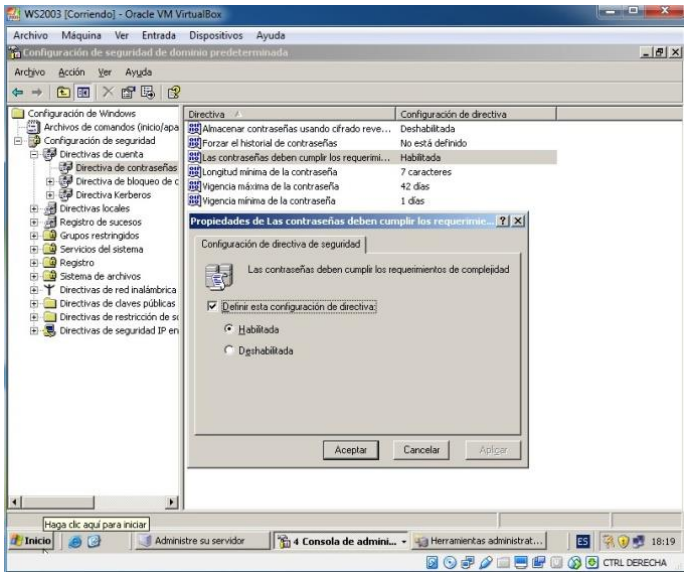


Figura 167 Máquina Virtual Servidor Windows – Establecer la complejidad de contraseñas

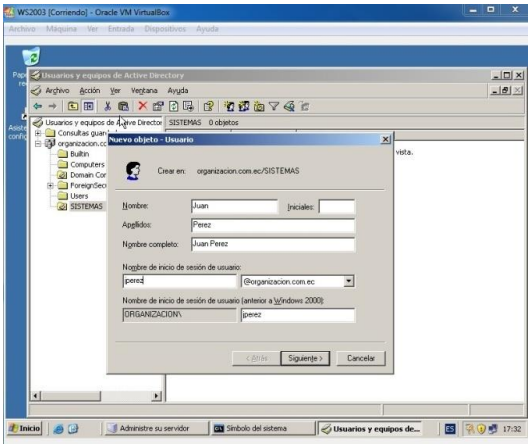


Figura 168 Máquina Virtual Cliente Windows – Creación de un usuario

Figura 169 Máquina Virtual Cliente Windows – Pantalla de inicio de cliente al dominio

3.6.5.4.3. Integración Cliente Windows – OSSIM

- **Cliente Windows**

En el servidor Windows 2008 se realiza la instalación del agente OSSEC, este agente se encarga de recolectar y enviar los registros o logs al servidor OSSIM a través de su dirección IP, en las Figuras 170 a 171 se muestra la instalación del agente como un programa común:

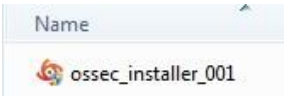


Figura 170 Agente a ser instalado en el Cliente Windows

Figura 171 Comprobación que se ejecuta el agente en el Cliente Windows

- **OSSIM:**

Para monitorear las actividades del cliente Windows, se instalará el agente en el servidor OSSIM. Ingresando al módulo “Asset” ->“Enviroment”-> “Assets Groups” -> “Add Assets” se creará el nuevo activo *Windows- Cliente* como muestra la Figura 1672.

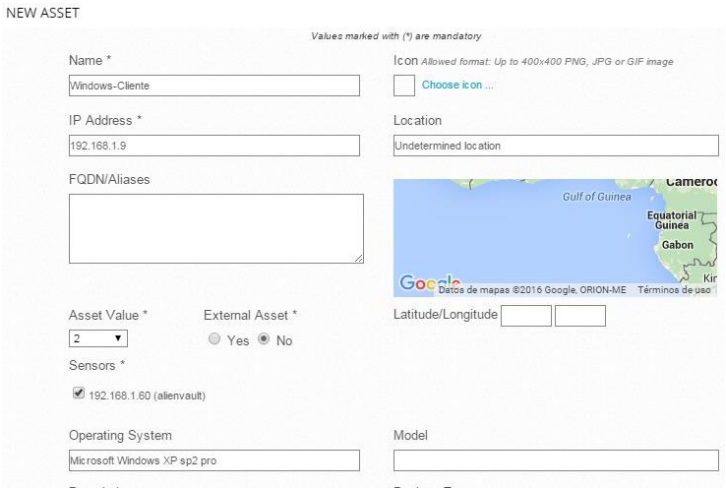


Figura 172 Ingreso de información del nuevo Activo (Asset)

Para finalizar la integración del cliente Windows con OSSIM, se crea un nuevo agente dentro del módulo “Enviroment”->“Detection. El status del agente cambiará al activar el agente en la sección “Actions”. En las Figura 173 se muestra el agente activado.

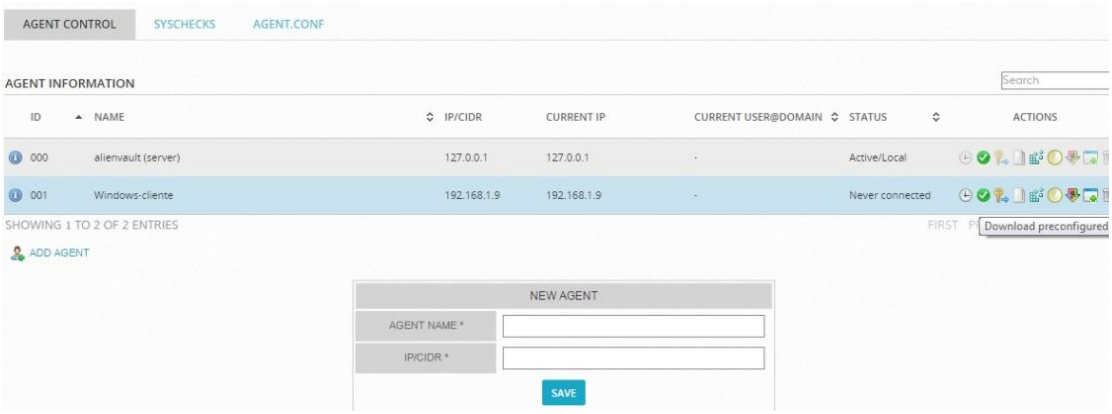


Figura 173 Creación agente Windows Cliente y activación

Para verificar el correcto funcionamiento del agente OSSEC con el cliente Windows, se visualiza los logs recolectados por el servidor OSSIM, como se muestra en la Figura 163.

NOMBRE DEL EVENTO	RIESGO	GENERADOR	SENSOR	IP ORIGEN
ossec: Ossec agent started.	0	ossec-ossec	alienvault	Windows-Cliente
ossec: Ossec agent started.	0	ossec-ossec	alienvault	Windows-Cliente
ossec: Windows Audit event.	0	ossec-rootcheck	alienvault	Windows-Cliente

Figura 174 Recolección en tiempo real de logs Agente Windows

3.7. Ejemplo Caso de Negocio

En esta sección se describirá un caso de negocio sobre el cual se ilustrará la gestión de eventos de seguridad informática utilizando la herramienta OSSIM y considerando algunas de las configuraciones realizadas y detalladas en la sección “3.6. Configuración de Fuentes de Eventos”; cabe mencionar que el ejemplo de caso de negocio es un escenario típico en una organización. En la Figura 164, se muestra el diagrama lógico secuencial del atacante (intruso).

Figura 175 Diagrama Lógico de Atacante Interno

- *Descripción del Caso de Negocio:*

El objetivo del Atacante (usuario desvinculado de la organización) es sustraer información confidencial de clientes de la base de datos y modificar información de la nómina del personal de la organización, accediendo a varios servidores

- *Etapa 1:* El Atacante, valiéndose de credenciales de un usuario legítimo, accede al computador. Se registra los logs de acceso al Cliente-Ubuntu.

- *Etapa 2:* Desde el computador, el Atacante accederá al sistema de talento humano, servidor web (192.168.200.3/sistema) alojado en el servidor Ubuntu-Server; Se registra los logs de acceso a Ubuntu-Server

- *Etapa 3:* El Atacante realiza una modificación en la información del sistema de recursos humanos alterando la base de datos. Se registra el log de acceso a la base de datos MySQL.

En la Figura 176 se muestra el diagrama del ataque interno de red realizado en base al caso de negocio planteado.

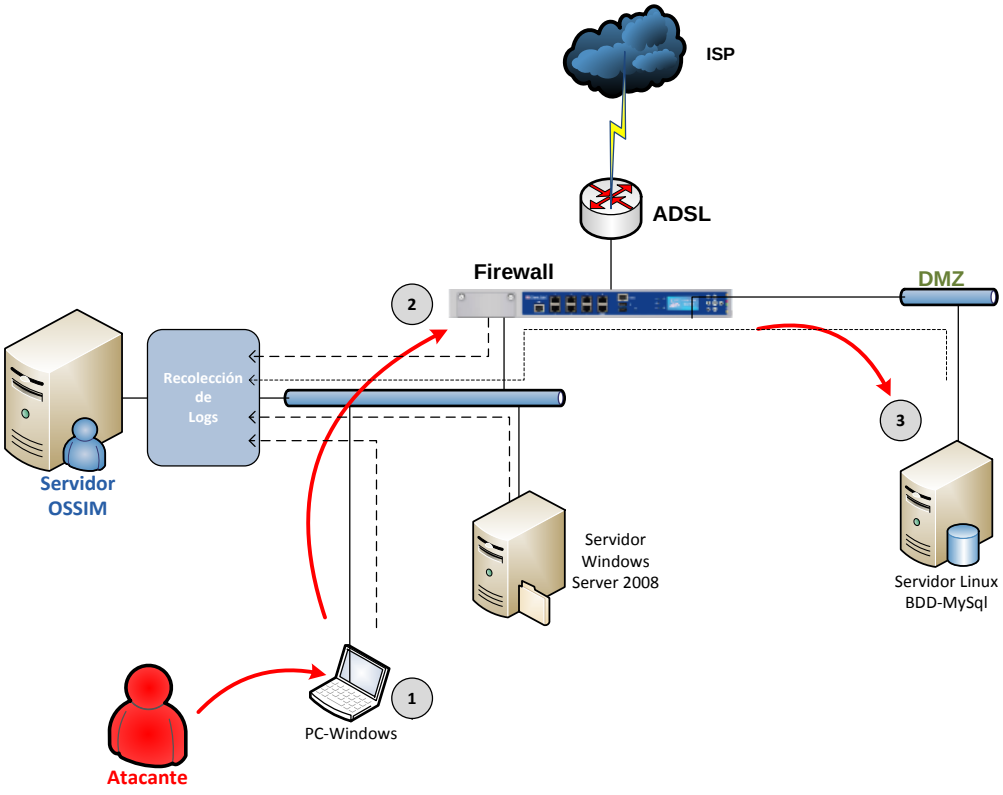


Figura 176 Diagrama de Ataque interno en la red

3.7.1. Creación y Configuración de Directivas

A continuación, se detallan los pasos para la creación de las directivas en OSSIM, las que permitirán generar alarmas según las reglas que se definan. Dichas reglas serán definidas y configuradas de acuerdo al evento que se desee monitorear o detectar de acuerdo a algún comportamiento inusual o anormal en la red de la organización. Para propósitos del prototipo del caso de negocio aquí expuesto, se ha definido que se creará y configurará una directiva por cada log o registro generado en cada etapa del ataque interno realizado por el usuario mal intencionado.

La creación y configuración de estas directivas brindarán de manera general ejemplos de configuraciones que se deseen realizar para casos específicos. Es recomendable previamente a la creación de directivas, analizar el contenido y estructura del log que deseemos monitorear y generar alarmas.

- **Etapa 1:** El usuario atacante ingresa al computador host Windows-Cliente.

Nombre de la Directiva: Acceso-Windows-Exitoso

Log generado:

Date	Event Name	Risk	Generator	Sensor	Source IP	Dest IP
2016-11-30 16:40:16	ossec: Windows Logon Success.	0	ossec-authentication_success	alienvault	Windows-Cliente:1870	Windows-Server

Para creación de directicas se debe dirigir a la sección Configuración, Inteligencia y a continuación a Directivas; la configuración de la directiva “Acceso-Windows-Exitoso” se ilustra en las Figuras 177 a 187.

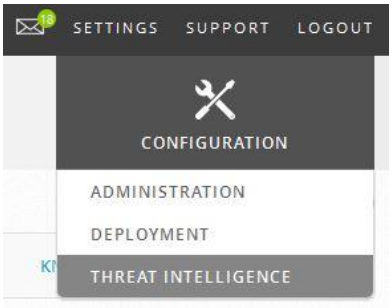


Figura 177 Directiva Acceso Windows Exitoso – Ingreso a Threat Inteligence

Figura 178 Directiva Acceso Windows Exitoso – Selección Directivas

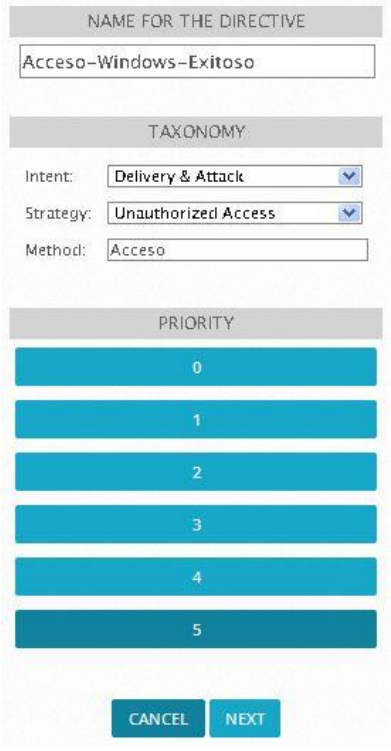


Figura 179 Directiva Acceso Windows Exitoso – Configuración de Directiva / Selección de Prioridad

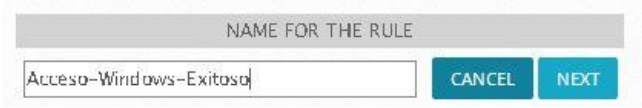


Figura 180 Directiva Acceso Windows Exitoso – Nombre de la Regla

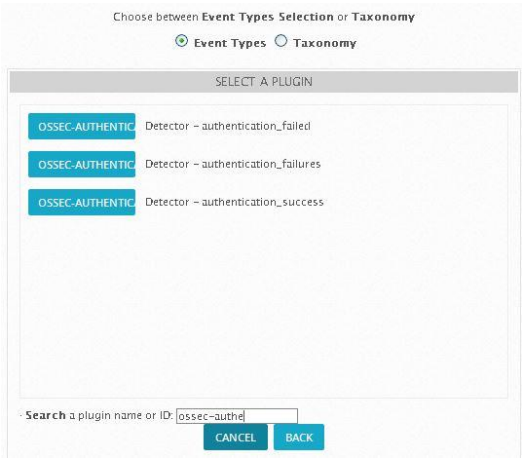


Figura 181 Directiva Acceso Windows Exitoso – Selección del Agente Detector

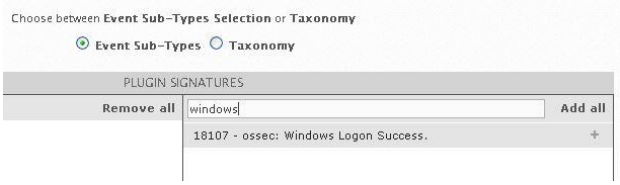


Figura 182 Directiva Acceso Windows Exitoso – Selección del tipo de Evento

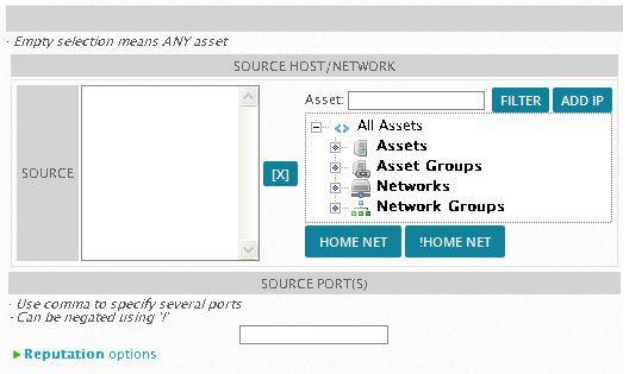


Figura 183 Directiva Acceso Windows Exitoso – Selección de Host/Network Origen

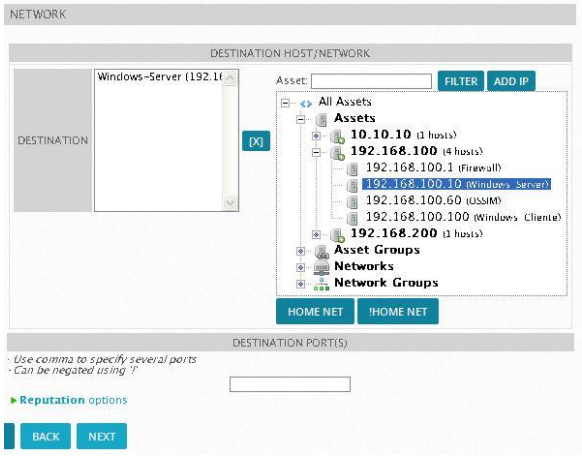


Figura 184 Directiva Acceso Windows Exitoso – Selección de Host/Network Destino

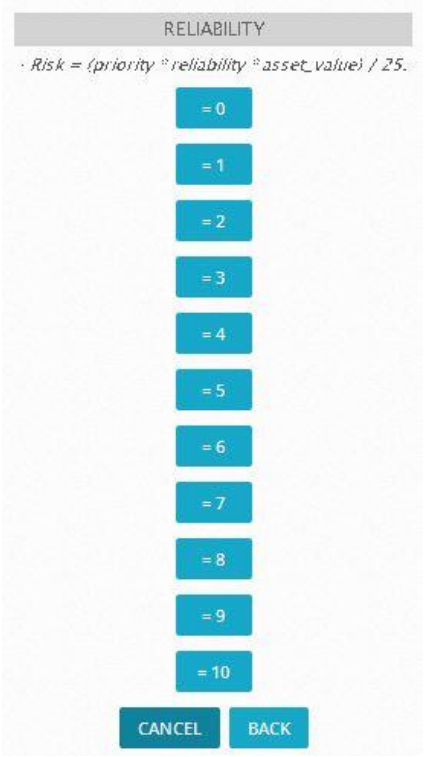


Figura 185 Directiva Acceso Windows Exitoso – Selección confiabilidad

Figura 186 Directiva Acceso Windows Exitoso – Confirmación para Finalizar Regla

Figura 187 Directiva Acceso Windows Exitoso – Directiva creada

Para ilustrar que la directiva efectivamente funciona se realiza un ingreso con el usuario administrador del dominio de Windows en el host Windows-Cliente, según se muestra en la Figura 188; y el resultado se muestra en la Figura 189.

Figura 188 Etapa 1 – Intento de conexión Windows

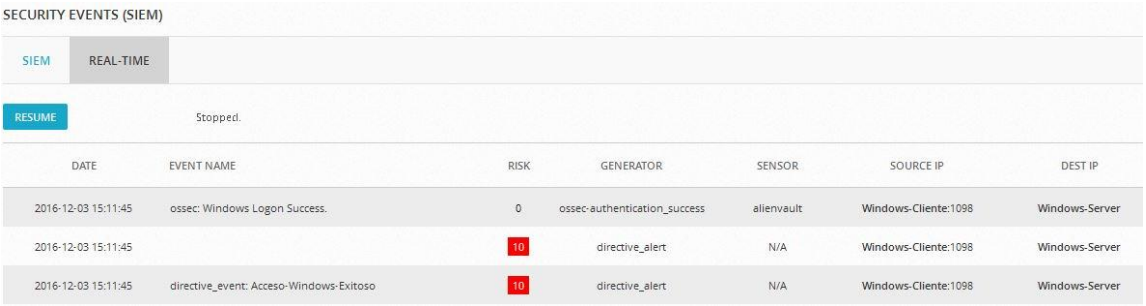


Figura 189 Etapa 1 - Log generado por Directiva Acceso Windows Exitoso

- **Etapa 2:** El usuario atacante una vez accedido al computador, ingresa al sistema web de recursos humanos mediante el navegador de Internet a la siguiente dirección: http://192.168.200.3/sistema/login.php.

Nombre de la directiva: Conexión-UbuntuServerWeb-Exitoso

Log generado:

Date	Event Name	Risk	Generator	Sensor	Source IP	Dest IP
2016-11-23 16:08:13	checkpoint: accept Success.	0	Checkpoint	alienvault	Windows-Cliente:4173	Ubuntu-Server

La configuración de la directiva "Conexión-UbuntuServerWeb-Exitoso" se ilustra en las Figuras 190 a 198.

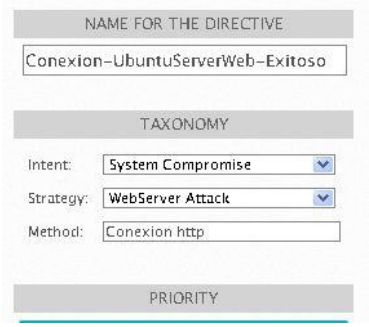


Figura 190 Directiva Acceso Ubuntu Exitoso - Configuración de Directiva / Selección de Prioridad

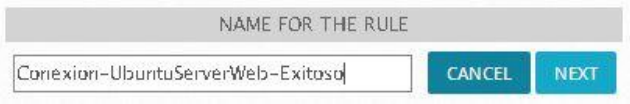


Figura 191 Directiva Acceso Ubuntu Exitoso – Nombre de la regla

Figura 192 Directiva Acceso Ubuntu Exitoso – Selección agente detector

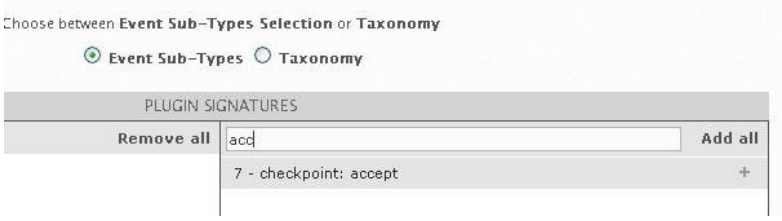


Figura 193 Directiva Acceso Ubuntu Exitoso – Selección tipo de evento

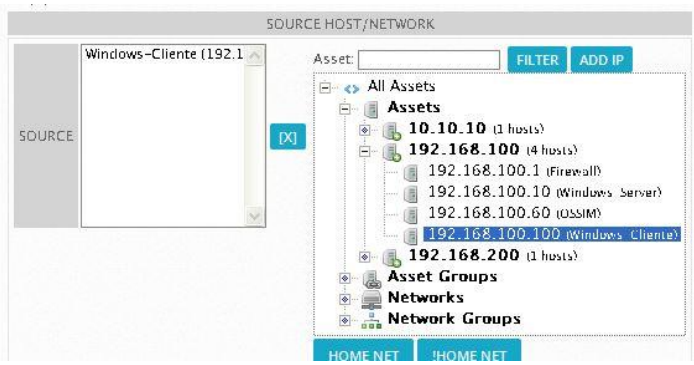


Figura 194 Directiva Acceso Ubuntu Exitoso – Selección de Host/network Origen

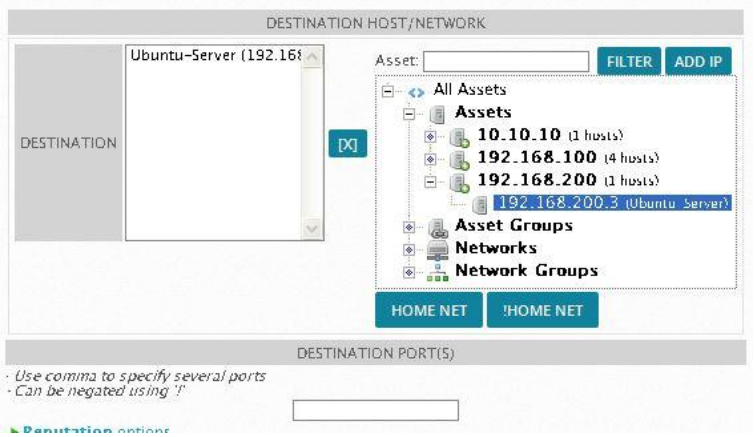


Figura 195 Directiva Acceso Ubuntu Exitoso – Selección de Host/Network Destino

Figura 196 Directiva Acceso Ubuntu Exitoso – Selección confiabilidad

Figura 197 Directiva Acceso Ubuntu Exitoso – Confirmación para Finalizar Directiva

Figura 198 Directiva Acceso Ubuntu Exitoso – Directiva Creada

En la Figura 199 se ilustra el funcionamiento de la directiva y en la Figura 200 el resultado obtenido:

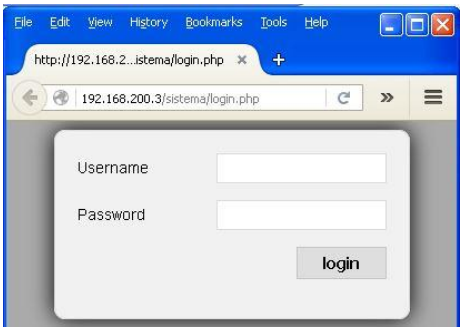


Figura 199 Etapa 2 – Intento de conexión Ubuntu

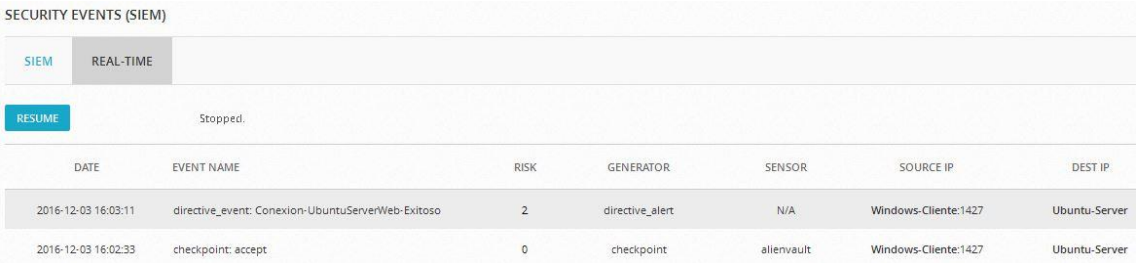


Figura 200 Etapa 2 – Log generado por Directiva Acceso Ubuntu Exitoso

- **Etapa 3: Una** vez ingresado al sistema de recursos humanos, el atacante realiza una modificación en la información la cual se refleja adicionalmente en una tabla de auditoria sobre los cambios realizados en la tabla de los empleados de la organización.

Nombre de la Directiva: *Conexión-BaseDatos-Exitosa*

Log Generado

Date	Event Name	Risk	Generator	Sensor	Source IP	Dest IP
2016-11-30 16:45:26	ossec: Database authentication success.	0	ossec-authentication_success	alienvault	Ubuntu-Server	Ubuntu-Server

La configuración de la directiva “Conexión-BaseDatos-Exitosa” se ilustra en las Figuras 201 a la 210.

Figura 201 Directiva Acceso Base de Datos - Configuración de Directiva / Selección de Prioridad

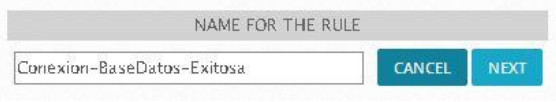


Figura 202 Directiva Acceso Base de Datos – Nombre de la regla

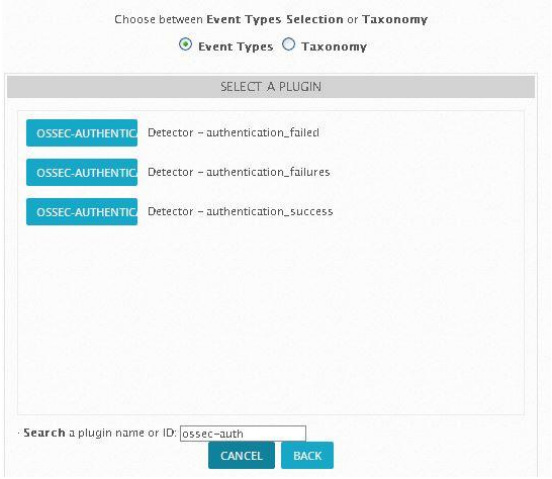


Figura 203 Directiva Acceso Base de Datos – Selección agente detector

Figura 204 Directiva Acceso Base de Datos – Selección del tipo de evento

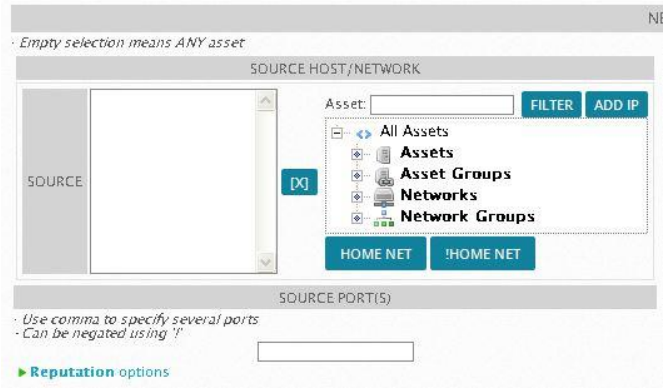


Figura 205 Directiva Acceso Base de Datos - Selección de Host/Network Origen

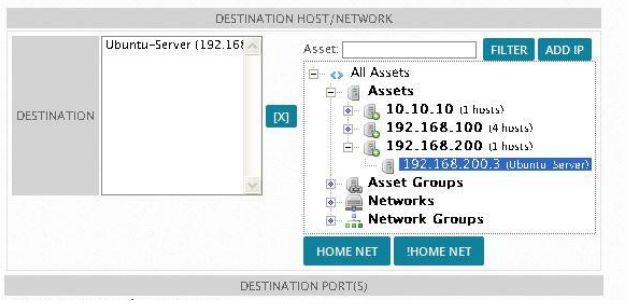


Figura 206 Directiva Acceso Base de Datos - Selección de Host/Network Destino

Figura 207 Directiva Acceso Base de Datos - Selección confiabilidad

Figura 208 Directiva Acceso Base de Datos - Confirmación para Finalizar Regla

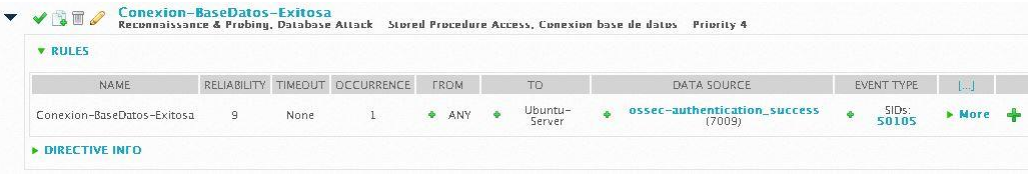


Figura 209 Directiva Acceso Base de Datos – Directiva creada

Para ilustrar el funcionamiento de la directiva creada, se realiza una actualización o modificación del valor de la remuneración de un usuario, según se ilustra en la Figura 210 y 213.

Figura 210 Etapa 3 – Ingreso a Base de Datos

Figura 211 Etapa 3 – Modificación de Datos de Tabla

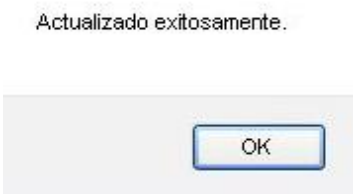


Figura 212 Etapa 3 – Modificación exitosa

LISTADO DE EMPLEADOS

Agregar

Nombre	Cargo	Fecha Ingreso	Remuneración	Dirección
Juan Perez	Gerente General	2015-07-10	1000	Quito
Dario Vera	Asistente Tecnico	2015-10-15	1500	Guayaquil
Lucia Yanez	Analista Tecnologia	2016-01-15	450	Cuenca
Pedro Torres	Asistente Uno	2015-01-10	1000	Sangolqui

Figura 213 Etapa 3 – Base de Datos Modificada

Figura 214 Etapa 3 - Directiva generada

Como se indicó anteriormente adicionalmente se genera un log en la tabla auditoria donde se guarda el valor anterior y el valor actual con la fecha actual de modificación, como se indica en la Figura 215.

idauditoria	idusrmod	nombreusrmod	cargousrmod	fechausrmod	pagousrmod	fechaaud	accion	cargousrnew	pagousrnew
57	1018	Dario Vera	Asistente Tecnico	2015-10-15	1000	2016-12-03 17:39:31	Modificado	Asistente Tecnico	1500

Figura 215 Etapa 3 – Detalle Tabla Auditoría

Como se pudo apreciar las alarmas generadas indican un valor de Riesgo que resulta del siguiente cálculo:

$$\boldsymbol{Riesgo} = \frac{\text{Prioridad} * \text{Confiabilidad} * \text{valor\_activo}}{25}$$

Cabe mencionar que el valor del activo se establece en el servidor OSSIM en función de su criticidad, por ejemplo, para servidores es 5 y para host a 3. Cuando en una directiva intervienen varios equipos (assets), OSSIM toma el menor valor del activo en cuestión.

3.7.2. Visualización y análisis de resultados

Una vez que se cuenta con las configuradas las directivas en OSSIM, así como la ilustración de la generación de las alarmas de cada etapa del ataque interno, se procede a ejecutar el escenario de pruebas del Caso de Negocio a manera de simulación de acciones secuenciales que lo realizaría rápidamente un lapso de tiempo no mayor a un minuto. En este punto es importante mencionar que por lo general cuando se comente algún acto ilícito, cometimiento actos fraudulentos, entre otros, utilizando los sistemas informáticos, es mayor aún la probabilidad de que ciertos patrones no normales sean perpetrados de manera que con sistemas de recolección de logs simples no se podría conseguir tener una detección temprana. En las Figuras 216 a la 219, se ilustra la ejecución del ataque interno.

Figura 216 Etapa 1 -Atacante ingresa a servidor Windows

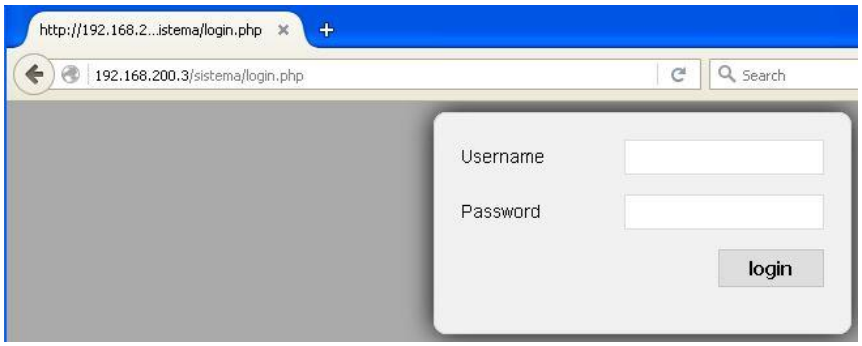


Figura 217 Etapa 2 – Atacante Ingresa a servidor Ubuntu

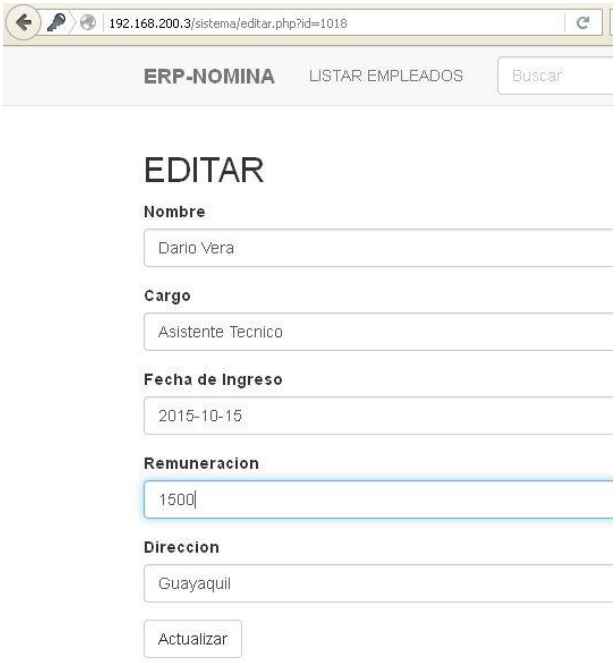


Figura 218 Etapa 3 – Atacante Ingresa a Base de Datos

Figura 219 Etapa 3 – Atacante Modifica la Base de Datos

En la siguiente Figura 220, se puede visualizar la generación de tres alarmas según las directivas creadas para el efecto. Conexión-BaseDatos-Exitosa Riesgo 7, Acceso-Windows-Exitoso Riesgo 10, y Conexión-UbuntuServerWeb-Exitoso.

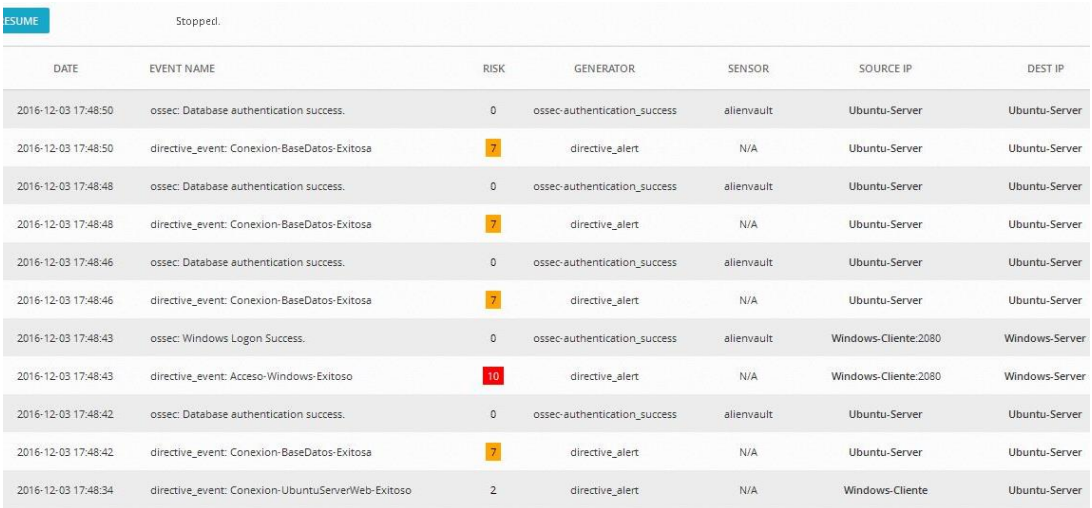


Figura 220 Resultados de Ataque

3.7.3. Alarmas Generadas

Como se pudo apreciar en la sección anterior las directivas permiten generar alarmas en tiempo real, mismas que son almacenadas en OSSIM para posterior análisis, así como los eventos o registros. OSSIM tienen la facilidad de visualizar dichas alarmas de una forma más descriptiva e intuitiva, para esto se debe ingresar a la sección Análisis - Alarmas como se indica en la Figura 221.

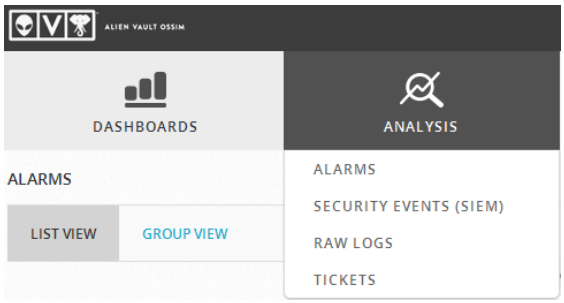


Figura 221 Ingreso a Sección Alarmas

Mediante la opción *List View,* en la Figura 222 se visualizan las alarmas generadas de manera cronológica, es decir los eventos y sus respectivas alarmas generadas en los últimos días representados con círculos; mientras el círculo sea más grande significa que se generaron mayor cantidad de alarmas.

Figura 222 Vista General de Alarmas

En la Figura 222 se pudo apreciar que existieron grupo de alarmas con fechas 1, 3 y 5 de diciembre 2016; se analizarán el grupo de alarmas del 3 de diciembre de 2016, dando clic en los círculos se puede apreciar con mayor detalle el tipo de alarma que corresponde.

3.7.3.1. Análisis alarma Acceso-Windows-Exitoso

En la Figura 223 se muestra el número de eventos en un lapso de tiempo, en este caso se tiene una cantidad grande de eventos puesto que el agente OSSEC del equipo Windows-Server genera más de un evento o log por el acceso exitoso al host Windows-Cliente.

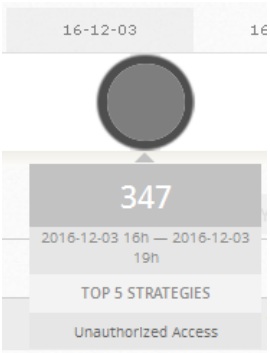


Figura 223 Número de Eventos Etapa 1

En la siguiente Figura 224, se detallan las alarmas generadas:

Figura 224 Alarmas Generadas Etapa 1

Se puede obtener mayor información de la alarma al hacer clic en el ícono del extremo derecho, la información que se obtiene es la que se muestra en la Figura 225:

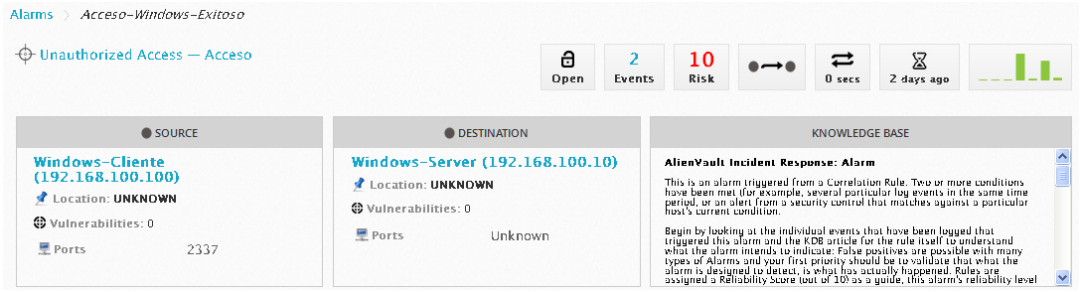


Figura 225 Detalles de Alarmas Etapa 1

3.7.3.2. Análisis alarma Conexión-UbuntuServerWeb-Exitoso

En la siguiente Figura 226 se muestra el número de eventos en el mismo lapso de tiempo del ataque interno, enviadas por el equipo Firewall que corresponden a las conexiones http entre el host Windows-Cliente y el servidor Ubuntu-Server.

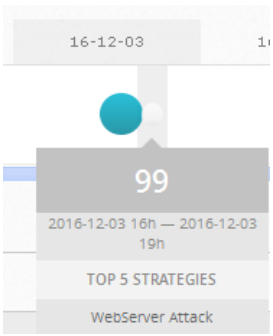


Figura 226 Número de Eventos Etapa 2

En la siguiente Figura 227, se detallan las alarmas generadas:

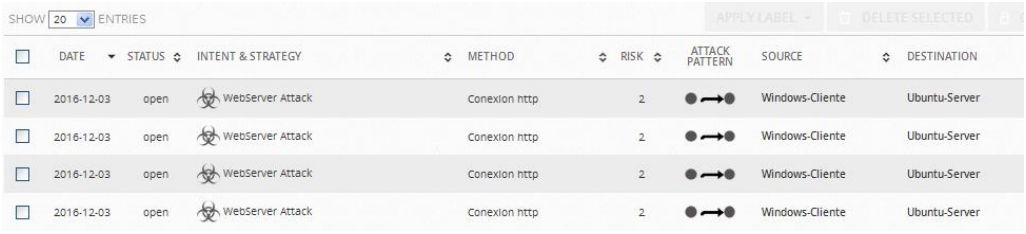


Figura 227 Alarmas Generadas Etapa 2

Se puede obtener mayor información de la alarma al hacer clic en el ícono del extremo derecho, la información que se obtiene es la que se muestra en la Figura 228:

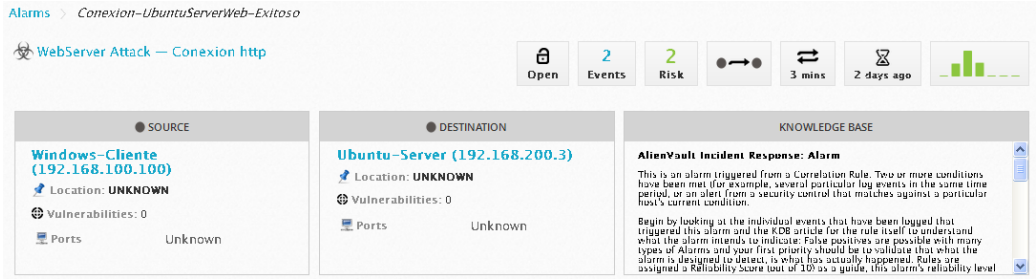


Figura 228 Detalle de Alarma Etapa 2

3.7.3.3. Análisis alarma Conexión-BaseDatos-Exitosa

En la siguiente Figura 229 se muestra el número de eventos que genera el agente OSSEC del equipo Ubuntu-Server que también genera muchos eventos o logs por el acceso exitoso a la base de datos.

Figura 229 Número de Eventos Etapa 3

En la siguiente Figura 230, se detallan las alarmas generadas:

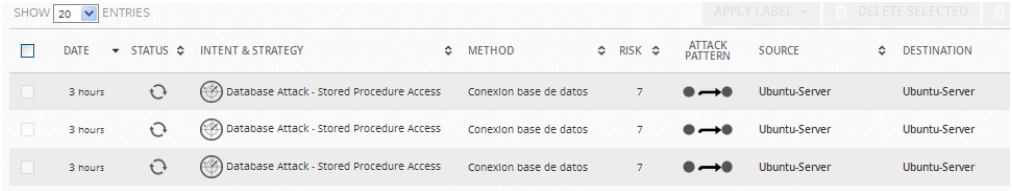


Figura 230 Alarmas Generadas Etapa 3

Para obtener mayor información de la alarma, se debe hacer clic en el ícono del extremo derecho de una alarma generada, la información que se obtiene es la que se muestra en la Figura 231:

Figura 231 Detalle de Alarma Etapa 3

En la Figura 232 se muestra las Alarmas mediante la opción *Group View*, se puede apreciar por grupos las alarmas que se han presentado en el sistema.

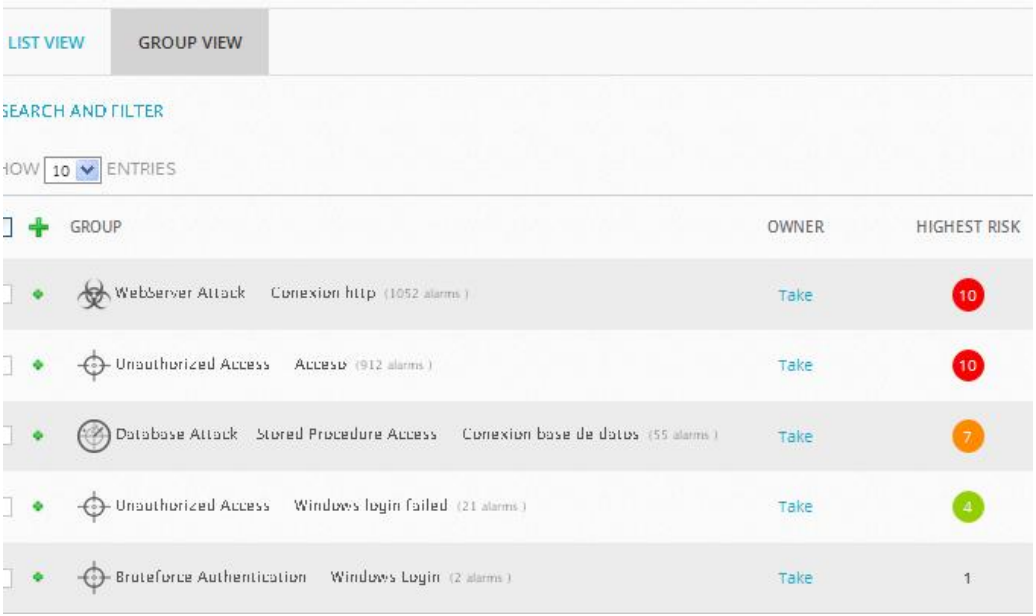


Figura 232 Alarmas por Group View

El administrador de seguridad o el responsable de la herramienta de gestión de eventos de seguridad informática OSSIM podrá hacer uso de estas características para realizar el análisis y revisión a detalle de los eventos de seguridad facilitándole su gestión en la resolución de incidentes.

3.7.4. Reportes de alarmas

En las opciones principales seleccionamos Reportes - Resumen, como se indica en la Figura 233:

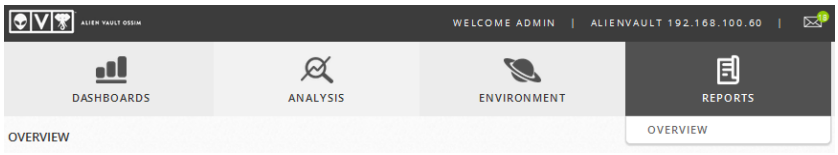


Figura 233 Sección Reportes

Seleccionamos la opción Reporte de Alarmas que se indica en la Figura 234:

Figura 234 Generación de Reportes

Para el escenario de pruebas realizado, se requiere establecer un rango de fechas para generar el reporte, en este caso será del 1 al 4 de diciembre 2016, a continuación, hacemos clic en “Download PDF”, en la Figura 235 se visualiza las principales alarmas detectadas:

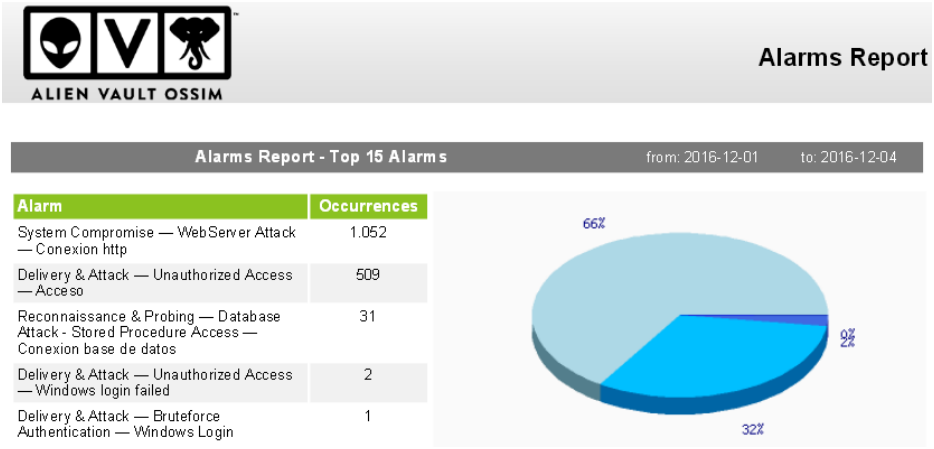


Figura 235 Vista de reporte generado

En el Anexo A se incluye el reporte completo de las alarmas generadas para el escenario de caso de negocio.

- **Conclusión**

La solución de gestión de eventos de seguridad informática OSSIM permite crear ciertas directivas, alarmas, correlación, y visualización de eventos que facilita el monitoreo, detección temprana y prevención de actividades en los sistemas de información; en tal sentido el escenario aquí descrito en sus diferentes etapas muestra un ejemplo clásico que se puede presentar en las organizaciones tradicionales.

CAPITULO 4: ANÁLISIS DE RESULTADOS

4.1. Escenario de Pruebas

En este capítulo se llevará a cabo un escenario controlado de ataques o de pruebas de seguridad informática mediante análisis de vulnerabilidades en una topología de red, mediante la selección y utilización de herramientas de análisis de seguridad no intrusivos en los sistemas. Se realizarán actividades de reconocimiento pasivo con la finalidad de identificar información disponible del objetivo o equipo analizado.

El esquema del ataque se realizará sobre los sistemas activos a nivel de infraestructura y de aplicaciones web con el propósito de que los activos o servidores atacados, generen eventos o logs de seguridad, que permita al sistema OSSIM detectarlos, disparar alarmas, reportes, estadísticas, entre otros, para una gestión integral. El principal objetivo es mostrar las bondades que tiene OSSIM como software libre y que permite contar con un sistema de gestión integral de seguridad, permitiendo a las organizaciones disminuir costos en la adquisición de equipos sofisticados de seguridad con licencia, soporte de mantenimiento, etc.

Finalmente, con los resultados obtenidos de los ataques controlados y con la integración de eventos al OSSIM, generados por dichos ataques, se realizará una evaluación de riesgos de seguridad tomando como referencia la norma ISO 27005, lo cual permitirá tener un visión amplia y general de lo que sucede en la red desde el punto de vista técnico y de gestión. Cabe indicar que no se detallarán las vulnerabilidades técnicas halladas por las herramientas de seguridad, pero si se analizarán los eventos o logs, así como las reglas de correlación definidas.

4.1.1. Topología

Para la ejecución del escenario de pruebas se utilizó una topología de red igual a la indicada en el capítulo 3, pues corresponde a un esquema de red que se encuentra comúnmente en organizaciones pequeñas y medianas. Para este caso el atacante ingresará a la red y realizará una serie de ataques directos hacia los tres servidores OSSIM, Ubuntu y Windows. Las pruebas utilizadas incluyen escaneo de puertos, escaneo de vulnerabilidades y ataques de fuerza bruta las cuales nos permitirán visualizar y analizar el comportamiento del prototipo antes implementado (máquina OSSIM) y analizar los riesgos detectados.

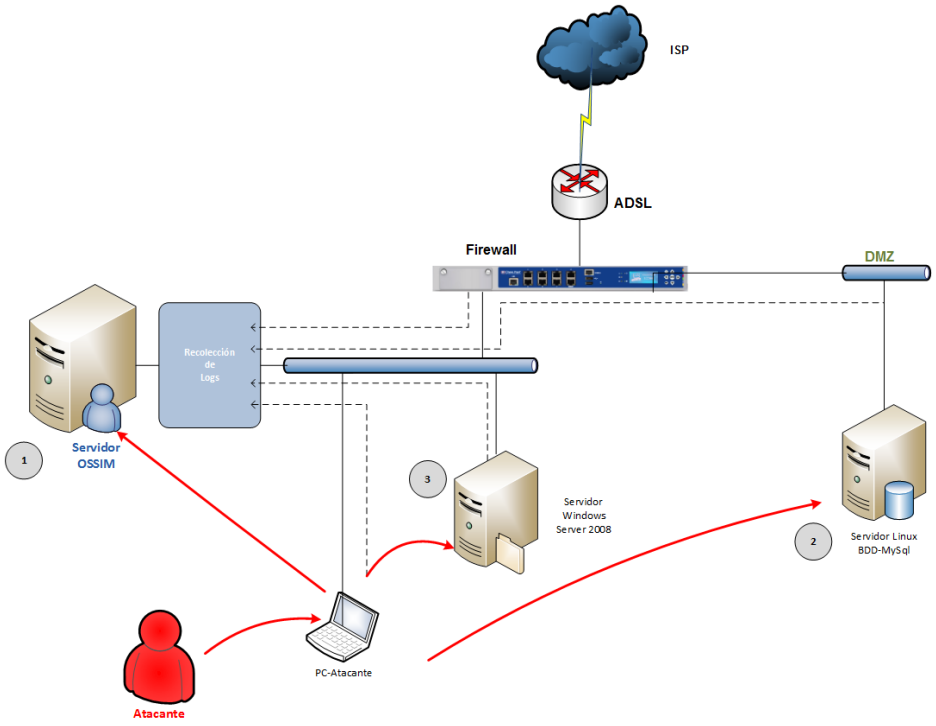


Figura 236 Topología de Escenario de Pruebas

4.1.2. Configuración de Ataque

Para ejecutar el ataque presentado en el escenario anterior se creó una máquina virtual llamada “Atacante”, basada en la distribución de software libre *Kali Linux* que está principalmente diseñada para realizar pruebas de penetración o auditoría de seguridad informática. Está distribución basada en Debian GNU/Linux cuenta con un conjunto de herramientas que permiten realizar ataques hacia la red física como escaneo de puertos, detección de vulnerabilidades, auditorías de seguridad, etc., y hacia aplicaciones como base de datos, servidores web, etc. Cabe recalcar que la filosofía base de Kali Linux es su utilización y desarrollo con fines educativos y éticos, para realizar un descubrimiento y evaluación de vulnerabilidades del sistema informático que permitan mejorar los controles de seguridad y minimicen la posibilidad de ataques reales que dañen la integridad y disponibilidad de los activos de una organización. En las Figuras 237 a 243 se muestran una descripción rápida

de la creación de la máquina virtual y la instalación del sistema operativo Kali Linux.

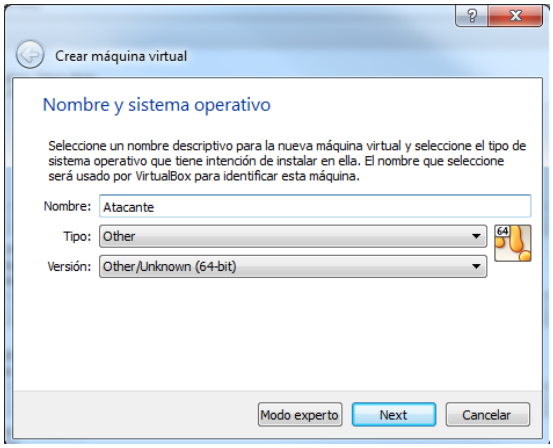


Figura 237 Máquina Virtual Atacante – Selección de sistema operativo

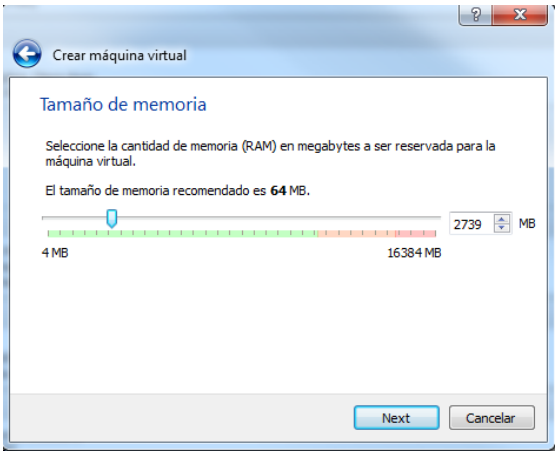


Figura 238 Máquina Virtual Atacante - Asignación de memoria

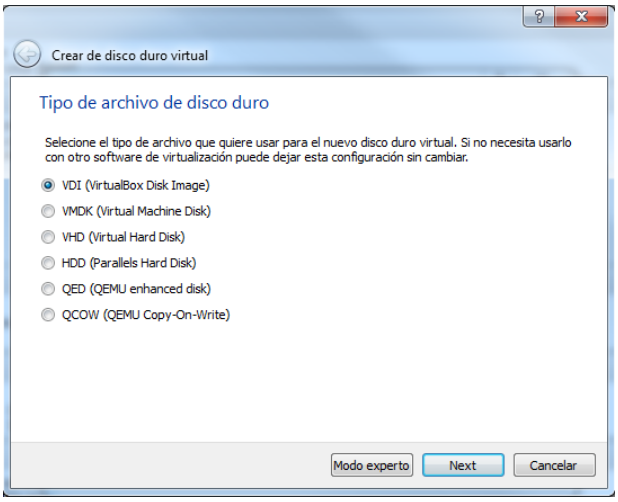


Figura 239 Máquina Virtual Atacante - Selección tipo de disco duro

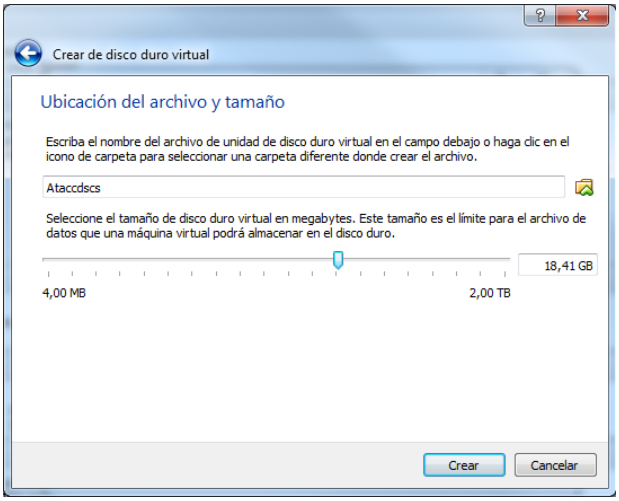


Figura 240 Máquina Virtual Atacante - Selección de tamaño de almacenamiento de disco duro

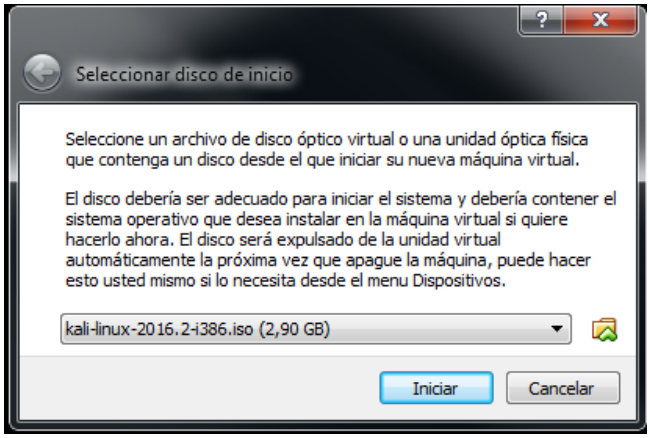


Figura 241 Máquina Virtual Atacante - Selección de imagen .iso software Kali Linux

Figura 242 Máquina Virtual Atacante - Inicio de Instalación Kali Linux

Figura 243 Máquina Virtual Atacante - Herramientas Kali Linux

La distribución Kali Linux tiene alrededor de 300 herramientas que permiten realizar una auditoría de seguridad hacia la red, de estas herramientas sean escogido 4 de ellas para realizar el ataque antes planteado, como son Nikto, Nmap, Hydra y Open Vas.

- **Nmap**

Uno de los primeros pasos para realizar un ataque informático es el reconocimiento de red, que permita disminuir el conjunto de direcciones IP en una lista de equipos activos. Una de las herramientas más utilizada a nivel mundial para realizar exploraciones de redes y escaneo de puertos de forma rápida y sencilla es Nmap “Network Mapper” o Mapeador de Puertos, la cual ofrece una gran variedad de técnicas que permiten el envío de sondas TCP SYN/ACK, UDP e ICMP a múltiples puertos de la red con el propósito de estas de solicitar respuestas que demuestren que una dirección IP está siendo utilizada por un equipo activo de red. Existen muchas técnicas de sondeo en base al tipo de escaneo que se desee realizar y las opciones que se desee obtener, para el presente caso se utilizará la técnica de análisis TCP SYN que permita identificar puertos abiertos, para obtener información de servicio utilizado.

Sintaxis Utilizada:

Nmap [Tipo de análisis] [Opciones] {IP Víctima}

Nmap –sS –sV *IP destino

- **Nikto**

Nikto es una herramienta gratuita de escaneo de vulnerabilidades web, permite realizar pruebas completas contra servidores web por varios elementos, entre ellos archivos potencialmente peligrosos, ficheros de instalaciones por defecto, controles de versiones, la presencia de archivos txt, csv, html, etc., opciones de servidor HTTP entre otras pruebas, que permiten identificar los servidores web instalados y el software utilizado. Para ejecutar la herramienta se hace uso de una instrucción sencilla que el host o equipo objetivo y el puerto deseado, en caso de no identificar el puerto Nikto utiliza por defecto el puerto 80.

Sintaxis Utilizada:

Nikto -h [IP Víctima] –p [Puerto]

Nikto -h *IP destino -p 80

- **THC-Hydra**

Es una herramienta utilizada para realizar ataques de fuera bruta contra servicios del sistema de manera remota, permite obtener el usuario y contraseña para ingresar al mismo y medir el nivel de facilidad con que se puede obtener acceso no autorizado hacia un sistema de red. Utiliza muchos protocolos como telnet, ftp, ssh, http, https, http-proxy, smb, smbnt, ms-sql, mysql, rexec, rsh, rlogin, cvs, snmp, smtp-auth, socks5, vnc, pop3, imap, nntp, pcnfs, icq, etc., a través de los cuales realiza los intentos de conexión en base a diccionarios de usuarios y contraseñas generados por archivos de textos o por programas especializados. En este caso para lanzar ataque contra un servidor utilizaremos el servicio SSH y para la creación automática de un

diccionario de contraseñas se utilizará la herramienta crunch, que generará contraseñas con un tamaño mínimo y máximo de 3 caracteres.

Sintaxis Utilizada:

Hydra -L [diccionario usuarios] –P [diccionario contraseñas] {IP Víctima} [protocolo] [opciones]

Hydra -L user_wordlist –P pass_wordlist *IP destino ssh –f -vV

- **Open VAS**

Como se ha indicado en capítulos anteriores Open VAS es una de las principales herramientas utilizadas por OSSIM, que permite realizar un análisis de vulnerabilidades y control de accesos. Para los administradores de red es importante conocer su manejo.

Por tanto, nos permite analizar un PC o un servidor local/remoto y realizar varios tipos de informes sobre las vulnerabilidades detectadas. También añade un motor de correlación para cruzar todo lo que se ha identificado/detectado y proponer soluciones asociadas. Open VAS funciona principalmente con 3 servicios:

- Un servicio de escaneo (scanner), quien se encarga de realizar los análisis de las vulnerabilidades.
- Un servicio cliente, utilizado como interfaz gráfico (web) necesario para configurar Open VAS y presentar los resultados obtenidos o la ejecución de informes.
- Un servicio manager, que mediante el OMP (Open VAS Management Protocol) es el encargado de interactuar con todos los módulos (Scanner, Cliente, Framework, CLI).

A continuación, en las figuras 244 a 250 se muestran las pantallas de ejecución de los distintos ataques descritos anteriormente, cada uno de ellos en base a la sintaxis especificada.

- **Ataque a Servidor OSSIM - NMAP (Escaneo de Puertos)**

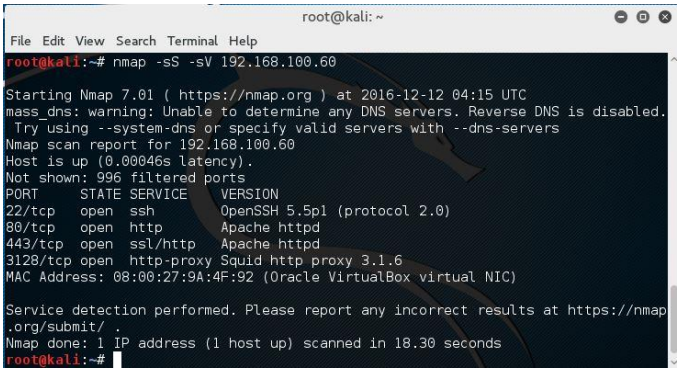


Figura 244 Ataque NMAP ejecutado hacia servidor OSSIM

- **Ataque a Servidor OSSIM – Nikto (Análisis de vulnerabilidades web)**

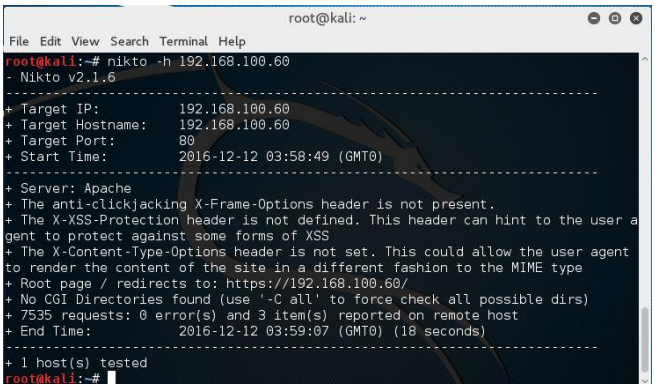


Figura 245 Ataque Nikto ejecutado hacia servidor OSSIM

- **Ataque a Servidor OSSIM – THC-Hydra (Fuerza Bruta)**

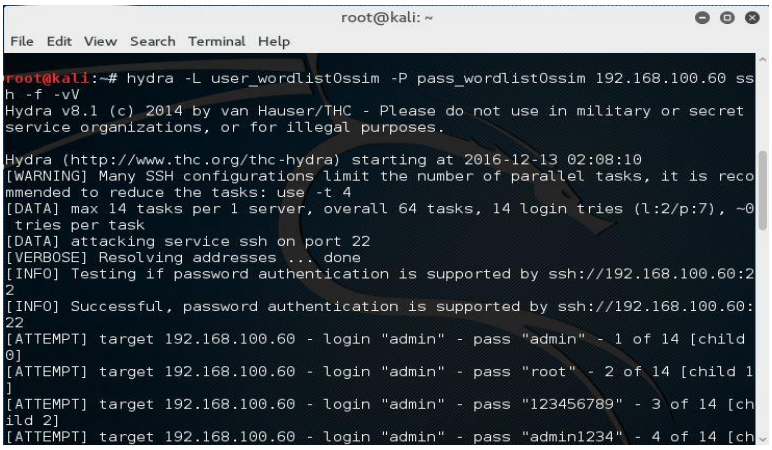


Figura 246 Ataque TCH-Hydra ejecutado hacia servidor OSSIM

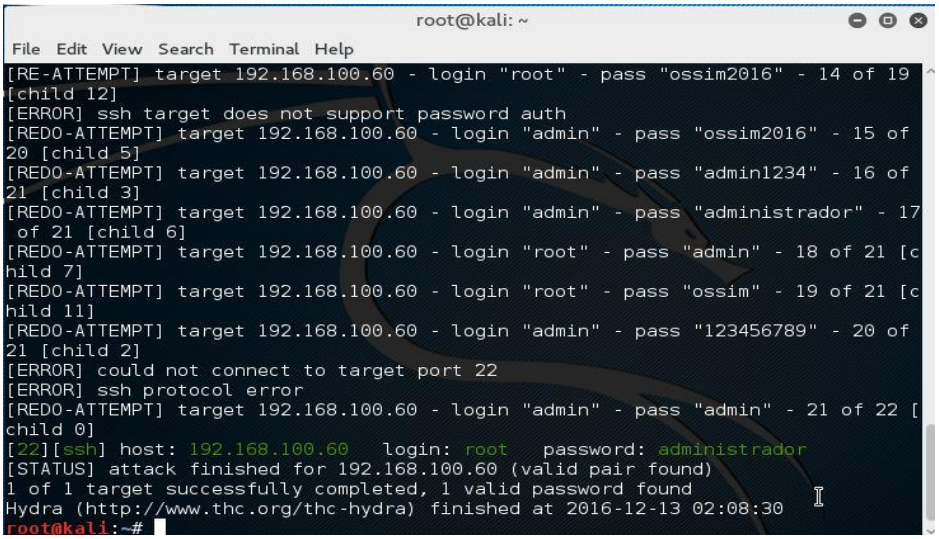


Figura 247 Ataque Hydra ejecutado hacia servidor OSSIM

- **Ataque a Servidor Ubuntu – THC-Hydra (Fuerza Bruta)**

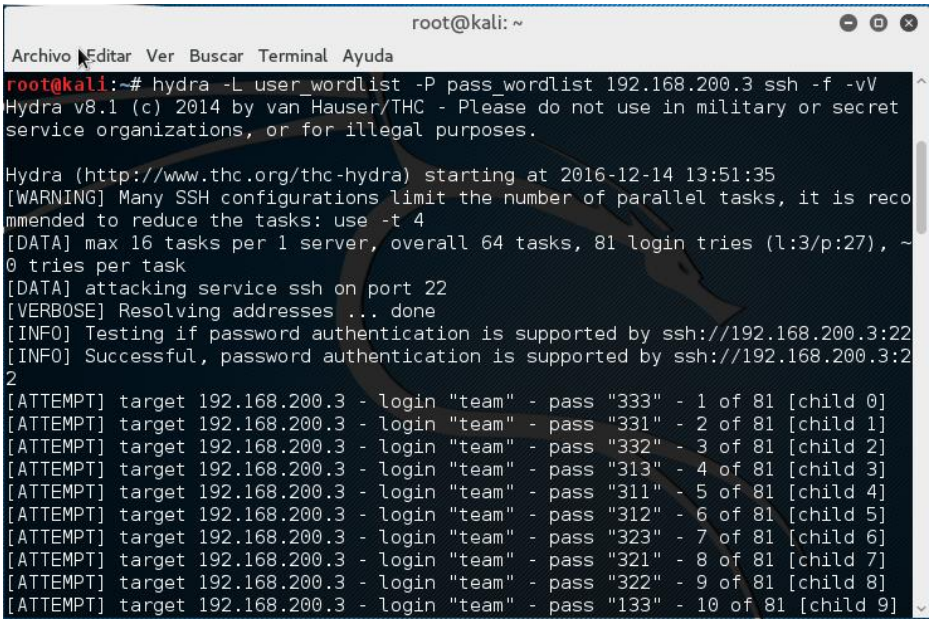


Figura 248 Ataque Hydra ejecutado hacia servidor Ubuntu

- **Ataque a Ubuntu-Server – Open VAS (Análisis de vulnerabilidades)**

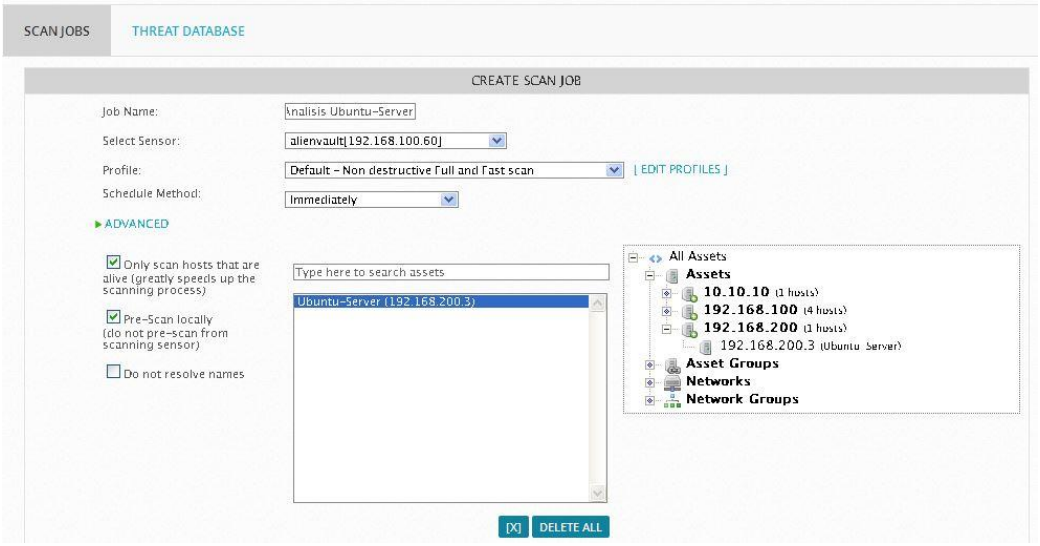


Figura 249 Ataque Open Vas ejecutado hacia servidor Ubuntu

- **Ataque a Windows-Server – Open VAS (Análisis de vulnerabilidades)**

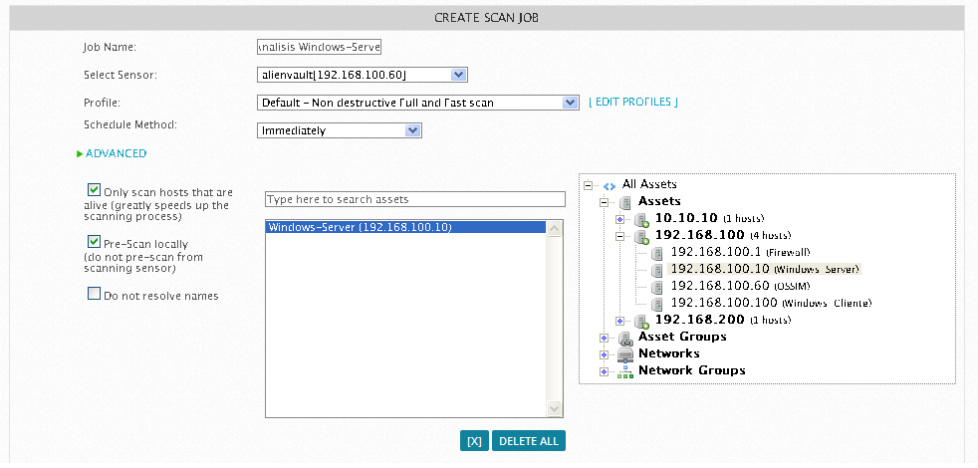


Figura 250 Ataque Open Vas ejecutado hacia servidor Windows

4.2. Procesamiento y Correlación de Eventos SIEM

Una vez ejecutados cada uno de los ataques propuestos, a través del módulo “Security Events (SIEM)” de OSSIM que es el encargado de mostrar en tiempo real o de forma histórica todos los eventos que son recolectados y

procesados por la herramienta de gestión, podremos observar los logs generados por los distintos agentes durante la ejecución de los ataques. En este caso del sin número de eventos dados en cada uno de los ataques nos centraremos principalmente en aquellos que presentan algún tipo de riesgo y que han sido procesados como Directivas de Correlación de Eventos, para posteriormente realizar un análisis detallado de los campos que lo conforman.

4.2.1. Eventos generados durante el ataque NMAP (Escaneo de Puertos) hacia el Servidor OSSIM

En la Figura 251 podemos observar los eventos registrados durante la ejecución del ataque NMAP relacionados con directivas propias del sistema de gestión OSSIM y en la Figura 252 y se muestra la directiva identificada.

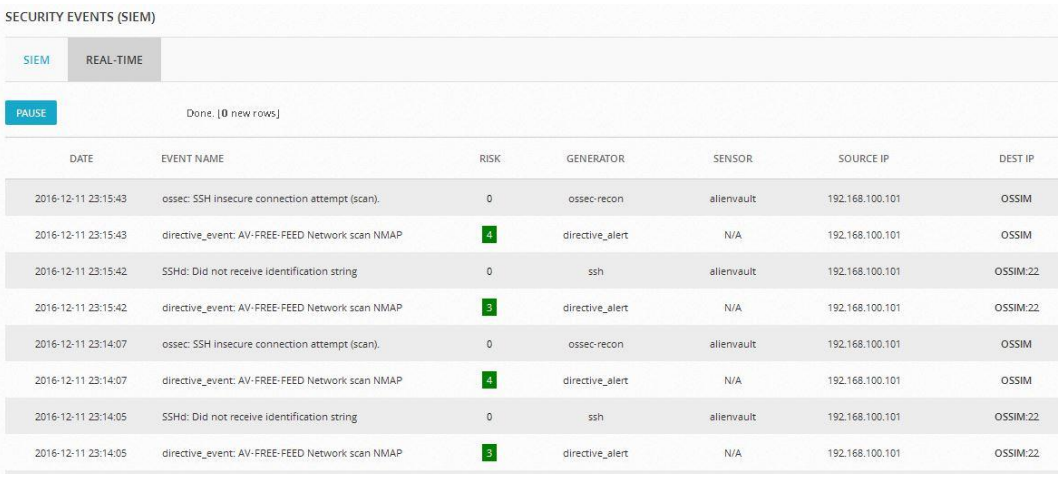


Figura 251 Procesamiento de Eventos en Tiempo Real

Figura 252 Directiva de Correlación de Eventos

4.2.2. Eventos generados durante el ataque Nikto (Análisis de vulnerabilidades web) hacia el Servidor OSSIM

En la Figura 253 podemos observar los eventos registrados durante la ejecución del ataque Nikto relacionados con directivas propias del sistema de gestión OSSIM y en la Figura 254 y se muestra la directiva identificada.

DATE	EVENT NAME	RISK	GENERATOR	SENSOR	SOURCE IP	DEST IP
2016-12-12 21:17:13	directive_event: AV-FREE-FEED Network scan, Nikto	4	directive_alert	N/A	192.168.100.101:45118	OSSIM:80
2016-12-12 21:17:13	directive_event: AV-FREE-FEED Network scan, Nikto	4	directive_alert	N/A	192.168.100.101:45118	OSSIM:80
2016-12-12 21:17:13	snort: "ET WEB_SERVER ColdFusion administrator access"	0	snort	alienvault	192.168.100.101:45398	OSSIM:80
2016-12-12 21:17:13	snort: "ET WEB_SERVER ColdFusion administrator access"	0	snort	alienvault	192.168.100.101:45398	OSSIM:80
2016-12-12 21:17:13	directive_event: AV-FREE-FEED Network scan, Nikto	3	directive_alert	N/A	192.168.100.101:45398	OSSIM:80
2016-12-12 21:17:13	directive_event: AV-FREE-FEED Network scan, Nikto	3	directive_alert	N/A	192.168.100.101:45398	OSSIM:80
2016-12-12 21:17:13	directive_event: AV-FREE-FEED Network scan, Nikto	3	directive_alert	N/A	192.168.100.101:45398	OSSIM:80

Figura 253 Procesamiento de Eventos en Tiempo Real – parte 1

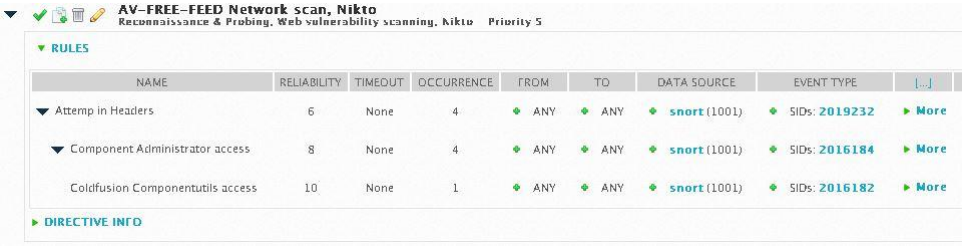


Figura 254 Directiva de Correlación de Eventos

4.2.3. Eventos generados durante el ataque de fuerza bruta THC-Hydra al Servidor OSSIM

En la Figura 255 podemos observar los eventos registrados durante la ejecución del ataque Hydra relacionados con directivas propias del sistema de gestión OSSIM y en la Figura 256 y se muestra la directiva identificada.

DATE	EVENT NAME	RISK	GENERATOR	SENSOR	SOURCE IP	DEST IP
2016-12-12 21:18:45	snort: "ET WEB_SERVER ColdFusion administrator access"	0	snort	alienvault	192.168.100.101:45398	OSSIM:80
2016-12-12 21:18:45	snort: "ET WEB_SERVER ColdFusion administrator access"	0	snort	alienvault	192.168.100.101:45398	OSSIM:80
2016-12-12 21:18:45	snort: "ET WEB_SERVER ColdFusion administrator access"	0	snort	alienvault	192.168.100.101:45398	OSSIM:80
2016-12-12 21:18:45	snort: "ET WEB_SERVER ColdFusion administrator access"	0	snort	alienvault	192.168.100.101:45398	OSSIM:80
2016-12-12 21:18:45	directive_event: AV-FREE-FEED Network scan, Nikto	3	directive_alert	N/A	192.168.100.101:45398	OSSIM:80
2016-12-12 21:18:45	directive_event: AV-FREE-FEED Network scan, Nikto	3	directive_alert	N/A	192.168.100.101:45398	OSSIM:80
2016-12-12 21:18:45	directive_event: AV-FREE-FEED Network scan, Nikto	3	directive_alert	N/A	192.168.100.101:45398	OSSIM:80

Figura 255 Procesamiento de Eventos en Tiempo Real

AV-FREE-FEED Bruteforce attack, SSH authentication attack against DST_IP
Delivery & Attack, Bruteforce Authentication, SSH Priority 5

RULES

NAME	RELIABILITY	TIMEOUT	OCCURRENCE	FROM	TO	DATA SOURCE	EVENT TYPE	[...]
Attempts to loggin using a non-existing user	6	None	1	ANY	ANY	ossec-authentication_failed (7010)	SIDs: 5710	More
SSHD authentication failed	8	None	1	ANY:1:SRC_PORT	ANY	ossec-authentication_failed (7010)	SIDs: 5716	More
SSH service authentication successful detected	10	None	1	ANY:1:SRC_PORT	ANY	ossec-authentication_success (7009)	SIDs: 5715	More

Figura 256 Directiva de Correlación de Eventos

4.2.4. Eventos generados durante el ataque de fuerza bruta THC-Hydra al Servidor Ubuntu

En la Figura 257 podemos observar los eventos registrados durante la ejecución del ataque Hydra relacionados con directivas propias del sistema de gestión OSSIM y en la Figura 258 y se muestra la directiva identificada.

DATE	EVENT NAME	RISK	GENERATOR	SENSOR	SOURCE IP	DEST IP
2016-12-13 22:34:54	ossec: Login session opened.	0	ossec-authentication_success	alienvault	Ubuntu-Server	Ubuntu-Server
2016-12-13 22:34:54	ossec: SSHD authentication success.	0	ossec-authentication_success	alienvault	192.168.200.101:49550	Ubuntu-Server
2016-12-13 22:34:54	directive_event: AV-FREE-FEED Bruteforce attack, SSH authentication attack against DST_IP	4	directive_alert	N/A	192.168.100.101:33754	Ubuntu-Server
2016-12-13 22:34:22	ossec: Login session closed.	0	ossec-syslog	alienvault	Ubuntu-Server	Ubuntu-Server
2016-12-13 22:34:22	ossec: SSHD authentication failed.	0	ossec-authentication_failed	alienvault	192.168.100.101:33770	Ubuntu-Server
2016-12-13 22:34:22	ossec: SSHD authentication failed.	0	ossec-authentication_failed	alienvault	192.168.100.101:33754	Ubuntu-Server
2016-12-13 22:34:22	directive_event: AV-FREE-FEED Bruteforce attack, SSH authentication attack against DST_IP	3	directive_alert	N/A	192.168.100.101:33754	Ubuntu-Server
2016-12-13 22:34:22	directive_event: AV-FREE-FEED Bruteforce attack, SSH authentication attack against DST_IP	3	directive_alert	N/A	192.168.100.101:33754	Ubuntu-Server
2016-12-13 22:34:22	directive_event: AV-FREE-FEED Bruteforce attack, SSH authentication attack against DST_IP	3	directive_alert	N/A	192.168.100.101:33754	Ubuntu-Server

Figura 257 Procesamiento de Eventos en Tiempo Real

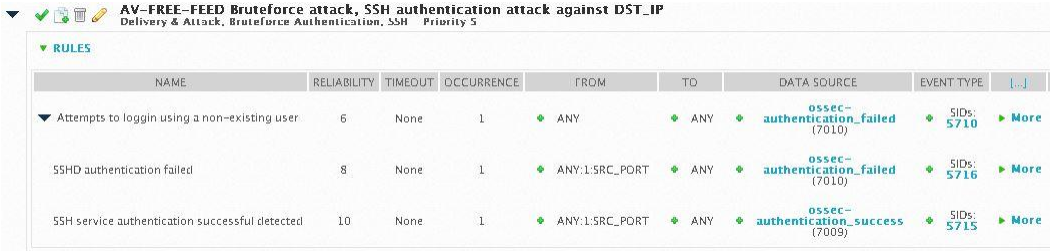


Figura 258 Directiva de Correlación de Eventos

4.2.5. Eventos generados durante el ataque o análisis de vulnerabilidades Open VAS al Servidor Ubuntu

En la figura 259 podemos observar los eventos registrados durante la ejecución del ataque Open VAS relacionados con directivas propias del sistema de gestión OSSIM y en la figura 260 y se muestra la directiva identificada.

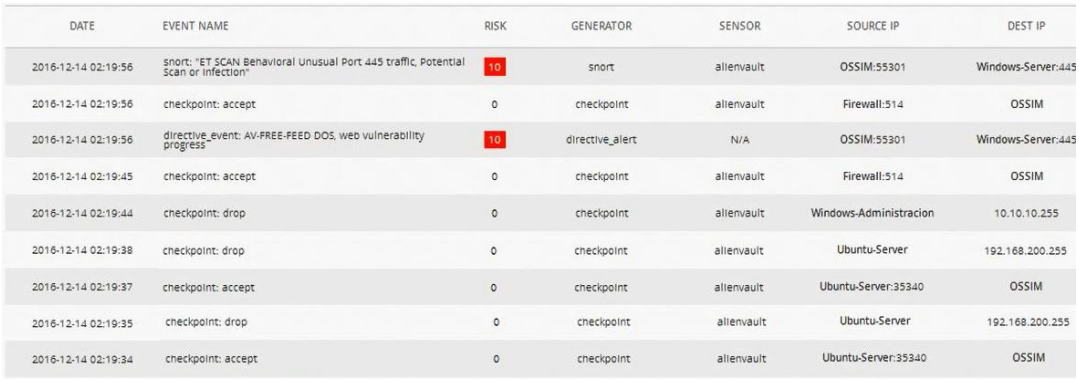
DATE	EVENT NAME	RISK	GENERATOR	SENSOR	SOURCE IP	DEST IP
2016-12-14 02:00:30	snort: "ET DOS Possible SSDP Amplification Scan In Progress"	10	snort	alienvault	OSSIM:2042	Ubuntu-Server:1900
2016-12-14 02:00:30	checkpoint: accept	0	checkpoint	alienvault	OSSIM:41557	Ubuntu-Server
2016-12-14 02:00:30	directive_event: AV-FREE-FEED DOS, web vulnerability progress	10	directive_alert	N/A	OSSIM:2042	Ubuntu-Server:1900
2016-12-14 02:00:22	checkpoint: accept	0	checkpoint	alienvault	OSSIM:41571	Ubuntu-Server
2016-12-14 02:00:22	checkpoint: accept	0	checkpoint	alienvault	OSSIM:56426	Ubuntu-Server
2016-12-14 02:00:22	checkpoint: accept	0	checkpoint	alienvault	OSSIM:41557	Ubuntu-Server
2016-12-14 02:00:22	checkpoint: accept	0	checkpoint	alienvault	OSSIM:41559	Ubuntu-Server
2016-12-14 02:00:22	checkpoint: accept	0	checkpoint	alienvault	OSSIM:41560	Ubuntu-Server
2016-12-14 02:00:22	checkpoint: accept	0	checkpoint	alienvault	OSSIM:41561	Ubuntu-Server
2016-12-14 02:00:22	checkpoint: accept	0	checkpoint	alienvault	OSSIM:41562	Ubuntu-Server

Figura 259 Procesamiento de Eventos en Tiempo Real

Figura 260 Directiva de Correlación de Eventos

4.2.6. Eventos generados durante el ataque o análisis de vulnerabilidades Open VAS al Servidor Windows

En la Figura 261 podemos observar los eventos registrados durante la ejecución del ataque Open VAS relacionados con directivas propias del sistema de gestión OSSIM y en la Figura 262 y se muestra la directiva identificada.



DATE	EVENT NAME	RISK	GENERATOR	SENSOR	SOURCE IP	DEST IP
2016-12-14 02:19:56	snort: "ET SCAN Behavioral Unusual Port 445 traffic, Potential Scan or Infection"	10	snort	alienvault	OSSIM:55301	Windows-Server:445
2016-12-14 02:19:56	checkpoint: accept	0	checkpoint	alienvault	Firewall:514	OSSIM
2016-12-14 02:19:56	directive_event: AV-FREE-FEED DOS, web vulnerability progress	10	directive_alert	N/A	OSSIM:55301	Windows-Server:445
2016-12-14 02:19:45	checkpoint: accept	0	checkpoint	alienvault	Firewall:514	OSSIM
2016-12-14 02:19:44	checkpoint: drop	0	checkpoint	alienvault	Windows-Administracion	10.10.10.255
2016-12-14 02:19:38	checkpoint: drop	0	checkpoint	alienvault	Ubuntu-Server	192.168.200.255
2016-12-14 02:19:37	checkpoint: accept	0	checkpoint	alienvault	Ubuntu-Server:35340	OSSIM
2016-12-14 02:19:35	checkpoint: drop	0	checkpoint	alienvault	Ubuntu-Server	192.168.200.255
2016-12-14 02:19:34	checkpoint: accept	0	checkpoint	alienvault	Ubuntu-Server:35340	OSSIM

Figura 261 Procesamiento de Eventos en Tiempo Real

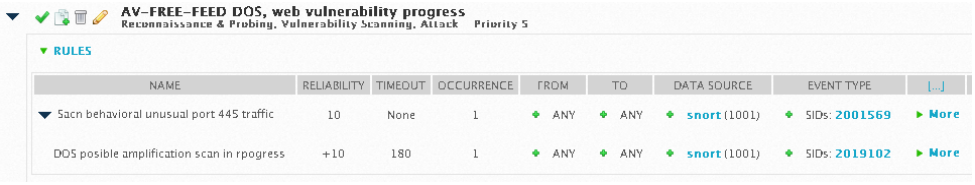


Figura 262 Directiva de Correlación de Eventos

4.3. Visualización de Resultados

OSSIM es una herramienta de gestión de eventos muy completa, que nos ofrece una consola de gestión gráfica con una visión general de los eventos producidos en el sistema de red. En la Figura 263, se ilustra el Dashboard también conocido como Tablero de Control que permite tener una visualización gráfica de las estadísticas de eventos de seguridad producidos en la red de la organización.

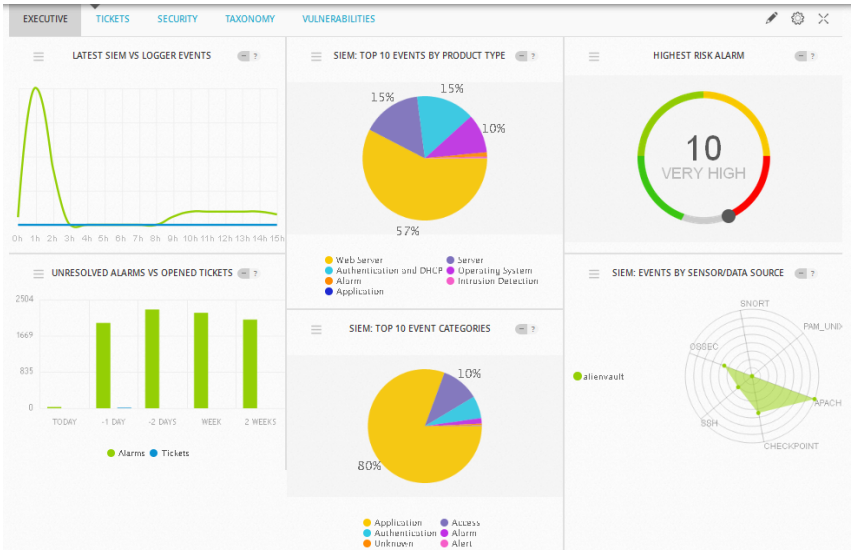


Figura 263 Dashboard OSSIM - Tableros de Control

Este Tablero de Control puede ser editable según las necesidades del administrador de red, cada una de las 6 secciones mostradas en la figura xx nos tiene información relevante de sucesos registrados por el sistema de gestión. A continuación, se cada sección.

- **Lastest SIEM vs Logger Events**

En la Figura 264 se muestra los últimos eventos producidos en un período de tiempo de 24 horas de los eventos del SIEM versus los eventos del Logger, en este caso el componente Logger no está habilitado en el OSSIM.

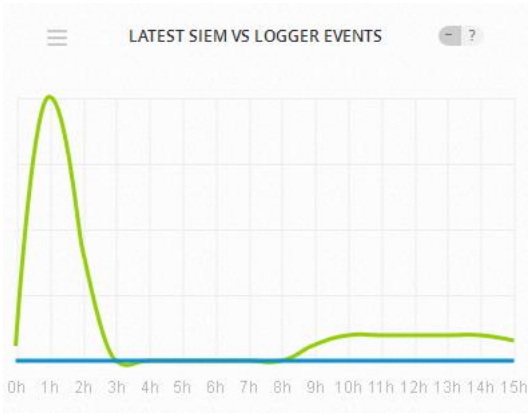


Figura 264 Lastest SIEM vs Logger Events

- **TOP 10 Events by product type**

En la Figura 265 se muestra un gráfico estadístico correspondiente a los 10 eventos registrados en mayor número de veces, divididos por colores según su tipo. Al presionar cada uno de ellos la herramienta los lleva al registro histórico donde se almacenan y se muestra detalladamente cada uno de los campos como, Fecha, IP origen, IP destino, y Riesgo.

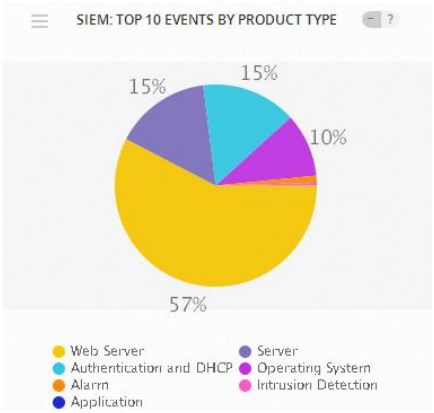


Figura 265 TOP 10 Events by product type

- **Highest Risk Alarm**

En la Figura 266 se muestra un gráfico estadístico que muestra la alarma de mayor riesgo, muestra un valor entero entre de 0 a 10 que se basa en el mayor riesgo de todas las alarmas abiertas que fueron encontradas en el sistema, el riesgo de un evento se calcula a través de la fórmula *Riesgo = (Valor del activo * Prioridad del evento * Fiabilidad del evento) / 25.* OSSIM en base al resultado obtenido de la fórmula de riesgo asignar las siguientes categorías de riesgo:

Color/Riesgo	Valor
Muy Alto	9, 10
Alto	7, 8
Elevado	5, 6
Precaución	3, 4
Bajo	0, 1, 2

Figura 266 Highest Risk Alarm

- **Unresolved Alarms**

La Figura 267, muestra las alarmas que se generaron en las dos últimas semanas y los tickets abiertos asociados a dichas alarmas.

Figura 267 Unresolved alarms vs opened tickets

- **SIEM Top 10 Event Categories**

En el siguiente gráfico se muestra el Top 10 de los eventos que más se han generado, para poder visualizarlos o tener un mayor detalle se debe dar clic en el tipo de evento deseado.

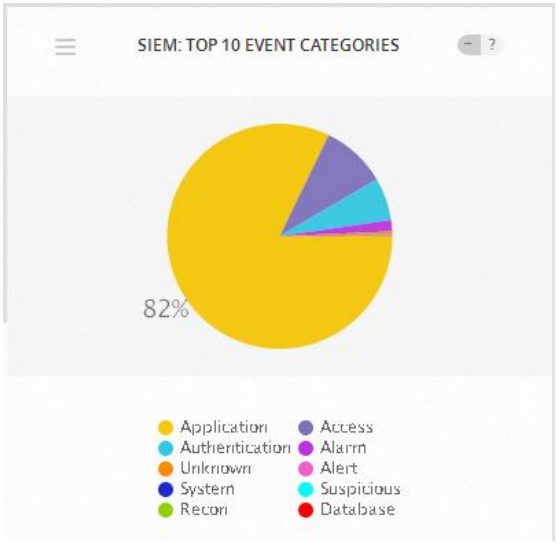


Figura 268 SIEM TOP 20 Event Categories

- **Events by Sensor/Data Source**

En la Figura 269, se muestra los eventos por el tipo de sensor u origen de datos, se puede apreciar que existen eventos producidos por el equipo de seguridad perimetral Checkpoint, agente OSSEC, SSH, Apache, entre los más principales.

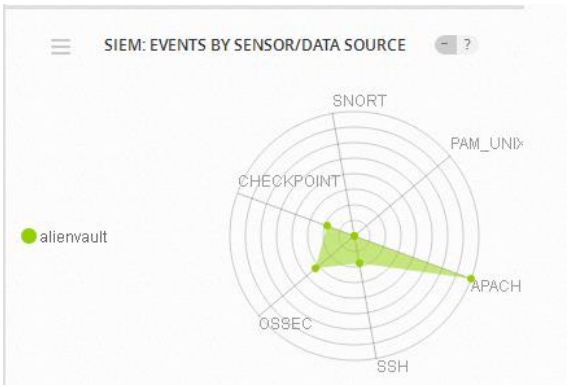


Figura 269 SIEM Events By Sensor

4.4. Detección y Análisis de Eventos

La sección de Alarmas de Alto Riesgo nos muestra la cantidad de alarmas y su criticidad, para realizar un análisis detallado, se debe ingresar a cada una de ellas haciendo clic en esta sección como se indica en la Figura 270; en este caso se analizarán las alarmas generadas por los diferentes ataques externos como se detalla a continuación:

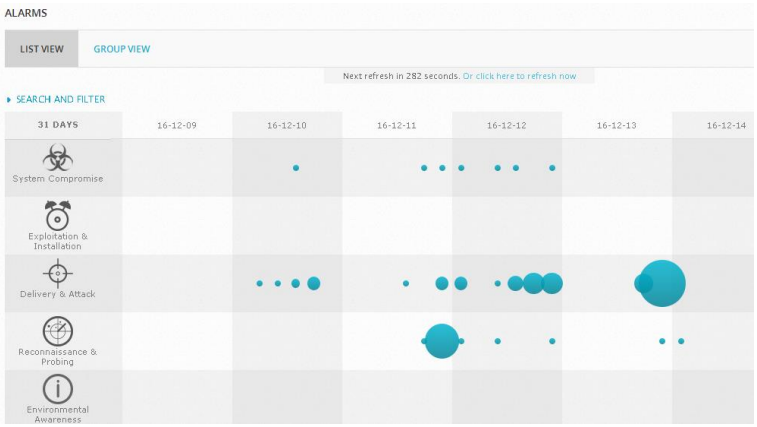


Figura 270 Vista de Alarmas reflejadas en el sistema

Seleccionamos la opción Group view como se ilustra en la Figura 271:

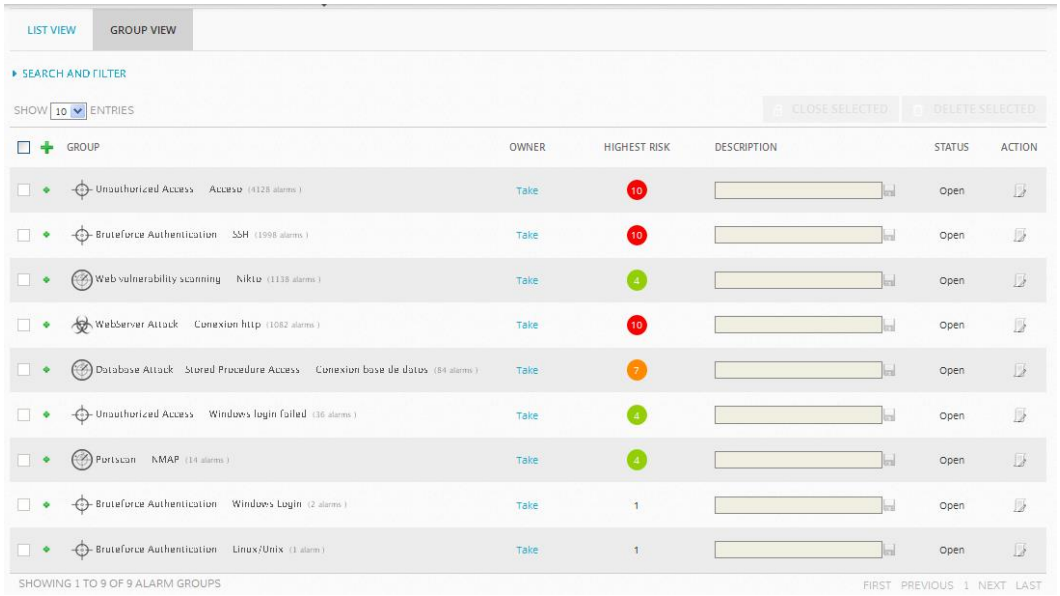


Figura 271 Alarmas Filtradas por Grupos

Filtramos la búsqueda mediante los parámetros deseados en los campos deseados:

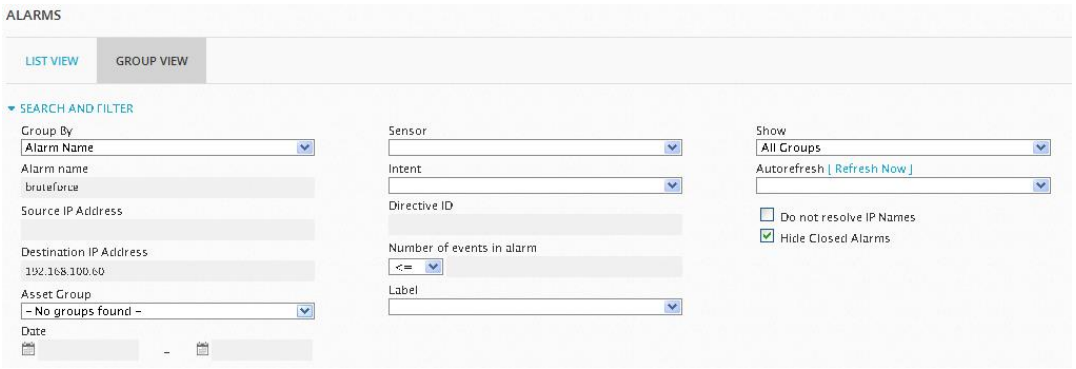


Figura 272 Campos de búsqueda de una alarma

Al ejecutar los distintos ataques planteados se generaron un sin número de eventos que activaron varias alarmas del sistema a continuación se observa en detalle cada una de acuerdo al tipo de ataque:

- **Ataque a Servidor OSSIM - NMAP (Escaneo de Puertos)**

	ALARM NAME	EVENTS	RISK	DURATION	SOURCE	DESTINATION	STATUS
◆	Reconnaissance & Probing — Portscan — NMAP	2	4	1 sec	192.168.100.101	OSSIM	Open
◆	Reconnaissance & Probing — Portscan — NMAP	2	4	1 sec	192.168.100.101	OSSIM	Open
◆	Reconnaissance & Probing — Portscan — NMAP	2	4	2 secs	192.168.100.101	OSSIM	Open
◆	Reconnaissance & Probing — Portscan — NMAP	2	4	1 sec	192.168.100.101	OSSIM	Open
◆	Reconnaissance & Probing — Portscan — NMAP	2	4	0 secs	192.168.1.101	OSSIM	Open

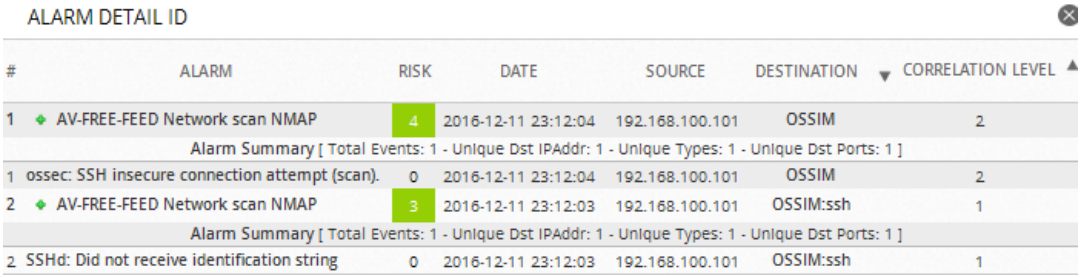
Figura 273 Evento Generado

Se despliega el detalle de una alarma en la Figura 273 y 274:

	Reconnaissance & Probing — Portscan — NMAP	2	4	1 sec	192.168.100.101	OSSIM	Open
#	ALARM	RISK	DATE	SOURCE	DESTINATION	CORRELATION LEVEL	
2	◆ AV-FREE-FEED Network scan NMAP	3	2016-12-11 23:12:03	192.168.100.101	OSSIM:ssh	1	
	Alarm Summary [Total Events: 1 - Unique Dst IPAddr: 1 - Unique Types: 1 - Unique Dst Ports: 1]						
1	◆ AV-FREE-FEED Network scan NMAP	4	2016-12-11 23:12:04	192.168.100.101	OSSIM	2	

Figura 274 Detalle de Alarma

Haciendo clic en la sección izquierda se visualiza la fuente u origen que produjo el evento y generó la alarma, para este caso se muestra que existe una correlación de eventos SIEM de nivel 2 generados por OSSEC y SSH como se muestra en la Figura 275.



ALARM DETAIL ID

#	ALARM	RISK	DATE	SOURCE	DESTINATION	CORRELATION LEVEL
1	◆ AV-FREE-FEED Network scan NMAP	4	2016-12-11 23:12:04	192.168.100.101	OSSIM	2
	Alarm Summary [Total Events: 1 - Unique Dst IPAddr: 1 - Unique Types: 1 - Unique Dst Ports: 1]					
1	ossec: SSH insecure connection attempt (scan).	0	2016-12-11 23:12:04	192.168.100.101	OSSIM	2
2	◆ AV-FREE-FEED Network scan NMAP	3	2016-12-11 23:12:03	192.168.100.101	OSSIM:ssh	1
	Alarm Summary [Total Events: 1 - Unique Dst IPAddr: 1 - Unique Types: 1 - Unique Dst Ports: 1]					
2	SSHd: Did not receive identification string	0	2016-12-11 23:12:03	192.168.100.101	OSSIM:ssh	1

Figura 275 Detalle de Alarma

Para visualizar la estructura la regla se tiene que hacer clic en el evento:

```
directive_event: AV-FREE-FEED Network scan NMAP, Priority: 5 Rule 1
[2016-12-12 04:12:03] [4003:10] [Rel: 8] 192.168.100.101:0 ->
192.168.100.60:22 Rule 2 [2016-12-12 04:12:04] [7014:5706] [Rel: 10]
192.168.100.101:0 -> 192.168.100.60:0
```

Por último, se genera un ticket como se muestra en la Figura 276, para su posterior tratamiento y seguimiento a su resolución:

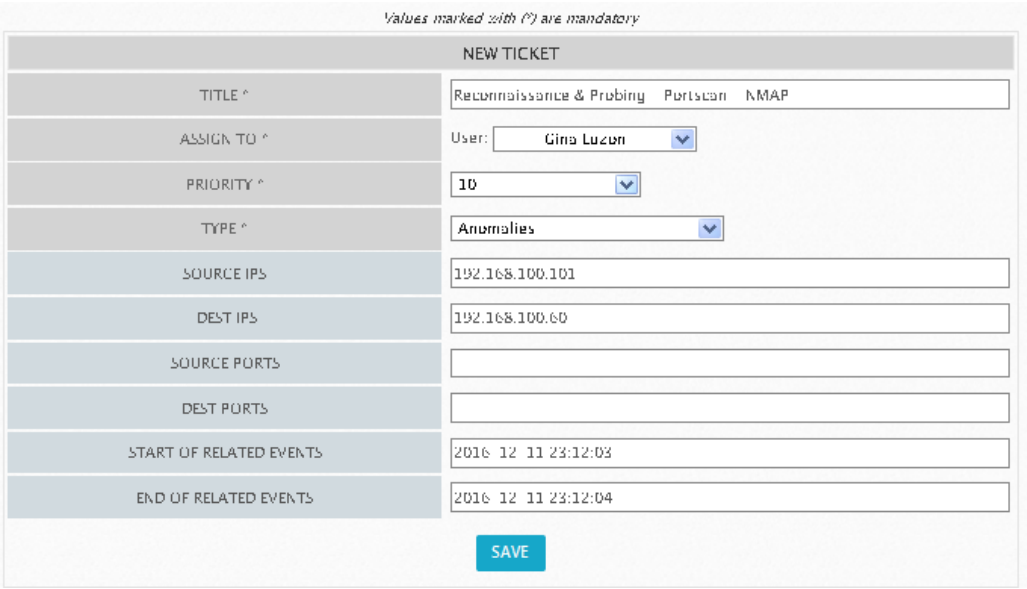


Figura 276 Generación ticket

- **Ataque a Servidor OSSIM – Nikto (Análisis de vulnerabilidades web)**

Las alarmas generadas por este ataque fueron las siguientes:

Figura 277 Evento Generado

Se despliega el detalle de una alarma:

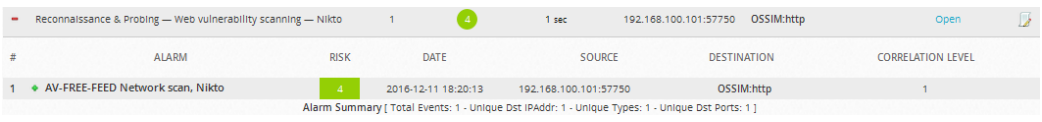


Figura 278 Detalle de Alarma

Haciendo clic en la sección izquierda se visualiza la fuente u origen que produjo el evento y generó la alarma, para este caso se muestra que existe una correlación de eventos SIEM de nivel 1 generado por SNORT, como se muestra en la Figura 279.

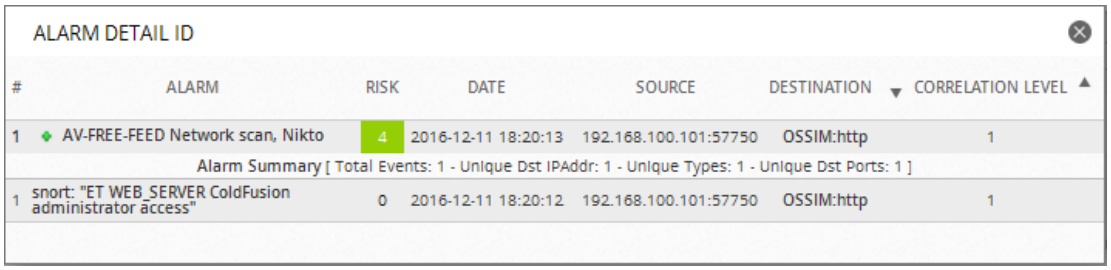


Figura 279 Detalle de Alarma

Para visualizar la estructura la regla se tiene que hacer clic en el evento:

directive_event: AV-FREE-FEED Network scan, Nikto, Priority: 5 Rule 1 [2016-12-11 23:20:13] [1001:2016184] [Rel: 10] 192.168.100.101:57750 -> 192.168.100.60:80

Por último, se genera un ticket para su posterior tratamiento y seguimiento a su resolución:

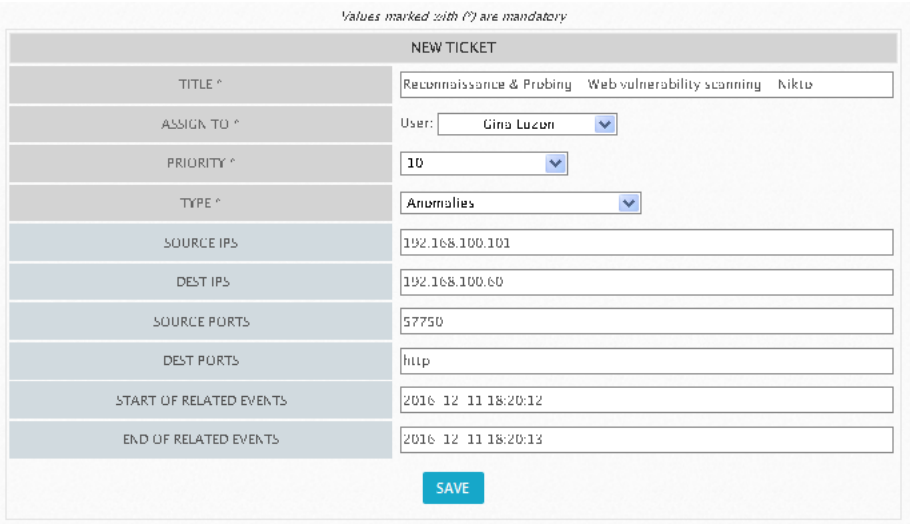


Figura 280 Generación ticket

- **Ataque a Servidor OSSIM – THC-Hydra (Fuerza Bruta)**

Figura 281 Evento Generado

Se despliega el detalle de una alarma:

Figura 282 Detalle de Alarma

Haciendo clic en la sección izquierda se visualiza la fuente u origen que produjo el evento y generó la alarma, para este caso se muestra que existe una correlación de eventos SIEM de nivel 2 generado por OSSEC.

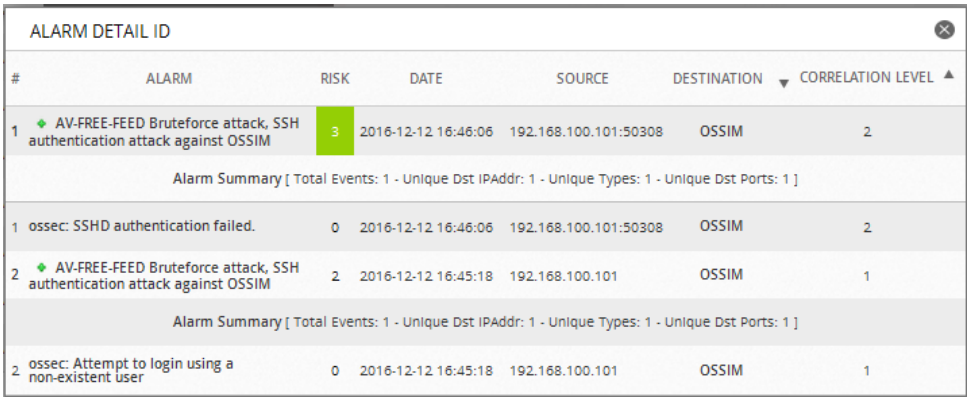


Figura 283 Detalle de Alarma

Para visualizar la estructura la regla se tiene que hacer clic en el evento:

directive_event: AV-FREE-FEED Bruteforce attack, SSH authentication attack against DST_IP, Priority: 5 Rule 1 [2016-12-12 21:45:18] [7010:5710] [Rel: 6] 192.168.100.101:0 -> 192.168.100.60:0 Rule 2 [2016-12-12 21:46:06] [7010:5716] [Rel: 8] 192.168.100.101:50308 -> 192.168.100.60:0

Por último, se genera un ticket para su posterior tratamiento y seguimiento a su resolución:

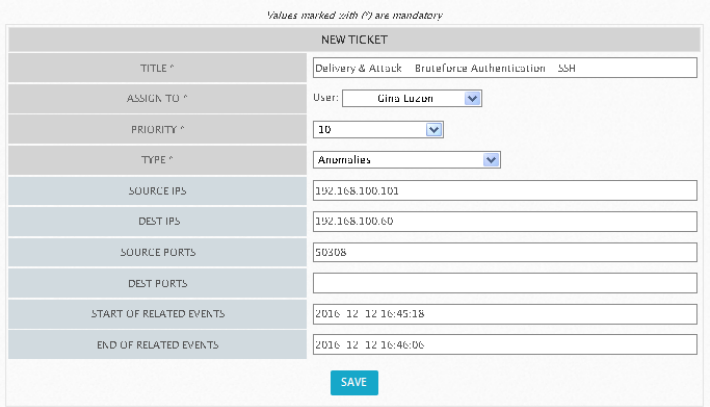


Figura 284 Generación ticket

- **Ataque a Servidor Ubuntu – THC-Hydra (Fuerza Bruta)**

Las alarmas generadas por este ataque fueron las siguientes:

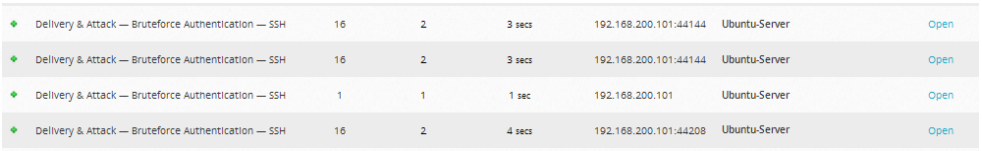


Figura 285 Evento Generado

Se despliega el detalle de una alarma:

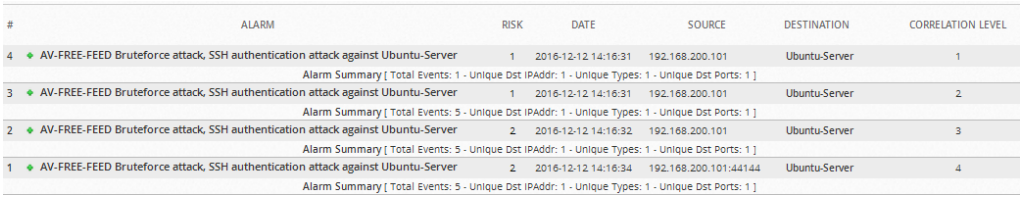
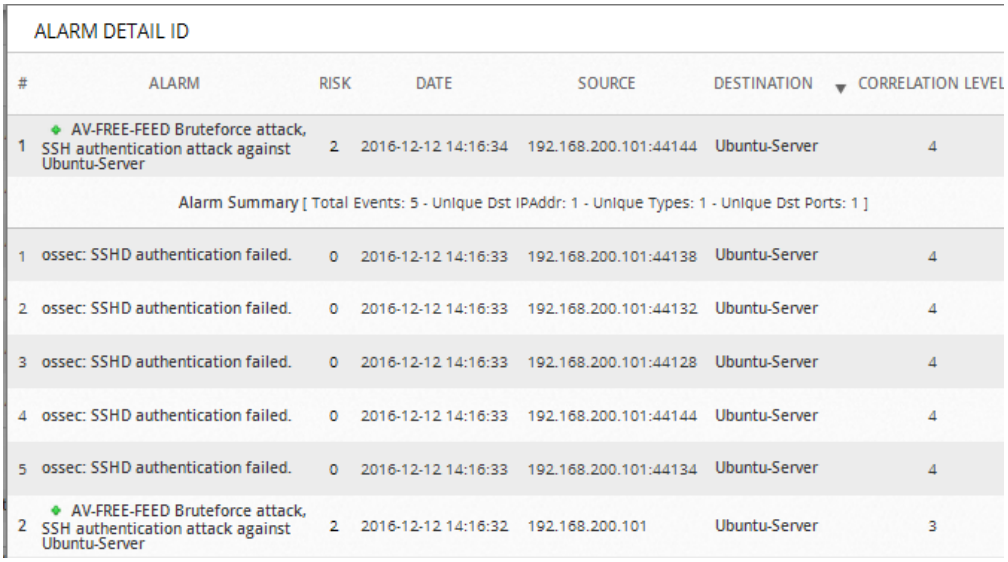


Figura 286 Detalle de Alarma

Haciendo clic en la sección izquierda se visualiza la fuente u origen que produjo el evento y generó la alarma, para este caso se muestra que existe una correlación de eventos SIEM de nivel 4 generado por OSSEC.



ALARM DETAIL ID

#	ALARM	RISK	DATE	SOURCE	DESTINATION	CORRELATION LEVEL
1	AV-FREE-FEED Bruteforce attack, SSH authentication attack against Ubuntu-Server	2	2016-12-12 14:16:34	192.168.200.101:44144	Ubuntu-Server	4
	Alarm Summary [Total Events: 5 - Unique Dst IPAddr: 1 - Unique Types: 1 - Unique Dst Ports: 1]					
1	ossec: SSHD authentication failed.	0	2016-12-12 14:16:33	192.168.200.101:44138	Ubuntu-Server	4
2	ossec: SSHD authentication failed.	0	2016-12-12 14:16:33	192.168.200.101:44132	Ubuntu-Server	4
3	ossec: SSHD authentication failed.	0	2016-12-12 14:16:33	192.168.200.101:44128	Ubuntu-Server	4
4	ossec: SSHD authentication failed.	0	2016-12-12 14:16:33	192.168.200.101:44144	Ubuntu-Server	4
5	ossec: SSHD authentication failed.	0	2016-12-12 14:16:33	192.168.200.101:44134	Ubuntu-Server	4
2	AV-FREE-FEED Bruteforce attack, SSH authentication attack against Ubuntu-Server	2	2016-12-12 14:16:32	192.168.200.101	Ubuntu-Server	3

Figura 287 Detalle de Alarma

Para visualizar la estructura la regla se tiene que hacer clic en el evento:

directive_event: AV-FREE-FEED Bruteforce attack, SSH authentication attack against DST_IP, Priority: 4 Rule 1 [2016-12-12 19:16:31] [7010:5710] [Rel: 5] 192.168.200.101:0 -> 192.168.200.3:0 Rule 2 [2016-12-12 19:16:31] [7010:5710] [Rel: 6] 192.168.200.101:0 -> 192.168.200.3:0 Rule 3 [2016-12-12 19:16:32] [7010:5710] [Rel: 7] 192.168.200.101:0 -> 192.168.200.3:0 Rule 4 [2016-12-12 19:16:34] [7010:5716] [Rel: 8] 192.168.200.101:44144 -> 192.168.200.3:0

Por último, se genera un ticket para su posterior tratamiento y seguimiento a su resolución:

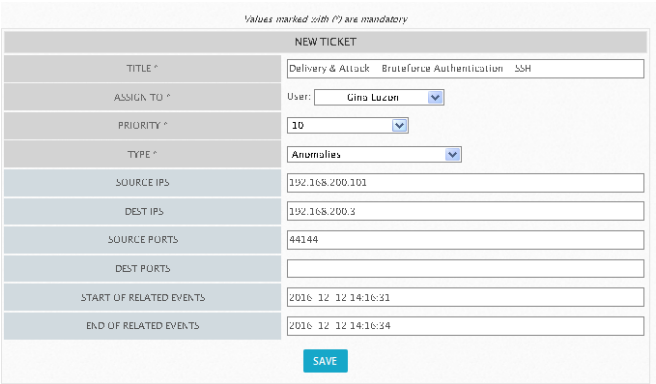
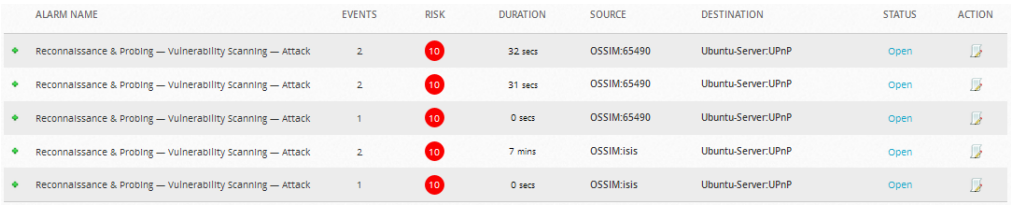


Figura 288 Generación ticket

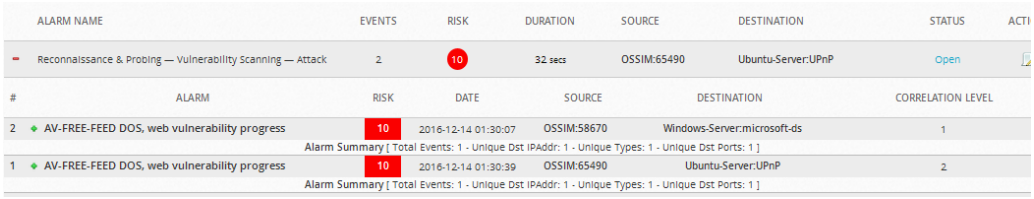
- **Ataque a Servidor Ubuntu – Open VAS (Análisis de vulnerabilidades)**



ALARM NAME	EVENTS	RISK	DURATION	SOURCE	DESTINATION	STATUS	ACTION
Reconnaissance & Probing — Vulnerability Scanning — Attack	2	10	32 secs	OSSIM:65490	Ubuntu-Server:UPnP	Open	
Reconnaissance & Probing — Vulnerability Scanning — Attack	2	10	31 secs	OSSIM:65490	Ubuntu-Server:UPnP	Open	
Reconnaissance & Probing — Vulnerability Scanning — Attack	1	10	0 secs	OSSIM:65490	Ubuntu-Server:UPnP	Open	
Reconnaissance & Probing — Vulnerability Scanning — Attack	2	10	7 mins	OSSIM:isis	Ubuntu-Server:UPnP	Open	
Reconnaissance & Probing — Vulnerability Scanning — Attack	1	10	0 secs	OSSIM:isis	Ubuntu-Server:UPnP	Open	

Figura 289 Evento Generado

Se despliega el detalle de una alarma:

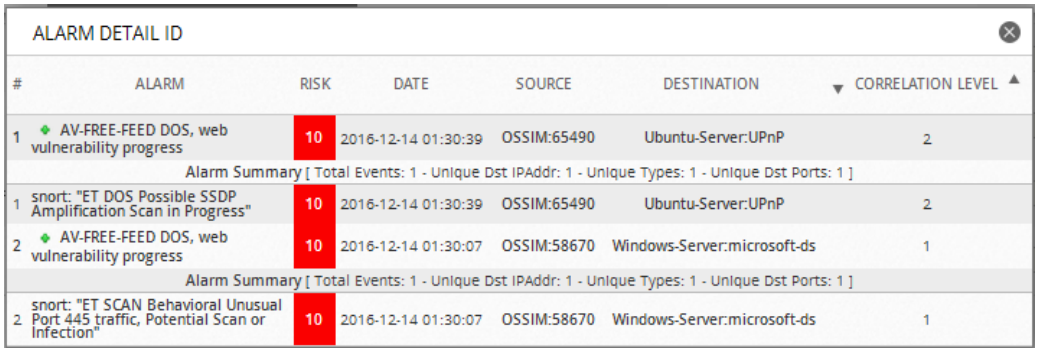


ALARM NAME	EVENTS	RISK	DURATION	SOURCE	DESTINATION	STATUS	ACTI
Reconnaissance & Probing — Vulnerability Scanning — Attack	2	10	32 secs	OSSIM:65490	Ubuntu-Server:UPnP	Open	

#	ALARM	RISK	DATE	SOURCE	DESTINATION	CORRELATION LEVEL
2	AV-FREE-FEED DOS, web vulnerability progress	10	2016-12-14 01:30:07	OSSIM:58670	Windows-Server:microsoft-ds	1
	Alarm Summary [Total Events: 1 - Unique Dst IPAddr: 1 - Unique Types: 1 - Unique Dst Ports: 1]					
1	AV-FREE-FEED DOS, web vulnerability progress	10	2016-12-14 01:30:39	OSSIM:65490	Ubuntu-Server:UPnP	2
	Alarm Summary [Total Events: 1 - Unique Dst IPAddr: 1 - Unique Types: 1 - Unique Dst Ports: 1]					

Figura 290 Detalle de Alarma

Haciendo clic en la sección izquierda se visualiza la fuente u origen que produjo el evento y generó la alarma, para este caso se muestra que existe una correlación de eventos SIEM de nivel 2 generados por OSSEC y SSH.



ALARM DETAIL ID

#	ALARM	RISK	DATE	SOURCE	DESTINATION	CORRELATION LEVEL
1	AV-FREE-FEED DOS, web vulnerability progress	10	2016-12-14 01:30:39	OSSIM:65490	Ubuntu-Server:UPnP	2
	Alarm Summary [Total Events: 1 - Unique Dst IPAddr: 1 - Unique Types: 1 - Unique Dst Ports: 1]					
1	snort: "ET DOS Possible SSDP Amplification Scan in Progress"	10	2016-12-14 01:30:39	OSSIM:65490	Ubuntu-Server:UPnP	2
2	AV-FREE-FEED DOS, web vulnerability progress	10	2016-12-14 01:30:07	OSSIM:58670	Windows-Server:microsoft-ds	1
	Alarm Summary [Total Events: 1 - Unique Dst IPAddr: 1 - Unique Types: 1 - Unique Dst Ports: 1]					
2	snort: "ET SCAN Behavioral Unusual Port 445 traffic, Potential Scan or Infection"	10	2016-12-14 01:30:07	OSSIM:58670	Windows-Server:microsoft-ds	1

Figura 291 detalle de Alarma

Para visualizar la estructura la regla se tiene que hacer clic en el evento:

directive_event: AV-FREE-FEED DOS, web vulnerability progress, Priority: 5 Rule 1 [2016-12-14 06:30:07] [1001:2001569] [Rel: 10] 192.168.100.60:58670 -> 192.168.100.10:445 Rule 2 [2016-12-14 06:30:39] [1001:2019102] [Rel: +10] 192.168.100.60:65490 -> 192.168.200.3:1900

Por último, se genera un ticket para su posterior tratamiento y seguimiento a su resolución:

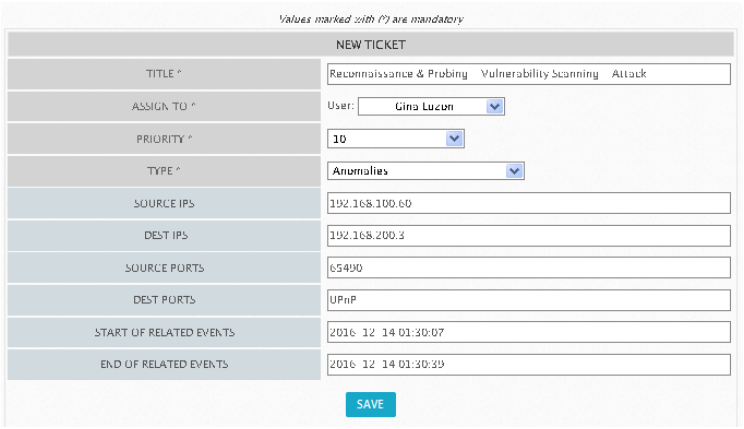


Figura 292 Generación ticket

- **Ataque a Windows-Server – Open VAS (Análisis de vulnerabilidades)**

Figura 293 Evento Generado

Se despliega el detalle de una alarma:

Figura 294 Detalle de Alarma

Haciendo clic en la sección izquierda se visualiza la fuente u origen que produjo el evento y generó la alarma, para este caso se muestra que existe una correlación de eventos SIEM de nivel 1 generados por SNORT.

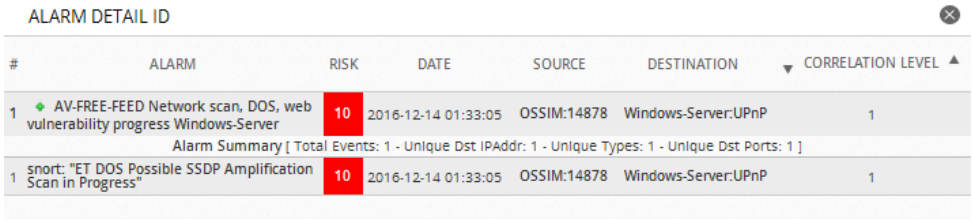


Figura 295 Detalle de Alarma

Para visualizar la estructura la regla se tiene que hacer clic en el evento:

directive_event: AV-FREE-FEED Network scan, DOS, web vulnerability progress DST_IP, Priority: 5 Rule 1 [2016-12-14 06:33:05] [1001:2019102] [Rel: 10] 192.168.100.60:14878 -> 192.168.100.10:1900

Por último, se genera un ticket para su posterior tratamiento y seguimiento a su resolución:

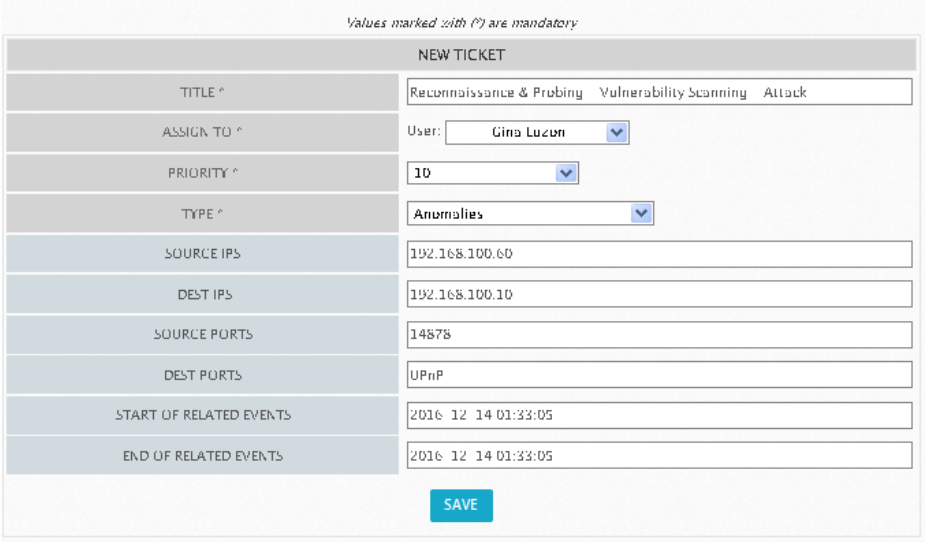


Figura 296 Generación ticket

4.5. Identificación y Análisis de Riesgos de Seguridad

En esta sección se realizará la evaluación de riesgos sobre los activos de información del prototipo propuesto en el escenario de ataque externo, para lo cual se considerará como amenazas los diferentes ataques realizados. La metodología de evaluación de riesgos a realizar será cualitativa. Se ilustrará la aplicación de la metodología de análisis y evaluación de riesgos de seguridad informática basado en la norma ISO 27005 para la gestión de riesgos que fue descrita en el Capítulo I.

Cabe mencionar que es importante realizar una evaluación de riesgos previamente a la aplicación de medidas, controles de seguridad informática o de seguridad de la información, por cuanto las organizaciones podrán además de contar con una herramienta y sistema de gestión de eventos de seguridad informática, gestionar adecuadamente los riesgos operativos tecnológicos, optimizando recursos centrada y enfocada en una verdadera gestión de riesgos.

Esto es importante puesto que por lo general las inversiones en seguridad informática son vistas como un gasto al igual que las de TICs, sin embargo, al estar enmarcados en una gestión de riesgos enfocándose en los riesgos prioritarios que se expone la organización generando interés en la alta dirección o gerencia, lo cual podrá ser visto como algo que agrega valor a la organización.

Se han identificado las siguientes posibles amenazas y vulnerabilidades que sugiere la Norma ISO 27005. De manera general la norma establece que los tipos de amenazas pueden ser de origen natural, humanas, deliberadas, accidentales, ambientes, acciones no autorizadas, entre otras. La categoría de amenazas que tienen un origen humano merecen una atención especial, por tal motivo y de acuerdo al escenario planteado, en la siguiente tabla se detallan las posibles amenazas.

- **Identificación de amenazas**

En la Tabla 18 se identificó y seleccionó las amenazas más comunes que se podrían presentar en el escenario de ataque propuesto, fueron tomadas del Anexo C de la norma ISO 27005.

Tabla 18
Identificación de Amenazas

Fuente de amenaza	Motivación	Acciones amenazantes
Pirata informático **Intruso ilegal**	Estatus Dinero	Intrusión, accesos forzados al sistema. Acceso no autorizado al sistema
Criminal de la computación	Ganancia monetaria Estatus	Crimen por computador (por ejemplo, espionaje cibernético) Intrusión en el sistema
Terrorismo	Chantaje, venganza, ganancia política	Ataques contra el sistema. Penetración en el sistema
Intrusos (empleados con entrenamiento deficiente, descontentos, malintencionados, negligentes, deshonestos o despedidos)	Ganancia monetaria Venganza Errores y omisiones intencionales (ej. error en el ingreso de datos)	Fraude y hurto Intrusión al sistema Código malicioso (ej. Virus, bomba lógica, troyano) Acceso no autorizado al sistema.

5. Identificación de vulnerabilidades

En la Tabla 19 se identificó y seleccionó las vulnerabilidades más comunes presentadas en los resultados de los ataques formulados detallados anteriormente, fueron tomadas del Anexo D de la norma ISO 27005.

Tabla 19
Identificación de Vulnerabilidades

Tipo	Ejemplos de vulnerabilidades	Ejemplos de amenazas
Software	Ausencia de pistas de auditoria	Abuso de los derechos
	Configuración incorrecta de parámetros	Error en el uso
	Ausencia de mecanismos de identificación y autentificación, como la autenticación de usuario	Falsificación de derechos
	Gestión deficiente de las contraseñas	Falsificación de derechos
Red	Arquitectura insegura de red	Espionaje remoto
Personal	Entrenamiento insuficiente en seguridad	Error en el uso
	Ausencia de mecanismos de monitoreo	Procesamiento ilegal de los datos
Organización	Ausencia de asignación adecuada de responsabilidades en la seguridad de la información	Negación de acciones
	Ausencia de registros en las bitácoras (logs) de administrador y operario.	Error en el uso

6. Valoración de riesgos

Se ha considerado las siguientes escalas de impacto y probabilidad para la valoración del riesgo.

Tabla 20
Valoración de riesgo Impacto y Probabilidad

Impacto	Probabilidad
Baja	Baja →

Media	Media
Alta	Alta

Para determinar el valor del riesgo se tendrá en cuenta la siguiente Tabla 21:

Tabla 21
Valoración de riesgo Impacto y Probabilidad

Impacto	Probabilidad	Riesgo
Bajo	Baja	Bajo
Bajo	Media	Bajo
Bajo	Alta	Medio
Medio	Baja	Bajo
Medio	Media	Medio
Medio	Alta	Alto
Alto	Baja	Medio
Alto	Media	Alto
Alto	Alta	Alto

7. Identificación y Análisis de Riesgos

En la Tabla 22, se asocian las amenazas con las vulnerabilidades anteriormente descritas y en base a esto se describe y redacta el riesgo siguiendo el siguiente formado:

Cualquier Evento, acción, hecho, situación no deseada impacta negativamente.

AMENAZA + VULNERABILIDAD+ CAUSARÍA + IMPACTO NEGATIVO.

Tabla 22
Identificación de Riesgos

Activo	Amenaza	Vulnerabilidad	Redacción del Riesgo
OSSIM	-Ataques contra el sistema. -Inyección de código malicioso. -Intrusión, accesos forzados al sistema.	-Entrenamiento insuficiente en seguridad.	R01: Ataques al sistema OSSIM y personal encargado de su administración con insuficiente entrenamiento en el manejo de la herramienta causaría que no se consiga gestionar adecuadamente todos los eventos e incidentes de seguridad informática.
	(Escaneo de puertos, análisis de vulnerabilidades web, ataque de fuerza bruta)	-Ausencia de asignación adecuada de responsabilidades en la seguridad informática.	R02: Ataques de tipo de inyección de código e intrusión forzada en el sistema OSSIM, y en ausencia de roles y responsabilidades en seguridad informática, al materializarse este riesgo, causaría que no se pueda disponer de personal técnico especializado para atención y remediación del incidente.
Servidor Ubuntu-Server	-Inyección de código malicioso. -Intrusión, accesos forzados al sistema.	-Entrenamiento insuficiente de seguridad.	R03: Ataques del tipo de inyección de código malicioso al servidor de aplicación Ubuntu-Server, y personal responsable de la administración del servidor con un insuficiente entrena miento de seguridad →

			informática causaría que no se pueda atender y remediar los incidentes.
	(Análisis de vulnerabilidades, ataque de fuerza bruta)	- Gestión deficiente de las contraseñas	R04: Ataques de intrusiones al servidor de aplicación Ubuntu-Server en ausencia de una gestión eficiente de contraseñas fuertes o seguras, causaría que se obtenga control y acceso del servidor por terceras personas.
Servidor Windows-Server	Inyección de código malicioso. (Análisis de vulnerabilidades)	- Configuración incorrecta de parámetros	R05: Ataques del tipo de inyección de código malicioso hacia el servidor Windows-Server, junto a una deficiente e incorrecta configuración de parámetros de seguridad en sus aplicativos y servicios, causaría que se afecte el sistema ocasionando indisponibilidad del sistema y por tanto de los servicios internos y externos que brinda.

8. Valoración del Riesgo

De los riesgos identificados y en base a la escala de valoración de impacto y probabilidad se determina el nivel de riesgo según se indica en la Tabla 23:

Tabla 23
Valoración del Riesgo

Activo	Redacción del Riesgo	Impacto	Probabilidad	Riesgo
OSSIM	R01: R01: Ataques al sistema OSSIM y personal encargado de su administración con un insuficiente entrenamiento en el manejo de la herramienta causaría que no se consiga gestionar adecuadamente todos los eventos e incidentes de seguridad informática.	Alto	Media	Alto
	R02: Ataques de tipo de inyección de código e intrusión forzada en el sistema OSSIM, y en ausencia de roles y responsabilidades en seguridad informática, al materializarse este riesgo, causaría que no se pueda disponer de personal técnico especializado para atención y remediación del incidente.	Medio	Media	Medio →

Servidor Ubuntu-Server	R03: Ataques del tipo de inyección de código malicioso al servidor de aplicación Ubuntu-Server, y personal responsable de la administración del servidor con un insuficiente entrenamiento de seguridad informática causaría que no se pueda atender y remediar los incidentes.	Medio	Baja	Bajo
	R04: Ataques de intrusiones al servidor de aplicación Ubuntu-Server en ausencia de una gestión eficiente de contraseñas fuertes o seguras, causaría que se obtenga control y acceso del servidor por terceras personas.	Alto	Media	Alto
Servidor Windows-Server	R05: Ataques del tipo de inyección de código malicioso hacia el servidor Windows-Server, junto a una deficiente e incorrecta configuración de parámetros de seguridad en sus aplicativos y servicios, causaría que se afecte el sistema	Media	Alta	Alto →

	ocasionando indisponibilidad del sistema y por tanto de los servicios internos y externos que brinda.

9. Matriz de riesgos

En la Tabla 24, se detalla a nivel de una matriz o mapa de calor la ubicación el nivel de riesgo evaluado.

Tabla 24
Matriz de riesgos

Impacto	**Alto**		R01- R04	
	Medio	R03	R02	R05
	Bajo			
		Baja	**Media**	**Alta**
	Probabilidad			

4.6. Recomendaciones Propuestas

En esta sección se propondrán opciones para el tratamiento del riesgo, de acuerdo a lo indicado en la Norma ISO 27005 entre las que se tiene: Reducción o Mitigación, Retención o Aceptación, Evitar o Eliminar y Transferir.

4.6.1. Tratamiento de Riesgos

El tratamiento de riesgos dependerá de la postura del riesgo que la organización adopte, esta es una decisión estratégica, debe ser aprobada por

la alta dirección dependiendo del tipo del activo o proceso involucrado, para el caso de riesgos operativos tecnológicos, particularmente para riesgos de seguridad informática puede ser adoptado y definido por el responsable del área o departamento. Para este caso se tomará la siguiente estrategia. En la Tabla 25, se describe las opciones de tratamiento a seguir:

Tabla 25
Valoración del Tratamiento

Riesgo	Tratamiento
Alto	Mitigar
Medio	Transferir
Bajo	Aceptar/Eliminar

Tabla 26
Tratamiento del Riesgo

Riesgo	Opciones de tratamiento	Plan de tratamiento
R01	Mitigar	Desarrollar programas de entrenamiento de seguridad informática a los responsables de la administración del sistema OSSIM.
R04	Mitigar	Elaborar e implementar procedimientos, estándares de contraseñas seguras en el servidor Ubuntu-Server.
R05	Mitigar	Elaborar estándares y procedimientos de *hardening* del servidor Windows-Server. Disponer de equipos de contingencia en caso de falla del servidor.
R02	Transferir	Establecer contratos con terceros para el soporte especializado en el tratamiento de incidentes específicos de seguridad informática, que contemple SLA´s.
R03	Aceptar	Se acepta el riesgo no se implementa o establece mecanismos de control.

En la Tabla 26, se deberá asignar responsables de la ejecución de los planes de tratamiento, por lo general se recomienda que esté a cargo en un área de control, pudiendo ser esta: Auditoría Interna, Control Interno, Gestión de Riesgos, Seguridad Informática, Seguridad de la Información, o alguna área que esté totalmente independiente de las áreas responsables de la ejecución de los planes de tratamiento, de esta manera se logra efectivamente una gestión verdadera del riesgo.

CAPITULO 5: CONCLUSIONES Y RECOMENDACIONES

5.1. Conclusiones y Recomendaciones

- El Sistema de Gestión de la Seguridad de la Información y Gestión de Eventos OSSIM es una herramienta significativa que permite realizar la gestión, monitoreo y registro ordenado de eventos ocurridos en los diferentes activos informáticos de una organización, brindando al Administrador o Analista de Red una base de información centralizada que permita detectar y analizar posibles ataques informáticos que afecten cualquiera de los principios fundamentales de la información, y poder implementar de forma efectiva medidas correctivas y procedimientos claros que disminuyan los riesgos a los cuales se encuentra expuesto el sistema.

- La metodología de identificación, análisis y evaluación propuesta y desarrollada en el capítulo 4 puede ser utilizada para cualquier tipo de riesgo a nivel organizacional o empresarial, sea estos a nivel de procesos, recursos humanos, tecnología, seguridad informática o de la información, al ser una metodología basada en un estándar internacional, puede ser comparados con otras metodologías o marcos de referencia, teniendo resultados similares.

- Es importante que las organizaciones implementen o incorporen además de sistemas o herramientas para gestionar las seguridades informáticas, marcos de trabajo, metodologías y procesos de evaluación de riesgos los cuales permitirán gestionar adecuadamente sus recursos atendiendo y priorizando sus riesgos, de esta manera se podrá implementar controles y mecanismos eficientemente.

Bibliografía

(s.f.). Obtenido de http://docs-asia.electrocomponents.com/webdocs/0e8b/0900766b80e8ba21.pdf

Alien Vault. (2015). *OSSIM vs. USM A Comparison of Open Source vs. Commercial.* AlienVault.

Cano, J. J. (2007). Inseguridad Informática un Concepto Dual en Seguridad Informática. *Infomation Systems Control Journal*.

Casares Stacey, D. (4 de Octubre de 2001). *Pontificia Universidad Católica del Ecuador*. Obtenido de ftp://ftp.puce.edu.ec/Facultades/Ingenieria/Sistemas/Network%20news/Gestion%20de%20Redes/GESTION_DE_RED.ppt

Chiavenato, I. (2006). *Introducción a la Teoría General de la Administración .* McGraw-Hill.

duarte, A. (2014). *ART INTERACTIVO.* Obtenido de http://www.artinteractivo.com/xbee-y-arduino

Flodo™, I. F. (20 de octubre de 2009). *FOTOLOG*. Obtenido de http://www.fotolog.com/cbtkd_itf/68486476/

Hegering , H.-G., Abeck , S., & Neumair , B. (1999). *Integrated Management of Networked Systems: Concepts, Architectures and their Operational Application.* Morgan Kaufmann.

ISO/IEC. (270002:2013). *Information technology — Security techniques — Code of practice for information security controls.*

ISO/IEC. (27001:2005). *Information technology - Security techniques - Information security management systems - Requirements.*

ISO/IEC. (27001:2005). *Information technology - Security techniques - Information security management systems - Requirements.*

Kavanagh, K., & Rochford, O. (2016). *Cuadrante Mágico de Seguridad de la Información y Gestión de Eventos.* Gartner.

Kotenko, I., Polubelova, O., Chechulin, A., & Saenko, I. (2013). Design and Implementation of a Hybrid Ontological-Relational Data Repository for SIEM Systems. *Journal Future Internet*.

Kotenko, Polubelova, Chechulin, & Saenk. (2013). *Design and Implementation of a Hybrid Ontological-Relational Data Repository for SIEM.*

López de Vergara Méndez, J. E. (2003). *Especificación de Modelos de Información de Gestión de Red Integrada mediante el uso de Ontologías y Técnica de representación del conocimiento.* Madrid.

Muñoz, J. D. (2003). *OSSIM (Open Source Security Information Management), Descripcion General del Sistema.*

Oracle. (2010). *WBEM* . Obtenido de http://docs.oracle.com/

OWASP, F. (2013). *OWASP Top 10 -2013: Los diez riesgos más críticos en aplicaciones web.* Creative Commons (CC) Attribution Share-Alike.

Puchades, A., & Peñalver, L. (2003). *Análisis de la Plataforma "OSSIM".* Valencia.

Ramos Cabrer, M. (Junio de 2008). *Grupo de Servicios para la Sociedad de la Información.* Obtenido de http://gssi.det.uvigo.es/users/mramos/public_html/gprsi/gprsi1.pdf

Soporte_Sony. (24 de 08 de 2015). *Soporte Sony.* Obtenido de https://la.es.kb.sony.com/app/answers/detail/a_id/7069/~/%C2%BFqu%C3%A9-es-la-intel-virtualization-technology-(intel-vt)%3F-y-%C2%BFes-compatible-con-las

Tejada, E. C. (2014). *Gestión de Incidenctes de Seguridad Informática.* IC Editorial.

Torres, M., & Villegas, D. (2010). *Integración de OSSIM y UNTANGLE.*

Villalón Huerta, A. (2000). *Seguridad en Unix y Redes.* Open Publication License.

WBEM Solutions Inc. (26 de Octubre de 2009). *The Java API for Web Based Enterprise Management.* Obtenido de http://download.oracle.com/otn-pub/jcp/wbem-1.0-pfd-oth-JSpec/wbem-1_0-pfd-spec.pdf?AuthParam=1398403645_fa7e3b983cb85a4746a3b1f71b148f8d

ANEXOS