



# **ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL**

Facultad de Ingeniería en Electricidad y Computación

**“IMPLANTACIÓN DE UNA HERRAMIENTA OSSIM  
PARA EL MONITOREO Y GESTIÓN DE LA  
SEGURIDAD DE LA RED Y PLATAFORMAS  
WINDOWS Y LINUX APLICADO A EMPRESAS  
MEDIANAS”**

**INFORME DE PROYECTO DE GRADUACIÓN**

Previa a la obtención del Título de:  
**LICENCIADO EN REDES Y SISTEMAS OPERATIVOS**

Presentada por:  
**ALVARO LUIS VILLAFUERTE QUIROZ  
ANGEL HERALDO BRAVO BRAVO**

**GUAYAQUIL – ECUADOR  
2015**

## **AGRADECIMIENTO**

Mis más grandes sentimientos de gratitud para mi Dios todopoderoso por brindarme esa fuerza sobrenatural e inspiración en cada meta y sueño alcanzados a lo largo de mi vida.

A mi madre, hermanos y familiares por su apoyo incondicional y por brindarme esa confianza para que continúe alcanzando metas profesionales.

A mi compañero y amigo de Tesis Álvaro, a mis amigos de la vida, compañeros de clase y prestigiosos docentes que impartieron sus conocimientos y experiencias durante esta etapa de mi crecimiento profesional.

A la Escuela Superior Politécnica del Litoral por esa oportunidad brindada como estudiante y por las exigencias de formación para ser un profesional competente para la sociedad.

***Ángel H. Bravo Bravo***

Agradezco a mi compañero de Proyecto de Grado Ángel Bravo Bravo puesto que sin su ayuda y su apoyo y en algunos casos la presión y control para terminar dicho proyecto, sin esa característica no hubiera concluido y no estaría ahora alcanzando una de mis metas profesionales.

***Álvaro L. Villafuerte Quiroz***

## **DEDICATORIA**

A Dios por su fidelidad, a mi madre por enseñarme a luchar en la vida, a Kenia L. “mi gatita” y a todos los soñadores que se atreven a luchar y esforzarse cada día por alcanzar ese sueño.

***Ángel H. Bravo Bravo***

Dedico toda esta felicidad en especial a mi madre que en el pasado no pensó que su hijo con tantos tropiezos que tuvo en su vida este graduándose en la universidad que todos mis hermanos han estudiados, a mi hermano Jorge Villafuerte que con su apoyo económico y emocional estuvo en los momentos cuando me sentía débil y en algunas ocasiones pensé abandonar mis estudios, a mi hermana María Villafuerte que con su apoyo he llegado lejos, a Juan Villafuerte que con sus clases de matemáticas pude ingresar a la universidad y como olvidar a mi padre Wilfrido Villafuerte que es un gran ejemplo de superación.

Finalmente a mi hermanito Alexander Villafuerte para que supere mis pasos y pueda seguir con la tradición de seguir sus estudios en la ESPOL.

***Álvaro L. Villafuerte Quiroz***

## **TRIBUNAL DE SUSTENTACIÓN**

---

Ing. Sara Ríos Orellana  
SUBDECANA DE LA FIEC  
PRESIDENTE

---

Ing. José Patiño S., MSIG  
DIRECTOR DEL PROYECTO DE GRADUACIÓN

---

Ing. Albert Giovanny Espinal Santana  
MIEMBRO PRINCIPAL DEL TRIBUNAL

## DECLARACIÓN EXPRESA

“La responsabilidad del contenido de este Informe nos corresponde exclusivamente; y el patrimonio intelectual de la misma a la ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL”.

(Reglamento de Exámenes y Títulos profesionales de la ESPOL).

---

Ángel H. Bravo Bravo

---

Álvaro L. Villafuerte Quiroz

## RESUMEN

Este proyecto consistió en el análisis de la seguridad de una infraestructura de red y servidores en una empresa privada, el enfoque principal es de mantener centralizado todos los logs que son generados por los diferentes servidores y equipos de red en una sola consola de administración centralizada y realizar un análisis detallado de cada evento, así mismo como obtener reportes personalizados de las vulnerabilidades existentes en los hosts y la red en general.

OSSIM es la herramienta implementada en esta solución informática, siendo una aplicación Open Source y más que una herramienta de monitoreo de logs es un SIEM (Security Information and Event Management) y trae incorporado diversas formas para gestión de seguridad como un antivirus que se encarga de detectar y eliminar software malicioso de un sistema informático, cuenta con detectores de intrusos basados en host (HIDS, Host-based Intrusion Detection Systems) encargado de monitorear procesos y archivos críticos del sistema bajo análisis, cuenta con Detectores de intrusos basados en red (NIDS, Network-based Intrusion Detection Systems) responsables de la revisión de los datos que circulan por la red y avisan cuando observan tráfico que evidencia un ataque, detectores de vulnerabilidades que hacen un análisis detallado y arrojan como resultado



las vulnerabilidades que existen en el sistema operativo y el software instalado.

El enfoque general de este proyecto con OSSIM está limitado solo al monitoreo de logs y realizar un escaneo de vulnerabilidades básicas en la red y hosts, además de monitorear la disponibilidad en tiempo real de los dispositivos y servidores principales de la empresa. Pero cabe recalcar que la funcionalidad total de OSSIM está más allá de un simple análisis básico de lector de logs y su función está en un sistema de seguridad integrado, que dependiendo del conocimiento avanzado en el uso de la herramienta se puede explotar al máximo todas las funcionalidades y como resultado se obtendrá un sistema seguro contra amenazas externas, amenazas internas en huecos abiertos por puertos de red, escaneo de virus, malware y seguridad en las bases de datos.

Como resultado final presentamos un estudio general de OSSIM, un análisis de compatibilidad y requerimientos para proceder con la instalación, análisis financiero y conocimientos elementales del administrador de red y la configuración paso a paso de las características más importantes de OSSIM que debe conocer todo administrador de red para poder implementar la herramienta en su empresa.

Para obtener conclusiones sobre la factibilidad y la correcta funcionalidad de la herramienta se detalla reportes generados por OSSIM donde se observa el resultado arrojado por la integración de diferentes equipos de red y servidores en una consola unificada, se presenta información de eventos de acceso a los diferentes servidores y equipos de red, registros de autenticaciones erróneas, escaneo de todos los agentes en tiempo real y, además se puede verificar detalladamente las vulnerabilidades localizadas en la red de la empresa y en las estaciones de trabajo que acceden a ella, otorgando una visión general de la magnitud en la parte de seguridades informáticas que puede ofrecer OSSIM a un administrador de Infraestructura.

## ÍNDICE GENERAL

AGRADECIMIENTO .....	II
DEDICATORIA .....	IV
TRIBUNAL DE GRADUACIÓN .....	VI
DECLARACIÓN EXPRESA.....	VII
RESUMEN.....	VIII
ÍNDICE GENERAL .....	XI
ÍNDICE DE FIGURAS.....	XIV
ÍNDICE DE TABLAS .....	XVIII
INTRODUCCIÓN.....	XIX
1 ANÁLISIS CONTEXTUAL .....	1
1.1 Tema del Proyecto .....	1
1.2 Descripción.....	2
1.3 Alcance.....	2
1.4 Problemática.....	3
1.5 Justificación.....	4
1.6 Objetivo General .....	5
1.7 Objetivos Específicos.....	6
1.8 Propuesta Metodológica.....	7
1.9 Resultados Esperados.....	10
2 MARCO TEÓRICO .....	11
2.1 OSSIM .....	11
2.1.1 Definición .....	11
2.1.2 Características .....	13
2.1.3 Comparación con otras aplicaciones.....	14
2.1.4 Tabla de Comparación.....	15
2.1.5 Ventajas .....	15
2.1.6 Desventajas.....	17
2.1.7 Compatibilidad .....	17
2.2 Componentes y Arquitectura .....	19
2.2.1 Ossim-server .....	19

2.2.2	Ossim-framework .....	21
2.2.3	Ossim-agent .....	23
2.2.4	Arquitectura de OSSIM.....	25
2.2.5	Diagrama de la Arquitectura de Ossim.....	27
2.3	Tipos de monitoreo .....	27
2.3.1	Arpwatch .....	27
2.3.2	Pads.....	28
2.3.3	Openvas.....	29
2.3.4	Spade .....	30
2.3.5	Tcptrack .....	30
2.3.6	Ntop .....	31
2.3.7	NfSen.....	32
2.3.8	Osiris.....	34
2.4	Licenciamiento .....	35
2.4.1	Costo .....	35
3	FASE DE IMPLEMENTACIÓN .....	37
3.1	Instalación cliente y servidor .....	37
3.1.1	Requisitos técnicos para la instalación del servidor OSSIM .....	37
3.1.2	Requisitos del personal administrador .....	38
3.1.3	Instalación de OSSIM .....	39
3.1.4	Parámetros de configuración en el servidor .....	43
3.1.5	Configuración de servicios y plugins en el servidor .....	45
3.1.5.1	Configuración del Plugin OSSEC .....	45
3.1.5.2	Configuración del servicio Rsyslog .....	47
3.1.5.3	Configuración de los plugins CFG y SQL .....	54
3.1.5.4	Activación de los plugins en OSSIM .....	58
3.1.6	Instalación del cliente recolector de registros .....	60
3.1.6.1	Instalación del Cliente ossec en Windows .....	60
3.1.6.2	Configuración del cliente Rsyslog en Linux .....	62
3.1.6.3	Configuración del Cliente Syslog en un Firewall Cyberoam. 63	
3.1.6.4	Configuración del Cliente Syslog en un Switch Cisco .....	64
3.1.7	Parámetros de configuración del cliente .....	66

3.2	Funcionabilidad y desempeño .....	67
3.2.1	Generación de informes de los eventos de la red .....	68
3.2.2	Generación de informes de los eventos del S.O Windows .....	69
3.2.3	Generación de informes de los eventos del S.O Linux .....	72
3.2.4	Informes de vulnerabilidades y alarmas en general .....	73
3.2.5	Generación de informes de la disponibilidad de la red .....	76
3.2.6	Generación de informes de seguridad de la red .....	78
3.3	Análisis de resultados .....	82
4	ANÁLISIS FINANCIERO, VIABILIDAD Y FACTIBILIDAD .....	85
4.1	Viabilidad del proyecto.....	85
4.2	Estudio de Factibilidad.....	87
4.3	Recursos Humanos .....	88
4.4	Recursos Materiales.....	89
4.5	Recursos Financieros .....	90
4.5.1	Costo de implementación.....	90
4.5.2	Costo de mantenimiento .....	91
4.6	Recursos Legales.....	91
	CONCLUSIONES Y RECOMENDACIONES.....	93
	Bibliografía.....	96

## ÍNDICE DE FIGURAS

Figura 1.1 Fase de Planeación .....	7
Figura 2.1 Modelo de OSSIM .....	12
Figura 2.2 Arquitectura Ossim Server .....	19
Figura 2.3 Ossim Fframework.....	22
Figura 2.4 Agentes de Ossim .....	23
Figura 2.5 Arquitectura de Ossim .....	27
Figura 2.6 Tcptrack.....	31
Figura 2.7 Funcionamiento del NfSen.....	33
Figura 3.1 Seleccionar la versión de Ossim .....	40
Figura 3.2 Selección de Idioma del Ossim .....	40
Figura 3.3 Selección de Idioma del teclado .....	41
Figura 3.4 Configuración de la Red .....	41
Figura 3.5 Establecer contraseña .....	42
Figura 3.6 Configuración de la Región.....	42
Figura 3.7 Copia de Archivos Necesarios Para la Instalación .....	43
Figura 3.8 Terminando la Copia de Archivos Necesarios .....	43
Figura 3.9 Configuración de Acceso Web.....	44
Figura 3.10 Ingresando a OSSIM Web .....	44
Figura 3.11 Configuración de Plugins .....	45
Figura 3.12 Creación del Agente .....	46

Figura 3.13 Asignación de IP de Los Agentes .....	46
Figura 3.14 Generar Autenticación Ossec .....	46
Figura 3.15 Panel de Administración Ossec .....	47
Figura 3.16 Configuración del Rsyslog .....	48
Figura 3.17 Script de rotación de Archivo .....	49
Figura 3.18 Verificación de la Lectura de los Logs.....	49
Figura 3.19 Configuración Rsyslogs Para Switch Cisco.....	50
Figura 3.20 Reiniciar el Rsyslog .....	50
Figura 3.21 Verificación de Lectura de los Logs del Switch .....	51
Figura 3.22 Configuración Syslog Linux.....	51
Figura 3.23 Verificación de lectura de los Logs desde Linux.....	51
Figura 3.24 Configuración Plugin Nagios.....	52
Figura 3.25 Búsqueda de Host desde ASSETT .....	53
Figura 3.26 Configuración de Disponibilidad.....	53
Figura 3.27 Activando Parámetros de Disponibilidad.....	54
Figura 3.28 Creación de Plugins CFG Central PBX.....	55
Figura 3.29 Creación de Plugins CFG Firewall .....	55
Figura 3.30 Creación de Plugins CFG Switch Cisco .....	56
Figura 3.31 Creación de Plugin SQL .....	57
Figura 3.32 Verificación de Logs de la Central PBX.....	57
Figura 3.33 Verificación de Logs del Firewall.....	57
Figura 3.34 Verificación de Logs del Switch .....	58

Figura 3.35 Activación de Plugins en Ossim.....	58
Figura 3.36 Activación de Plugins en Ossim.....	59
Figura 3.37 Activación de Plugins Central PBX .....	59
Figura 3.38 Activación de Plugins del Syslog Switch .....	59
Figura 3.39 Activación de Plugin Nagios.....	59
Figura 3.40 Instalación de Ossec en Windows .....	60
Figura 3.41 Selección de la Versión de Ossec.....	61
Figura 3.42 Instalación en curso Ossec.....	61
Figura 3.43 Redireccionando los registros de Linux a Ossim.....	62
Figura 3.44 Configuración de Syslog en Cyberoam .....	63
Figura 3.45 Creación de Nuevo Syslog en Cyberoam .....	64
Figura 3.46 Configuración del cliente Syslog en el Switch .....	64
Figura 3.47 Accediendo al Rsyslog de Cisco .....	65
Figura 3.48 Creando Nuevo Rsyslog en Cisco .....	65
Figura 3.49 Configurando Autenticación en Ossec .....	67
Figura 3.50 Informe de la red en OSSIM .....	68
Figura 3.51 Escaneo realizado de la Red .....	69
Figura 3.52 Escaneo Realizado a un Servidor Windows.....	70
Figura 3.53 Escaneo General en Hosts Windows .....	71
Figura 3.54 Sucursales remotas ubicadas en el mapa.....	71
Figura 3.55 Informe del Servidor Ossim.....	72
Figura 3.56 Informe del Servidor Linux PBX.....	73



Figura 3.57 Análisis de Vulnerabilidad .....	74
Figura 3.58 Análisis Estadístico de los últimos Eventos.....	75
Figura 3.59 Análisis resumido de los Sensores .....	75
Figura 3.60 Políticas Ejecutadas en Tiempo Real.....	76
Figura 3.61 Reporte de Equipos Activos en la Red.....	77
Figura 3.62 Monitoreo Personalizado de Disponibilidad .....	77
Figura 3.63 Monitoreo del Firewall.....	78
Figura 3.64 Monitoreo del Servidor Linux .....	78
Figura 3.65 Informe de Amenazas de Seguridad.....	78
Figura 3.66 Informe de Múltiples Eventos.....	79
Figura 3.67 Trafico de Puertos de Capa 4 .....	79
Figura 3.68 Reporte de un Host Específico .....	80
Figura 3.69 Intento Fallido de Autenticación .....	80
Figura 3.70 Informe de Accesos al Switcho cisco .....	81
Figura 3.71 Eventos del Firewall.....	81
Figura 3.72 Acceso a la Central PBX.....	82

## ÍNDICE DE TABLAS

Tabla 1 Comparaciones de Software con OSSIM .....	15
Tabla 2 Tabla de Puertos de comunicación .....	20
Tabla 3 Costo de Ossim .....	35
Tabla 4 Costo de Implementación del Proyecto.....	90
Tabla 5 Costo de Mantenimiento de OSSIM .....	91

## INTRODUCCIÓN

Las estadísticas mundiales presentan que el uso del internet tiene un crecimiento exponencial, los proveedores de servicios de internet en sus informes de ventas establecen un crecimiento en la demanda de los usuarios, esto se origina por la facilidad que tienen los usuarios de adquirir equipos Smartphones, los mismos que permiten la navegación a muchos servicios en la internet. Entonces la pregunta es ¿En que afecta el crecimiento del internet a las empresas?, Las empresas cambian su mercado acorde a la tecnología y aprovechando el mercado digital se ven en la obligación de llegar a los usuarios con diferentes servicios, y para esto hacen el uso de redes convergentes y servidores que puedan soportar el tráfico interno y externo.

Las empresas medianas en la actualidad invierten en redes de datos y voz, esta red esta apta para soportar todo el tráfico requerido por los usuarios y permite compartir diferentes recursos, adquieren servidores robustos con sistemas operativos multiplataforma capaces de brindar varios servicios a los usuarios internos y externos, y obviamente que con mayor cantidad de servicios y equipos accediendo a la red, también crece la complejidad de la administración, sin embargo intrusos, los hackers y delincuentes informáticos cada vez encuentran nuevas formas para continuar con su accionar y esta

situación ha llevado a la aparición de nuevas amenazas que desean ingresar en los sistemas computarizados.

En la actualidad, la seguridad informática ha adquirido gran auge, dadas las cambiantes condiciones y las nuevas plataformas de computación disponibles, la posibilidad de interconectarse a través de redes han abierto nuevos horizontes que permiten explorar más allá de las fronteras de la organización. Es en este sentido, la importancia de tener una herramienta para visualizar en tiempo real el funcionamiento de la red y verificar los sucesos que están siendo ocasionados por los usuarios o atacantes a nuestra red y servidores.

La Seguridad Informática necesita de una herramienta que le ayude al administrador de la red a la toma de decisiones oportunas en la información y servicios críticos que favorecen el desarrollo de la organización y su buen funcionamiento.

Las actividades a desarrollarse deben servir para la correcta planificación preventiva de seguridad de una red corporativa, y es necesario dar a conocer alternativas a las típicas herramientas de monitoreo de redes existentes y mostrar técnicas diferentes, utilizando un conjunto de herramientas que están unificadas en una sola herramienta de libre distribución denominada OSSIM.

## **CAPÍTULO 1**

### **1 ANÁLISIS CONTEXTUAL**

#### **1.1 Tema del Proyecto**

“IMPLANTACIÓN DE UNA HERRAMIENTA OSSIM PARA EL MONITOREO Y GESTIÓN DE LA SEGURIDAD DE LA RED Y PLATAFORMAS WINDOWS Y LINUX APLICADO A EMPRESAS MEDIANAS”

El proyecto es realizado por los estudiantes:

- ✓ ALVARO LUIS VILLAFUERTE QUIROZ
- ✓ ANGEL HERALDO BRAVO BRAVO

## **1.2 Descripción.**

El proyecto contempla el análisis, estudio y la implementación de la herramienta OSSIM en una infraestructura de red de datos en donde existen servidores físicos y virtuales corriendo bajo las plataformas Windows y Linux, los mismos que proporcionan servicios de telefonía IP, servicio web y Active-Directory, nuestro enfoque es específicamente al análisis del estado de la red, información de errores y advertencias que son generados por los diferentes servidores, gestionar auditoría y control de seguridad de la red; El proyecto está orientado especialmente a los Administradores de red de empresas medianas que necesitan tener un monitoreo general de su infraestructura, obtener reportes en tiempo real de lo que está sucediendo en la red para poder analizar las anomalías y le ayuden en la toma de decisiones y correcciones oportunas.

## **1.3 Alcance**

El alcance del proyecto abarca los siguientes puntos específicos:

- ✓ Monitoreo y Análisis del tráfico de la red.
- ✓ Control de seguridad de la red de voz y datos
- ✓ Análisis de errores de un servidor Windows y Linux
- ✓ Análisis de ataques ocasionados en la red.
- ✓ Análisis de fallos en servidor Windows y Linux
- ✓ Análisis de conexiones y consumo de ancho de banda en la red.

- ✓ Análisis de los diferentes servicios ejecutados.
- ✓ Análisis de puertos LAN/WAN en la red.
- ✓ Instalación de OSSIM en una empresa privada.
- ✓ Análisis de registros anormales en nuestra red
- ✓ Monitorización de máquinas y equipos de usuarios
- ✓ Control de intrusiones, detección de intrusos en nuestra red basado en host/mac/IP.
- ✓ Monitoreo de Accesos o sesiones de usuarios.

#### **1.4 Problemática**

Los problemas a los que nos enfrentamos como administradores de una red se derivan fundamentalmente en la seguridad; en la actualidad se implementan múltiples herramientas que ayudan a la gestión y monitoreo de la red, el inconveniente que se presenta es que todas estas herramientas recolectan una gran cantidad de ficheros de registro (logs) que debemos analizar por separado, en determinadas ocasiones configurar estas herramientas es muy complejo y por último tenemos que soportar los reportes generados que a veces presenta información errónea.

Dado este gran problema de que tenemos muchas anomalías en la red, en la recolección de los registros (logs) generados por los diferentes servicios que están en los servidores, presentamos OSSIM como la herramienta de

monitoreo avanzado, la misma que nos permite obtener una foto en tiempo real de nuestra red y permite obtener información de fácil entendimiento y muy práctica al momento de tomar decisiones.

### **1.5 Justificación.**

El proyecto es de vital ayuda para gestionar y monitorizar la red en casi todas las pequeñas y medianas empresas de nuestro país, convirtiéndose en una herramienta indispensable para los administradores de una red, a la vez es un apoyo principal en la toma de decisiones relacionadas a la seguridad, disponibilidad y ejecución de los servicios que administramos en la empresa.

La implementación de OSSIM en una empresa donde existe una red de datos y tenemos servidores en producción hace que nuestro proyecto no solo quede en un estudio teórico, además enseñaremos como usar dicha tecnología para hacer un monitoreo ágil y eficiente y esto permite generar confianza a los administradores de red al momento que deseen usar una herramienta Open Source que se encuentra en el medio.

Entre las causas principales que hacen posible el planteamiento del problema antes mencionado tenemos.

- ✓ Ausencia parcial o total del estado de la red.
- ✓ Ausencia de alertas de vulnerabilidades y errores en los servidores.



- ✓ Ausencia de monitoreo del uso de recursos y servicios en la red generado por los usuarios.

Los principales efectos que producen estas causas son:

- ✓ Poco interés de usos de nuevas tecnologías en gestión de red.
- ✓ Genera huecos de seguridad en los servidores e inestabilidad en los servicios.
- ✓ Se altera la disponibilidad de la red al no conocer el funcionamiento y la carga que se está generando por los usuarios creando lentitud para acceder a los servicios.

Al no ejecutarse este proyecto, se daría como resultado el descuido del monitoreo en la infraestructura de red y un déficit en la toma de decisiones realizadas por el administrador, generando mayor carga laboral de forma manual.

## **1.6 Objetivo General**

Implementar la herramienta OSSIM en una empresa donde existe servidores en producción y poder integrar todos los registros (logs) generados por los diferentes servicios, los registros (logs) generados en la red de voz y datos, siendo la finalidad principal tener un sistema de gestión y monitoreo de recursos centralizados, el mismo que servirá de ayuda indispensable al administrador de una red.

## **1.7 Objetivos Específicos**

1. Instalación de la herramienta OSSIM en la red de una empresa privada.
2. Identificar los métodos que le permiten a OSSIM recolectar la información generada por los diferentes servidores y dispositivos.
3. Análisis del tráfico, ancho de banda y disponibilidad de la red de voz y datos.
4. Análisis de registros (logs) de seguridad en los servidores Linux y Windows.
5. Monitoreo y análisis de ataques, seguridad y disponibilidad en la red.
6. Monitoreo y análisis de vulnerabilidades de la red.
7. Análisis de registros de errores, registros de advertencias y fallos en los servicios ejecutados.

## 1.8 Propuesta Metodológica

El desarrollo del presente proyecto se llevará a cabo en 5 fases ejecutadas secuencialmente, para aquello se hará uso de la metodología PDIOO (Planificación, Diseño, Implementación, Operación, Optimización), con la finalidad de obtener la información necesaria y seguir un adecuado orden durante el proceso de ejecución del presente proyecto.

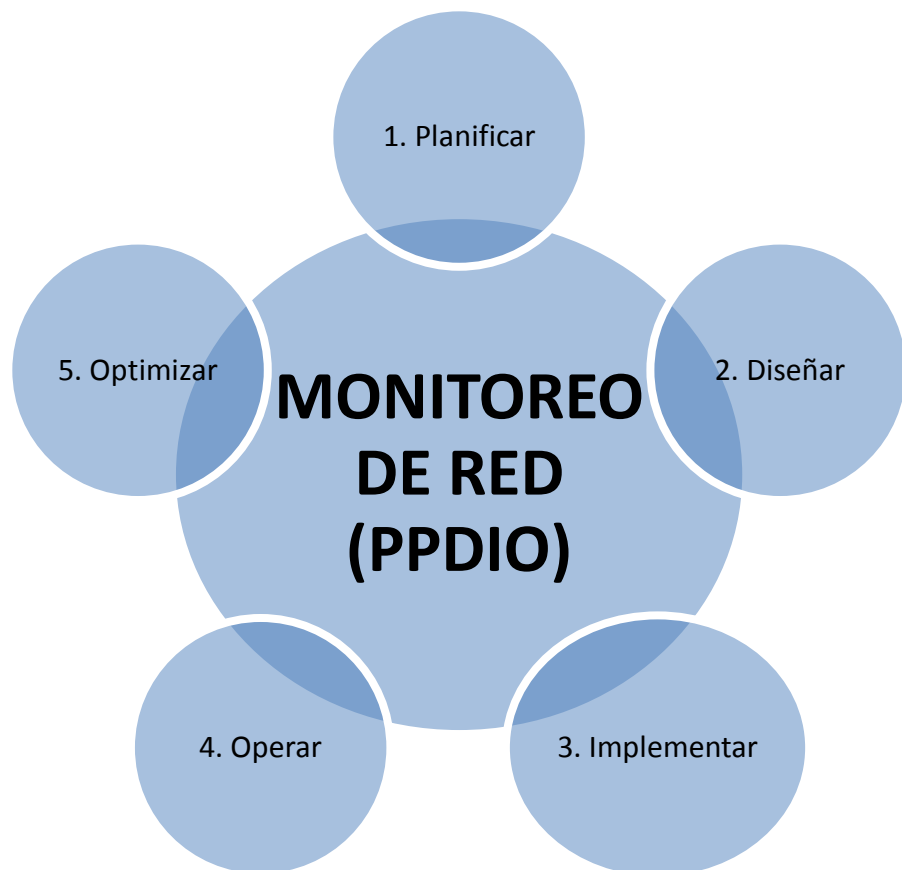


Figura 1.1 Fase de Planeación

**FASE I: Planificar**, En la etapa inicial, se cubre el proceso de análisis e investigación de las operaciones necesarias que vamos a necesitar para el monitoreo de red y los registros (logs) de los servidores, su proceso básico consiste en seleccionar que tipo de registros (logs) de los servicios vamos a recolectar, qué importancia se le dará a cada registro, seleccionar los dispositivos de red que serán auditados. Esta fase se lleva a cabo en las instalaciones físicas de la Organización acorde al cronograma de actividades.

**FASE II: Diseñar**, Se procede a diseñar el plan estratégico acorde al análisis inicial y poder implementar los distintos roles que nos ofrece OSSIM para el monitoreo respectivo, categorizar la información en los niveles bajo, medio y alto según los servicios monitorizados. Diseñar como se presentara la información acorde al nivel de riesgo de los logs generados, establecer un plan de ejecución automática para contrarrestar las vulnerabilidades y finalmente diseñar el envío de notificaciones vía email al administrador de la red para tener informado de todos los acontecimientos u cambios en la red.

**FASE III: Implementar**, se da inicio a la parte práctica de la fase anterior, se ejecuta el diseño planificado y esta fase consiste en la instalación de la herramienta OSSIM en un servidor específico, instalación de aplicaciones libres que son agentes de recolección de los diferentes eventos generados en la red interna, recolectar los registros (logs) de los servicios existentes,

recolectar información importante de los logs de estado de los servidores. La finalidad de esto es analizar el comportamiento y la relación entre las tablas cuando los eventos se almacenan. Esta fase es supervisada por el Administrador y personal de apoyo que participen en la implementación acorde al cronograma de actividades.

**FASE IV: Operar**, En esta fase nos enfocamos a trabajar con los diferentes servicios existentes, a realizar cambios en los servidores, a generar tráfico en la red interna. Esta es la fase donde la herramienta OSSIM está capturando toda la información enviada por los agentes de recolección desde los diferentes servidores y equipos de red, OSSIM es puesta en operación siendo monitoreada por personal capacitado, la finalidad es identificar los errores en los sistemas operativos, identificar ataques, saturación de enlace, detención de intrusos, eventos de advertencias, anomalías en la red interna, y otra información relevante generada que no tenga la autorización correspondiente dada por el administrador de red. La ejecución de esta fase es íntegra de forma automática y transparente para los usuarios, no afectando sus labores cotidianas en la empresa.

**FASE V: Optimizar**, con todas las herramientas que se implementarán se optimiza el trabajo del administrador de red, obteniendo información confiable, procesada y con estadísticas de lo ocurrido en la red desde la

consola de seguridad de OSSIM. En esta fase se evalúa la operación de los servicios, los servidores, los equipos de red y la red en general para detectar errores en configuraciones de los agentes de recolección, fallas o malas configuraciones en la herramienta OSSIM, se corrige todos los problemas encontrados, se optimiza la presentación de los informes para que sean más fáciles de interpretar y faciliten a la toma de decisiones por el administrador o agente encargado de la red, en el caso de no existir problemas después de la operación se crea un plan de prevención.

### **1.9 Resultados Esperados**

- ✓ Tener control centralizado de los eventos registrados en los servidores Linux y Windows.
- ✓ Mantener un análisis en tiempo real de la infraestructura de red y los servicios ejecutados.
- ✓ Priorizar los eventos recibidos de vulnerabilidades y errores en la red.
- ✓ Presentar gráficos de reportes de los diferentes eventos que suceden en la red de datos y voz para realizar la evaluación de riesgos y disparar alarmas.
- ✓ Reenviar eventos o alarmas a través de correos para mantener informado al administrador de red de los acontecimientos anormales.

## **CAPÍTULO 2**

### **2 MARCO TEÓRICO**

#### **2.1 OSSIM**

##### **2.1.1 Definición**

La sigla OSSIM se deriva para Open Source Security Information Management (Herramienta de Código Abierto para la Gestión de Seguridad de la información), OSSIM no es una herramienta única, al decir OSSIM se entiende que es un conjunto de herramientas unidas en un solo programa que facilita el análisis, visualización y la gestión de manera centralizada de los eventos que ocurren en los diferentes componentes de la infraestructura IT de la empresa, obteniendo de

esta forma mayor efectividad a la hora del monitoreo y de encontrar errores u vulnerabilidades en la seguridad de la red.

OSSIM es una herramienta que nos ayuda mucho en el monitoreo de la red, permitiéndonos controlar algo tan básico desde un log de la contraseña mal digitada hasta un posible ataque que se esté dando a nuestra infraestructura.

Esta herramienta trae incorporada cerca de 22 Funciones, todas estas son Open Source capaces de correlacionarse y así poder tener el control centralizado, básicamente se lo puede representar en el siguiente diagrama.

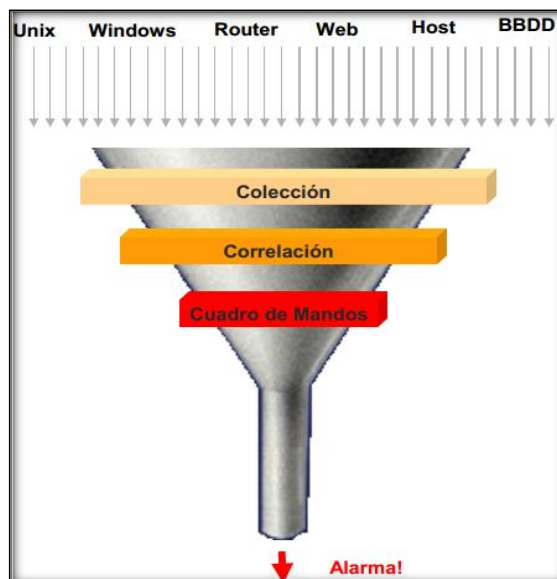


Figura 2.1 Modelo de OSSIM



### 2.1.2 Características

Ossim trae un conjunto de características que permite al administrador de red gestionar de forma más eficiente la seguridad interna de los servidores, de la red de datos y voz, entre las cuales podemos mencionar los siguientes:

- ✓ Es gratuito.
- ✓ Monitoreo centralizado.
- ✓ Analiza el comportamiento de nuestra Red
- ✓ Presenta informes técnicos.
- ✓ Realiza un análisis de los posibles riesgos y anomalías en la red.
- ✓ Controla los posibles ataques/intruso en la red.
- ✓ Monitorea el excesivo tráfico que se pueda generar.
- ✓ Presenta una interfaz gráfica web amigable hacia al Administrador
- ✓ Permite recolectar logs de los servidores sin importar que distribución de Linux tenga instalado.
- ✓ El cliente recolector de logs que se instala en Windows es muy sencillo de configurar.
- ✓ Realiza test de vulnerabilidad.
- ✓ Realiza notificaciones automáticas mediante alertas.
- ✓ Cuenta con gran cantidad de plug-ins gratuitos.
- ✓ Las notificaciones que se envían pueden ser:
  - Falso supuesto

- Alerta de duplicidad de mac
- Clave incorrecta
- Alerta de intruso
- Posible ataque
- Trafico excesivo... etc.

### **2.1.3 Comparación con otras aplicaciones.**

Ossim cuenta con 22 herramientas de libre distribución embebidas y así poder contar con más facilidades para la detención de intrusos en la red, la misma facilita el monitoreo a través de una interfaz Web y de esta forma hace más fácil el uso y control por parte del administrador de red, también genera notificaciones automáticas de los eventos generados.

Presentamos una comparativa de nuestra herramienta Ossim con algunas herramientas gratuitas y otra pagadas, mostrando que Ossim aunque sea una herramienta Gratuita puede competir e incluso superar a una herramienta de pago.

### 2.1.4 Tabla de Comparación.

En la siguiente tabla se ilustra de forma resumida como OSSIM supera a otras aplicaciones gratuitas e incluso a una herramienta específica licenciada.

	OSSIM	Hyperic HQ	Securia SGSI	RSA	NET IQ
<b>TIPO DE LICENCIA</b>	Gratis	Gratis	Gra/Pag	Pagada	Pagada
<b>Exploración de redes</b>	☐	X	✓	✓	✓
<b>Detección de intrusos</b>	✓	✓	✓	✓	✓
<b>Detección de vulnerabilidades</b>	✓	X	✓	X	X
<b>Monitorización de equipos</b>	✓	✓	X	✓	✓
<b>Plugins Free</b>	✓	✓	✓	X	X
<b>Notificaciones Automáticas</b>	✓	✓	X	✓	✓
<b>Network IDS</b>	✓	X	X	X	X
<b>Interfaz Web</b>	✓	☐	✓	X	X

Tabla 1 Comparaciones de Software con OSSIM

### 2.1.5 Ventajas

Tiene muchas ventajas para hacer la vida fácil al administrador de red, ya que su prioridad es presentar un ambiente centralizado para el fácil monitoreo y correcciones. En esta herramienta se pueden destacar dos funciones primordiales y que son de gran ayuda a la hora de hacer un plan de mejoras en la seguridad de la red, podemos

mencionar entre las ventajas más evidentes de las herramientas las siguientes:

- ✓ **Correlación:** agrupa todos los eventos de los logs que está pasando en la red y así brinda una mejora ya que podemos visualizar todos los eventos en una sola pantalla y un solo formato, mediante esta facilidad que nos brinda esta herramienta podemos relacionar y procesar la información adquirida mediante el monitoreo y así poder aumentar la capacidad del IT para la detecciones de lo error, posibles ataques, IP duplicadas entre otras, poder priorizar los eventos como bajo, medio o alto según sean clasificados.
  
- ✓ **Valoración de Riesgo:** en este ámbito le brinda al IT una acción a seguir mediante los errores que se presenta, es decir poder ejecutar una acción mediante la información que se logra en la correlación de los eventos según su clasificación teniendo en cuenta lo concurrente del error en la red.
  
- ✓ Costo y flexibilidad en la configuración centralizada.
  
- ✓ Organizar y mejorar las capacidades de detección.
  
- ✓ Visibilidad de los eventos de seguridad de la organización.

- ✓ Es el uso de notificaciones mediante correo electrónicos con el propósito de tener informado al administrador de red si estuviera fuera del lugar de monitoreo.

### **2.1.6 Desventajas**

No presenta una mayor desventaja ya que es una herramienta fácil de usar y de manipular, además se le puede añadir herramientas como sea necesario, pero para algunos usuarios estas mejoras podrían ser vista como una desventaja ya que si se le añade demasiados plugins puede que el administrador de Red no esté capacitado en manipular todas las aplicaciones que nos brinda OSSIM.

Otra de las desventajas es que esta herramienta solo almacena los logs en los cuales están todos los problemas e inconvenientes que pasa en la red y en los servidores, y solo los reporta a la persona encargada. La aplicación no realiza ninguna acción para impedir los ataques como por ejemplo el simple hecho de una contraseña mal ingresada.

### **2.1.7 Compatibilidad**

OSSIM fue creado bajo el lenguaje de debían y está hecho para funcionar en plataformas Linux ya sea de 32 o 64 bits según crea

necesario el administrador IT, al ser una aplicación robusta necesita que el hardware donde se va a instalar sea potente para aprovechar el máximo desempeño.

Unos de los requerimientos de mayor importancia es la tarjeta de red que vamos a utilizar, se recomienda tener la marca Intel (R) porque es compatible con el núcleo de Linux y permitirá que la herramienta funcione normalmente.

Podemos decir que para el Mainboard puede ser indiferentes, solo el requisito para la placa seria que soporte procesadores Pentium y controladores para Linux.

Con respecto a los discos duros, OSSIM se instala en sata o IDE particionado con los requerimientos que tienen que tener y se lo muestra a continuación: *“/boot 100mb ext3 / 1 GB ext3 con lvm /var 4 GB ext3 con lvm /usr 2 GB ext3 con lvm /home 140 GB ext3 con lvm swap 1 GB.”*

En cuanto con la compatibilidad requerida de software tiene que contar lógicamente con una distribución Linux que contenga Apache2, Php4 o Php5.

## 2.2 Componentes y Arquitectura

### 2.2.1 Ossim-server

Como toda aplicación, Ossim funciona con un estándar cliente servidor y es obligatorio tener un solo servidor en toda nuestra red en el cual al instalar el perfil server (servidor) estamos configurando el ambiente que se encargue de procesar y recoger todos los logs que son generados por los diferentes dispositivos y servidores de nuestra red interna.



Figura 2.2 Arquitectura Ossim Server

Toda información que se genera mediante el continuo monitoreo que se da en la red se almacena en una base de datos, en el cual nuestro servidor procesa toda la información, esto permite que el administrador de red realice las correcciones necesarias para obtener un reporte más eficiente.

Los puertos que OSSIM utiliza para la comunicación son:

- ✓ Por default utiliza el 40001 y 40002 TCP entrantes con el cual se comunica con todos los agentes que están integrados y obtener los id de cada uno de los sucesos que se presenta.
- ✓ Para interactuar con la base de datos MYSQL es el 3306 de salida.
- ✓ Ossim puede ser administrado vía comando mediante conexión remota atreves del puerto 22 (SSH)
- ✓ Permite la administración atreves de interfaz web utilizando el puerto seguro 443 (HTTPS).

PUERTOS	ESTADO	SERVICIOS
40001-40002 TCP	Abierto	
3306 TCP	Abierto	MYSQL
22 TCP	Abierto	SSH
443 TCP	Abierto	HTTPS
25 TCP	Abierto	SMTP
80 TCP	Abierto	HTTP
8080	Abierto	HTTP-PROXY

Tabla 2 Tabla de Puertos de comunicación



### 2.2.2 Ossim-framework

Esta herramienta sirve como intermediario para que la aplicación web del servidor no haga tareas en segundo plano como la lectura y escritura de la información que recibe, evitando así un innecesario uso de requerimiento como memoria y almacenaje y optimizar su funcionalidad. También permite acceder a la base de datos de conocimiento de Ossim y a la base de datos de los eventos guardamos.

Podemos mencionar que los propósitos primordiales de esta herramienta son los siguientes:

- ✓ *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*

### 2.1.1. Diagrama de funcionamiento del Ossim-framework

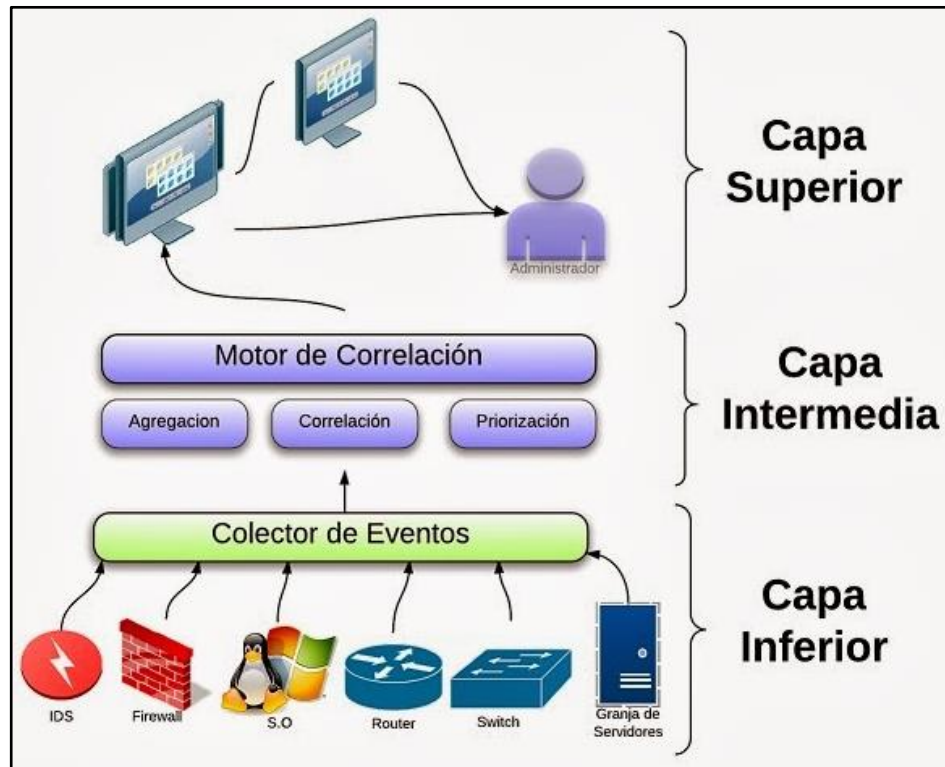


Figura 2.3 Ossim Framework

En el diagrama se puede observar como OSSIM- FRAMEWORK siendo la capa intermedia en la demostración, interactúa con los plugins o recolectores de la información y esta información es presentada al usuario mediante la interfaz web del server.

### 2.2.3 Ossim-agent

El nombre de Agent en la herramienta Ossim se les da a los plugins y aplicaciones que permite analizar todos los eventos específicos que se generan en la red de trabajo o en los diferentes servidores en la cual se está haciendo el monitoreo y seguimiento.

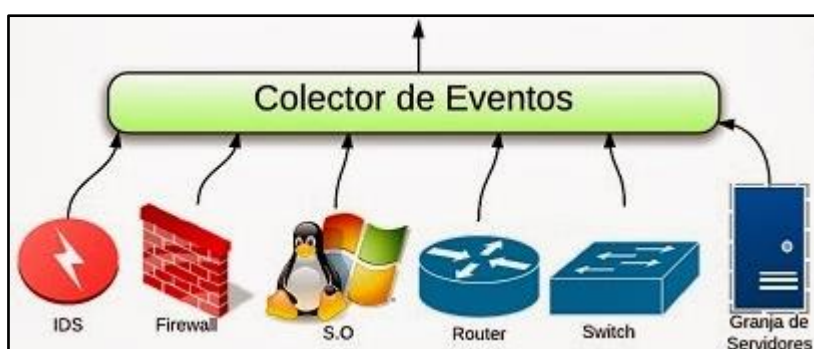


Figura 2.4 Agentes de Ossim

En un ambiente Windows es muy fácil agregar los agents para así tener un mayor control y un mejor mecanismo en cuanto a nuestros requerimientos, uno de los Agent que se utiliza es “Deploying HIDS”, este Agent puede realizar funciones de forma centralizada, una comunicación de cliente-servidor mediante SSL y se puede llegar a crear de forma personalizada el funcionamiento de HIDS, este agent también es compatible con Linux.

Otro Agent muy utilizado es "OSSEC-CLIENT", fácil de instalar y recolecta información de los eventos principales de los sistemas operativos, este agent es de libre distribución y licenciamiento y está disponible para Linux, MacOS, Solaris, HP-UX, AIX y Windows.

Syslog es otro agent muy utilizado para poder enviar eventos de un ordenador Linux a un syslog remoto con el cual cuentan casi todas las distribuciones, además en caso de no tener instalados estos paquetes se encuentran en los repositorios y fáciles de configurar, los agentes más utilizados son rsyslog y syslog-ng.

Rsyslog es otra forma de obtener información desde los diferentes dispositivos de red, esta herramienta fue creada como un syslog básico y la misma se ha ido adaptando para poder ser un aplicación muy robusta que puede entregar más de un millón de mensajes por segundo.

Los plugins son los agents que hacen fácil la recopilación de la información desde cualquier dispositivo que se encuentra en la red, mientras más plugins instalados existan, podemos contar con un sistema totalmente distribuido. Estos son los principales plugins que me permiten tener una visión de toda la red:

- **Snort:** Permite tener una actualización de firmas diarias en todos los OSSIM-AGENT que esten instalados.
- **Arpwatch:** Nos permite tener un monitoreo en la capa 2 del modelo OSI y evitar cualquier problema con direcciones MAC.
- **Ocs-NG:** Permite tener un inventario de los equipos que se encuentra en nuestra Red en tiempo real, el mismo puede ser soportado en diferentes sistemas operativos como *Linux, MacOS, Solaris, HP-UX, AIX y Windows.*

#### 2.2.4 Arquitectura de OSSIM

Esta herramienta de monitorización tiene una arquitectura abierta, compuesta por varios aplicativos antes mencionados y está en un amplio crecimiento en la tendencia de herramientas Open Source, siendo OsssimServer el eje central de esta arquitectura, se lo recomienda instalar en un lugar central de su red dando así un mayor alcance a todas las subredes de nuestra LAN, esto permite mejorar los tiempo de recepción y entrega de los logs, optimizando un mayor control a la hora de un problema eventual y a la vez mejorar su funcionalidad por los procesos que se realizan por separados en cada componente.

La arquitectura se divide en tres partes fundamentales y son:

- ✓ **EDB:** Base de Datos de Eventos, se almacena todo los logs que se puede generar en el monitoreo, es una pieza clave dado que esta base de datos servirá al administrador para obtener los reportes de las diferentes alarmas que se generarán en nuestra red.
- ✓ **KDB:** Base de Datos de Framework, se almacena los diferentes paquetes que sirve para poder identificar la información que se genera en los distintos host que están en nuestra red, y en los hosts que se aplicada las políticas de seguridad.
- ✓ **UDB:** Base de Datos de los Perfiles, aquí se almacena toda la información o datos que se proporciona al estar en un constante monitoreo y así poder aprender de los datos y tomar las precauciones necesarias a futuro.

## 2.2.5 Diagrama de la Arquitectura de Ossim

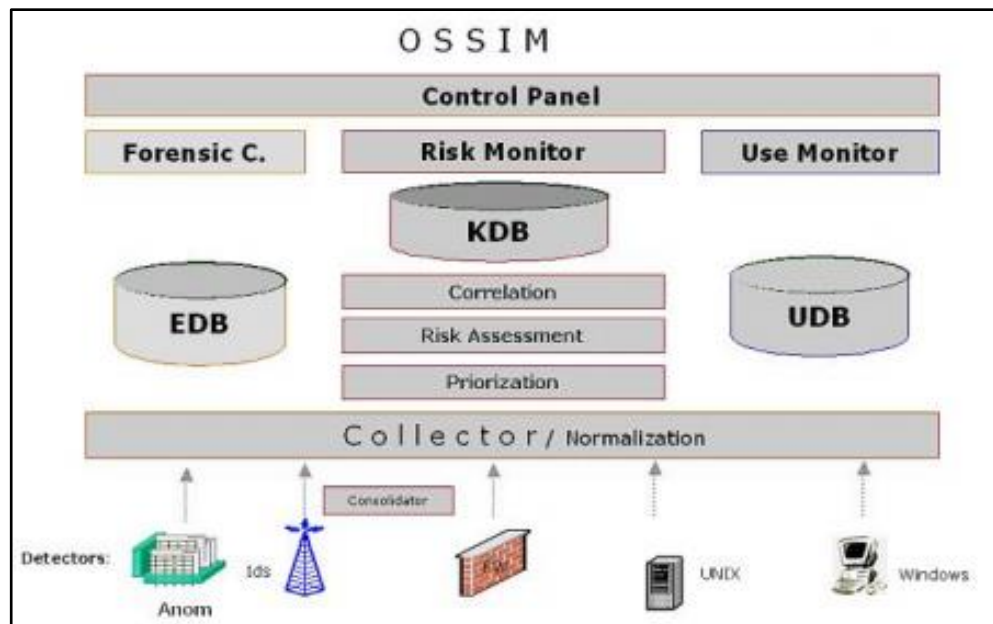


Figura 2.5 Arquitectura de Ossim

En el Diagrama se puede observar el funcionamiento de las tres bases de datos principales de OSSIM, la correlación que tienen entre si y como se hace el proceso desde la recepción de la información de los agentes y la respectiva presentación mediante la interfaz Web hacia el administrador de la red.

## 2.3 Tipos de monitoreo

### 2.3.1 Arpwatch

Utilizado para las anomalías en dirección Mac y corre en plataformas Linux, esta es una herramienta que solo puede monitorear subredes

dado que los paquetes ARP que monitoreo no permite el tráfico de Vlan a Vlan, esto hace que seamos cuidadosos al usar esta aplicación y se recomienda utilizarla en los ambientes más críticos de la red.

Al ser una herramienta Linux su funcionamiento e Instalación está en todos los repositorios de las principales distribuciones como Ubuntu, OpenSuSe, Fedora, Slackware, Debían, entre otras, en caso no estar embebido el paquete podrá instalarse directamente, una vez instalada las aplicación tenemos que realizar las respectivas configuraciones en el archivo "Arpwatch".

Esta herramienta funciona con el emparejamiento de las direcciones IP con las direcciones MAC de los host de manera que se muestra cuando hay una anomalía en esta estrategia o en algún ataque de ARP, también se puede configurar para que pueda enviar un correo electrónico al Administrador de red para notificar el emparejamiento o cambio que presente en la aplicación.

### **2.3.2 Pads**

Pads, cuyo significado es Passive Asset Detection System está basado en la detección de activos como nuevos host o los servicios que se está ejecutando en la red, utilizando la dirección Mac para



traducir al nombre del fabricante y enviar esta información a los servidores de almacenaje de los logs.

Pads fue hecho y relacionado para complementarse con la tecnología IDS (Sistema de detención de intruso) dando a conocer las alertas que suelen suceder en la red.

### 2.3.3 Openvas

En su principios también conocido como GNessus de su variante de escaneo de seguridad de Nessus y es una herramienta que se integra a Ossim para el escaneo y gestión de vulnerabilidad de seguridad de sistemas informáticos, esta herramienta presenta dos métodos o tipos de evaluación, una que se orienta a la red y otro al host.

- ✓ **Escaneo a la red:** El escaneo de la red se da mediante la localización de todos los sistemas que están funcionando en nuestra red y todos los servicios que se están ejecutando, este tipo de evolución puede ser fácilmente escalable según los requerimientos del Administrador de Red.
- ✓ **Escaneo al Host:** Este escaneo mediante host se da únicamente en los host que está instalado la herramienta con el cual hace un informe detallado sobre los puertos que están

abierto enviando una “Bacteria” para saber que host son vulnerables.

#### **2.3.4 Spade**

Motor de estadística de paquetes para detención de anomalías, se usa para obtener conocimiento sobre los ataques sin firmas, ¿Que es un ataque sin firma?, definimos que son paquetes enviados a los servidores de servicios sin poder asegurar su integridad, los mismos paquetes pueden contener algún tipo de virus, malware o algo similar.

#### **2.3.5 Tcptrack**

Utilizado para analizar datos de la sesión de información útiles en la detención de ataques, también conocido como el “TOP” de las conexiones TCP en unix, maneja una función de snifer para así visualizar todas la conexiones y el ancho de banda que se realiza en una interfaz determinada, se maneja también para dar un seguimiento al estado de una interfaz, este test muestra el origen y destino de los paquetes o conexiones, estado de conexión, tiempo de inactividad y uso del ancho de banda.

Client	Server	State	Idle	Speed
172.23.195.11:48328	67.39.222.44:22	ESTABLISHED	0s	38 KB/s
172.23.195.11:48646	196.30.80.10:80	ESTABLISHED	1s	30 KB/s
172.23.195.11:48661	64.37.246.17:80	ESTABLISHED	0s	387 B/s
172.23.195.11:48620	216.239.39.99:80	RESET	2s	0 B/s
128.230.225.95:3531	172.23.195.10:1220	ESTABLISHED	5s	0 B/s
172.23.195.11:48621	216.239.39.99:80	ESTABLISHED	7s	0 B/s
172.23.195.11:48606	64.233.167.99:80	ESTABLISHED	10s	0 B/s
172.23.195.11:48014	67.39.222.44:22	ESTABLISHED	16s	0 B/s
172.23.195.11:47988	67.39.222.44:22	ESTABLISHED	18s	0 B/s
TOTAL				69 KB/s
Connections 1-9 of 9				Unpaused Sorted

Figura 2.6 Tcptrack

### 2.3.6 Ntop

Es una herramienta muy popular en open source para el monitoreo del tráfico en la red que funciona en múltiples plataformas como Linux y Windows, esta herramienta proporciona información muy valiosa sobre el tráfico que se genera en la red y puede ser utilizada de una forma muy proactiva ya para analizar el tráfico normal y malicioso.

Esta herramienta da los resultados en tiempos reales y es útil para tener un control de todos los usuarios que acceden a nuestra red.

Los protocolos que pueden ser monitoreados son: TCP/UDP/ICMP, ARP, DLC, AppleTalk, Netbios, además en los paquetes TCP/UDP es capaz de agruparlos por FTP, HTTP, DNS, Telnet, SMTP/POP/IMAP entre otros.

### 2.3.7 NfSen

Visor de flujo de la red para la detección de anomalías, proporciona una interfaz gráfica que trabaja vía web y está basado para las herramientas Netflow y Nfdump que han sido modificadas para integrarse con los demás aplicativos de Ossim, esta herramienta puede trabajar en ambientes Linux y Windows, trabaja mediante líneas de comando y brinda una gama de características como:

- ✓ Fácil de navegar a través de los datos de NetFlow.
- ✓ Procesar los datos NetFlow en un tiempo especificado.
- ✓ Crear un historial, así como perfiles continuos.
- ✓ Establecer alertas, basado en diversas condiciones.

Como esta herramienta funciona sobre la base de NFDUMP conoceremos más sobre que función realiza esta aplicación para así conocer más sobre NFSen.

**Nfdump:** Es la acumulación o conjunto de herramientas encargadas de recolectar y procesar flujos de datos en la red en la que ha sido configurada.

Algunas de las herramientas con las que cuenta son:

- ✓ **Nfcapd**, Es un Script que captura el flujo de red. Lee datos que viajan y los almacena en archivos.
- ✓ **Nfdump**, Esta herramienta sirve como visualizador de los datos almacenados por nfcapd, puede crear varias estadísticas del tipo "top N" basado en datos IP, Ports, etc.
- ✓ **Nfprofile**, Lee los datos almacenados por nfcapd, estos datos son filtrados y se almacenan en nuevos archivos.
- ✓ **Nfreplay**, Esta es una herramienta simple que hace forward a los datos almacenados hacia otros hosts.
- ✓ **Nfclean**, Permite eliminar datos viejos que son guardados.

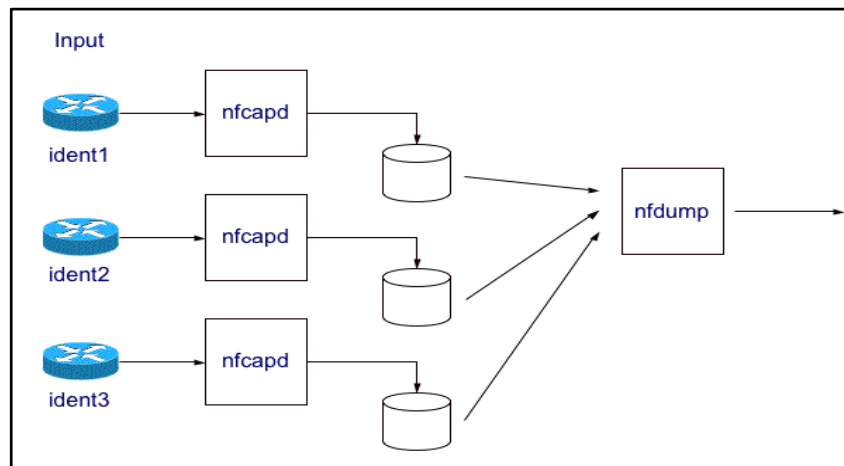


Figura 2.7 Funcionamiento del NfSen

Este diagrama explica el funcionamiento general de las herramientas que integra NFDUMP.

### 2.3.8 Osiris

Es un sistema de detención de intruso basado en host HIDS y Snare quien colecciona los log de los sistemas Windows. Osiris en su funcionamiento monitorea a los equipos con sistemas operativos Windows y hace un seguimiento en la red. La arquitectura de Osiris se basa en tres componentes:

- ✓ **Consola de administración (osirisimd):** Debe ser instalada y configurada en un equipo confiable ya que es a donde se va a almacenar la información de los equipos que están en nuestra red, incluyendo configuraciones, logs, y bases de datos.
- ✓ **Agente de Escaneo (osirisd):** Proceso que se va a correr en un equipo o host y su principal funcionalidad es de estar en un constante monitoreo al filesystem local y enviar la información al servidor que almacena los logs.
- ✓ **Aplicación de Administración CLI (osiris):** la utiliza el administrador para administrar los detalles de los hosts escaneados.

## 2.4 Licenciamiento

### 2.4.1 Costo

La herramienta tiene dos distribuciones, una versión gratuita y una versión profesional que es pagada, se presenta a continuación los módulos que contiene cada una de las versiones.

	Open Source OSSIM	Professional SIEM
<b>Support</b>	Community	7x24
<b>Quality Assurance</b>	Community	Professional Q&A
<b>Security</b>	Not audited	Audited
<b>Performance</b>	Moderate	30 x Open Source, Assured
<b>SIEM Intelligence</b>	Logical Correlation	Cross Correlation
	Simple Taxonomy	Rich Taxonomy
<b>Logger</b>	N/A	Unlimited Forensic Storage
<b>Reports</b>	< 25 + Jasper	> 200 + Web Wizard
<b>Scalability/HA</b>	N/A	HA, Distributed ,Multitenant, Unlimited
<b>Compliance</b>	High Level Reports	High and Low Taxonomy-based
<b>Updates</b>	None	Daily rules and reports
<b>User Management</b>	Individual, simple controls	Templates and Granular Controls

Tabla 3 Costo de Ossim

Ossim funciona como una estrategia de marketing, dándose a conocer una versión gratis, buena, confiable y robusta, permitiendo hacer una gran cantidad de monitoreo y estar informado de forma rápida lo que sucede en nuestra red de trabajo y, si en caso que se necesite

soporte online o características adicionales existe la versión profesional que cuenta con mejoras en base al Ossim gratuito.



## **CAPÍTULO 3**

### **3 FASE DE IMPLEMENTACIÓN**

#### **3.1 Instalación cliente y servidor**

##### **3.1.1 Requisitos técnicos para la instalación del servidor OSSIM**

Los requisitos de hardware para instalar OSSIM AlienVault dependerán en gran medida del número de eventos que tenga que procesar el servidor, de la cantidad de datos que pretendamos almacenar en la base de datos de OSSIM, y de la cantidad de hosts disponibles en la red que pretendamos analizar:

Como requisito mínimo son recomendables las siguientes características en el equipo físico donde se procederá con la instalación:

- ✓ Procesador de 1.5 Ghz doble núcleo o superior
- ✓ Memoria RAM de 2GB o superior
- ✓ Disco Duro de 40 GB libres o superior
- ✓ Tarjeta de Red 100/1000 Mbps
- ✓ Conexión a una red de Datos

### **3.1.2 Requisitos del personal administrador**

Para poder implementar la herramienta OSSIM y operar su funcionalidad es muy importante que el administrador cumpla con los siguientes conocimientos mínimos:

- ✓ Debe tener conocimientos fundamentales de seguridades informáticas.
- ✓ Debe tener conocimientos básicos en Sistemas operativos Linux.
- ✓ Debe tener conocimientos en Sistemas operativos Windows Server.
- ✓ Debe saber interpretan los logs generados por los diferentes eventos en los sistemas operativos.
- ✓ Debe Tener conocimientos básicos del modelo TCP/IP

- ✓ Debe tener conocimientos básicos de Redes LAN/WAN.
- ✓ Debe tener conocimientos de seguridades en redes de Datos.
- ✓ Debe saber interpretar gráficos estadísticos de reportes.

### **3.1.3 Instalación de OSSIM**

Para proceder con una instalación óptima de la herramienta OSSIM es necesario seguir los siguientes pasos de forma ordenada.

- ✓ Primero descargarse el archivo iso desde el sitio oficial de ossim
- ✓ Quemar la imagen .iso en un CD
- ✓ Arrancar o iniciar el boot desde el CD en el equipo donde se va a instalar.
- ✓ A continuación seguir el wizard de instalación paso a paso, es muy similar a la instalación de una distribución de Linux.

### Pasos del Wizard para instalar OSSIM:

- ✓ Seleccionar la versión del OSSIM a instalar

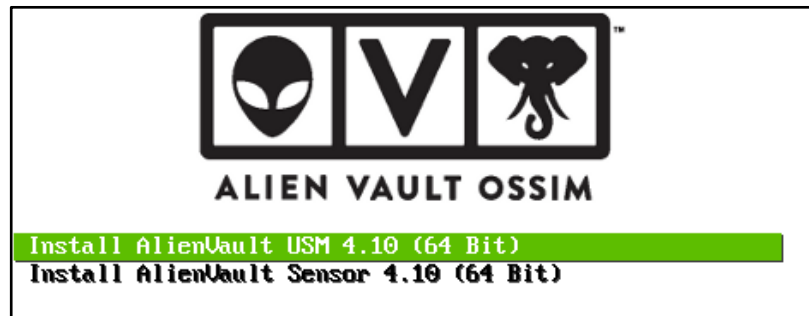


Figura 3.1 Seleccionar la versión de Ossim

- ✓ Seleccionar el idioma de la instalación



Figura 3.2 Selección de Idioma del Ossim

- ✓ Seleccionar el idioma del teclado

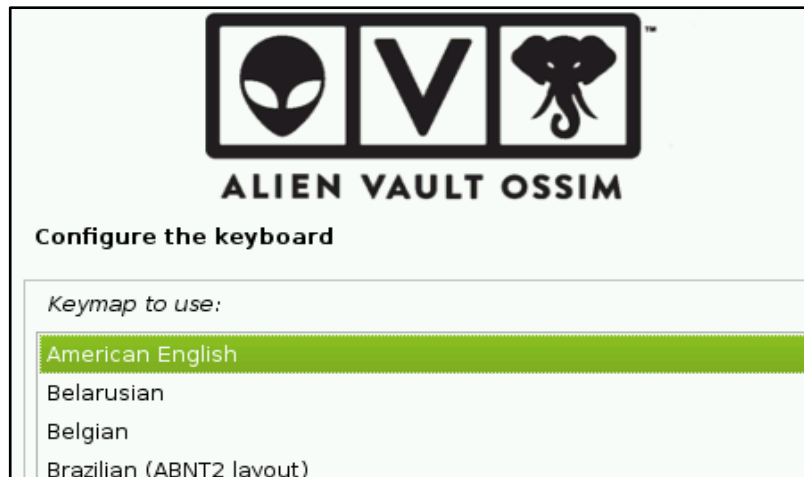


Figura 3.3 Selección de Idioma del teclado

- ✓ Configuración de la red para el servidor

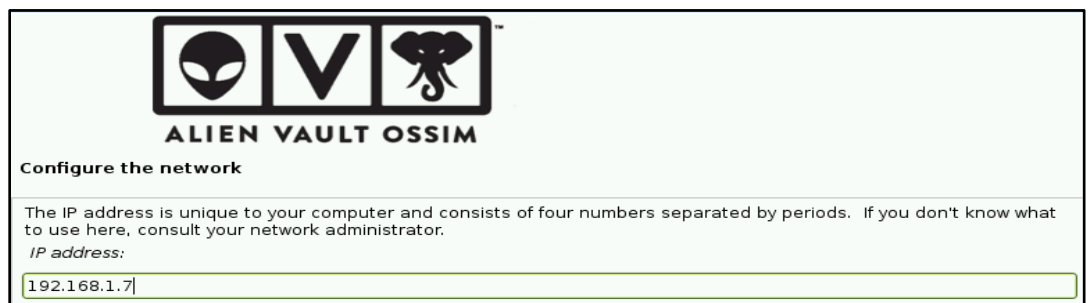
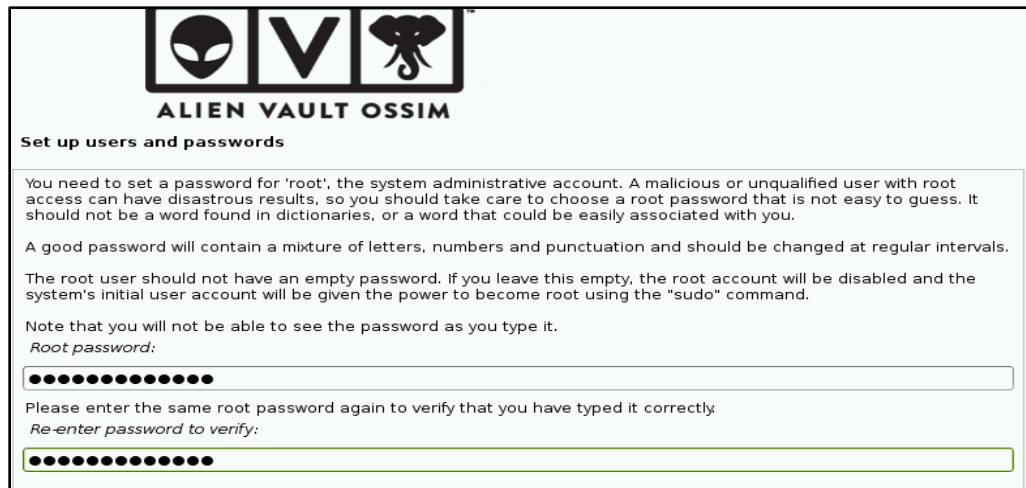


Figura 3.4 Configuración de la Red

## ✓ Configuración de contraseña de seguridad para acceder al servidor



The screenshot shows the 'Set up users and passwords' configuration screen for Alien Vault OSSIM. At the top, there is a logo consisting of three icons: an alien head, a 'V', and an elephant, with the text 'ALIEN VAULT OSSIM' below it. The main heading is 'Set up users and passwords'. The text explains that a password must be set for the 'root' user and provides guidelines for a strong password. It includes two password input fields: one for the root password and another for verification. The password fields are currently filled with black dots.

**ALIEN VAULT OSSIM**

**Set up users and passwords**

You need to set a password for 'root', the system administrative account. A malicious or unqualified user with root access can have disastrous results, so you should take care to choose a root password that is not easy to guess. It should not be a word found in dictionaries, or a word that could be easily associated with you.

A good password will contain a mixture of letters, numbers and punctuation and should be changed at regular intervals.

The root user should not have an empty password. If you leave this empty, the root account will be disabled and the system's initial user account will be given the power to become root using the "sudo" command.

Note that you will not be able to see the password as you type it.

Root password:

●●●●●●●●●●

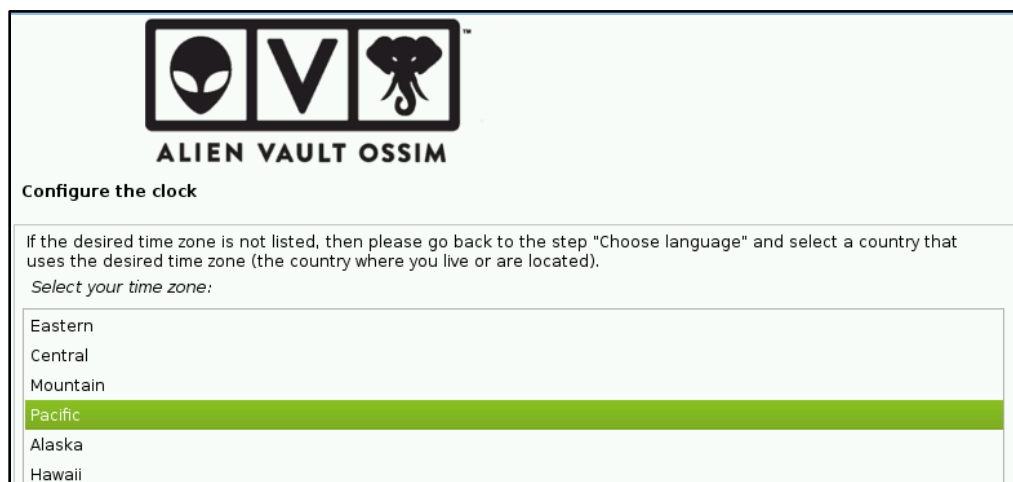
Please enter the same root password again to verify that you have typed it correctly.

Re-enter password to verify:

●●●●●●●●●●

Figura 3.5 Establecer contraseña

## ✓ Configuración regional



The screenshot shows the 'Configure the clock' configuration screen for Alien Vault OSSIM. At the top, there is a logo consisting of three icons: an alien head, a 'V', and an elephant, with the text 'ALIEN VAULT OSSIM' below it. The main heading is 'Configure the clock'. The text explains that if the desired time zone is not listed, the user should go back to the 'Choose language' step. It includes a list of time zones with 'Pacific' selected and highlighted in green.

**ALIEN VAULT OSSIM**

**Configure the clock**

If the desired time zone is not listed, then please go back to the step "Choose language" and select a country that uses the desired time zone (the country where you live or are located).

Select your time zone:

- Eastern
- Central
- Mountain
- Pacific**
- Alaska
- Hawaii

Figura 3.6 Configuración de la Región

- ✓ Finalmente hay que esperar que se copien los archivos necesarios para el funcionamiento hasta que salga el mensaje de finalización.

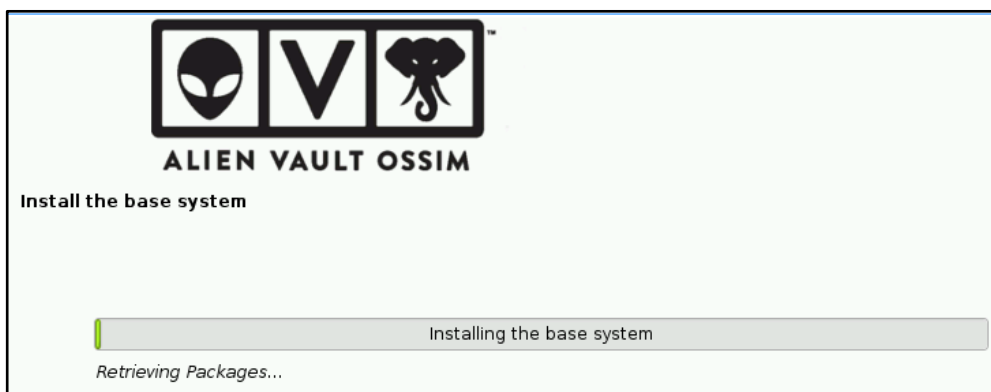


Figura 3.7 Copia de Archivos Necesarios Para la Instalación

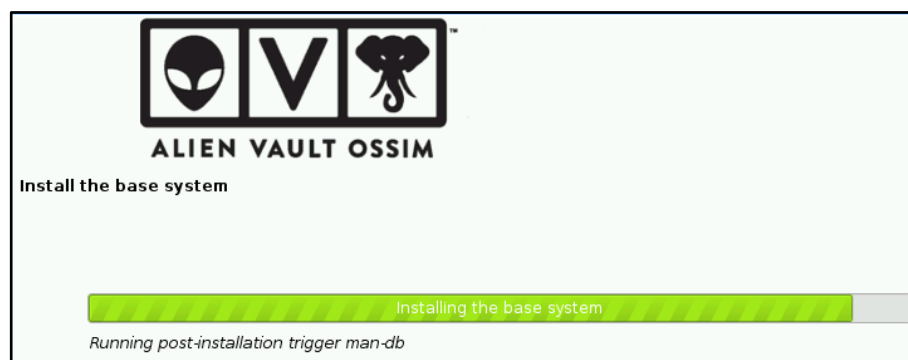


Figura 3.8 Terminando la Copia de Archivos Necesarios

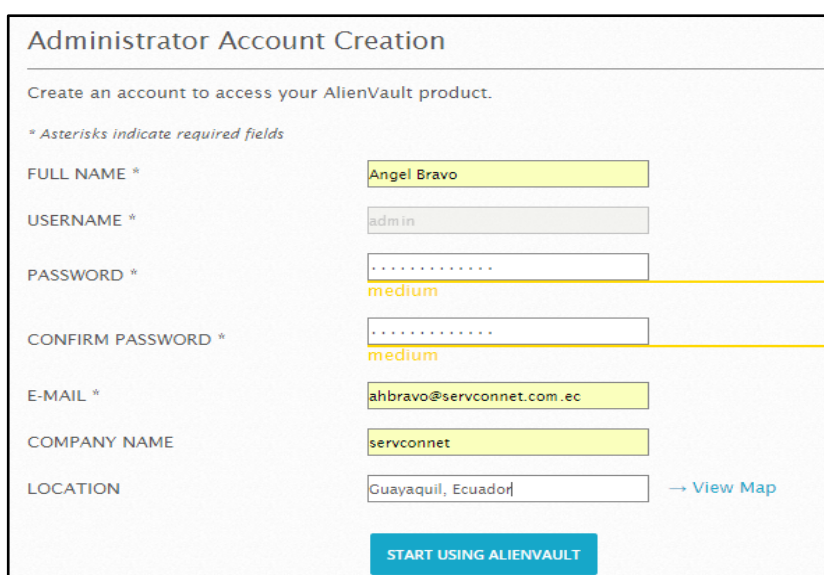
### 3.1.4 Parámetros de configuración en el servidor

Al terminar la instalación, por default se levantan algunos servicios y plugins de OSSIM, por ende es importante configurar los demás plugins y características con parámetros personalizados como:

- ✓ **Configuración de red:** En esta parte de configuración lo que más resalta y es de suma importancia que el servidor

tenga configuraciones estáticas de dirección IP, dirección del Gateway, dirección del DNS y el nombre del servidor.

- ✓ **Configuración Acceso Web:** En esta sección se procede a crear una cuenta para acceder a la interfaz web de administración, se recomienda que la cuenta creada sea la información del administrador de la red.



**Administrator Account Creation**

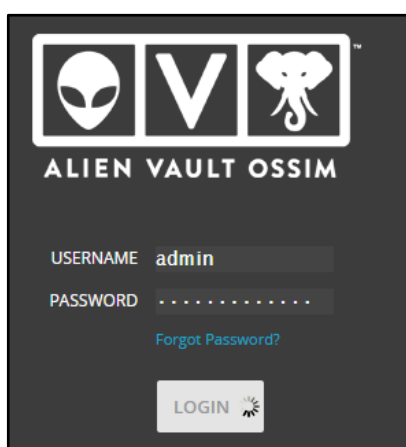
Create an account to access your AlienVault product.

*\* Asterisks indicate required fields*

FULL NAME *	Angel Bravo
USERNAME *	admin
PASSWORD *	..... medium
CONFIRM PASSWORD *	..... medium
E-MAIL *	ahbravo@servconnet.com.ec
COMPANY NAME	servconnet
LOCATION	Guayaquil, Ecuador <a href="#">→ View Map</a>

**START USING ALIENVAULT**

Figura 3.9 Configuración de Acceso Web



**ALIEN VAULT OSSIM**

USERNAME admin

PASSWORD .....

[Forgot Password?](#)

**LOGIN**

Figura 3.10 Ingresando a OSSIM Web



### 3.1.5 Configuración de servicios y plugins en el servidor

#### 3.1.5.1 Configuración del Plugin OSSEC

Dentro de OSSIM es necesario configurar el servicio OSSEC, este servicio permite recolectar la información de clientes externos en servidores Windows y Linux. Para configurar este servicio es necesario conectarse remotamente al servidor vía ssh y a continuación ingresar a la ruta del archivo de configuración de ossec “#cd /var/ossec/bin/” y ejecutar el script “./manage\_agents”.

```
srv-ossim:/var/ossec/bin# ./manage_agents

*****
* OSSEC HIDS v2.7 Agent manager.          *
* The following options are available:    *
*****
(A)dd an agent (A) .
(E)xtract key for an agent (E) .
(L)ist already added agents (L) .
(R)emove an agent (R) .
(Q)uit.
Choose your action: A,E,L,R or Q: █
```

Figura 3.11 Configuración de Plugins

A continuación procedemos añadir un agente presionando la opción “A”, después debemos crear un nombre para identificarlo en nuestra consola web, asignarle una dirección IP donde estará instalado nuestro agente y finalmente presionamos “Y” para confirmar la asignación correcta del agente.

```

Choose your action: A,E,L,R or Q: A
- Adding a new agent (use '\q' to return to the main menu).
Please provide the following:
* A name for the new agent: Antivirus-Console-Server
* The IP Address of the new agent: 192.168.1.14
* An ID for the new agent[001]:
Agent information:
ID:001
Name:Antivirus-Console-Server
IP Address:192.168.1.14
Confirm adding it?(y/n): y

```

Figura 3.12 Creación del Agente

```

Choose your action: A,E,L,R or Q: A
- Adding a new agent (use '\q' to return to the main menu).
Please provide the following:
* A name for the new agent: Samba-Linux-Server
* The IP Address of the new agent: 192.168.1.7
* An ID for the new agent[002]: y

```

Figura 3.13 Asignación de IP de Los Agentes

- ✓ **Generación de Authentication Key:** El servidor OSSEC siempre genera una clave de autenticación que debe ser copiada en los clientes al momento de su instalación y de esta forma se establece la comunicación entre servidor y cliente OSSEC.

```

*****
(A)dd an agent (A).
(E)xtract key for an agent (E).
(L)ist already added agents (L).
(R)emove an agent (R).
(Q)uit.
Choose your action: A,E,L,R or Q: E
Available agents:
  ID: 001, Name: Antivirus-Console-Server, IP: 192.168.1.14
  ID: 002, Name: Samba-Linux-Server, IP: 192.168.1.7
Provide the ID of the agent to extract the key (or '\q' to quit): 001
Agent key information for '001' is:
MDAxIEFudG12aXJ1cy1Db25zb2x1LVNlcnZ1ciAxOTIuMTY4LjEuMTQgZWxNTQyOWViMzI
ZTE5MjUwNDk0ODFkZGY2ODE0MjRkZGI1ZTdmMjgzMzNiM2NiMjI4MjczNDUyNg==

```

Figura 3.14 Generar Autenticación Ossec

✓ **Asignación del servidor en el panel de administración:**

Antes de ver los cambios en la consola web, es necesario reiniciar el servicio ossec con los comandos “service ossec restart” y luego dirigirnos a la consola y verificar que el cliente ossec este agregado y activo.



Figura 3.15 Panel de Administración Ossec

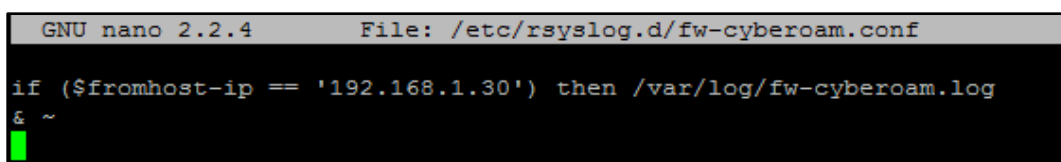
### 3.1.5.2 Configuración del servicio Rsyslog

Para poder recolectar los logs generados por los diferentes dispositivos de red como switches, router y firewalls es importante añadir este servicio, es indispensable que los dispositivos permitan la configuración de envío de logs a un servidor RSYSLOG, en este ejemplo se va a configurar un Switch cisco SF-200 y un Firewall Cyberoam 50iNG

✓ **Configurando Rsyslog para Firewall Cyberoam 50 iNG:**

Para poder receptor logs desde un equipo cyberoam hacemos uso de un plugin predeterminado de OSSIM y para aquello procedemos a conectamos a la consola ssh del servidor 192.168.1.30

A continuación nos dirigimos a la ruta de configuración del archivo donde se van añadir los logs que vienen del firewall y escribimos el código respectivo de redirección “nano /etc/rsyslog.d/fw-cyberoam.conf”



```
GNU nano 2.2.4 File: /etc/rsyslog.d/fw-cyberoam.conf
if ($fromhost-ip == '192.168.1.30') then /var/log/fw-cyberoam.log
& ~
```

Figura 3.16 Configuración del Rsyslog

Después de configurar el archivo es necesario reiniciar el servicio rsyslog para que acepte la configuración “/etc/init.d/rsyslog restart”, también es importante configurar un script de rotación de archivos para que mantenga un orden al momento de la presentación en la interface web de OSSIM.

Procedemos a la creación del archivo rotation en la ruta “nano /etc/logrotate.d/fw-cyberoam”

```
GNU nano 2.2.4      File: /etc/logrotate.d/fw-cyberoam
/var/log/fw-cyberoam.log
{
rotate 4 # save 4 days of logs
daily # rotate files daily
missingok
notifempty
compress
delaycompress
sharedscripts
postrotate
invoke-rc.d rsyslog reload > /dev/null
endscript
}
```

Figura 3.17 Script de rotación de Archivo

Finalmente para terminar con la configuración del firewall procedemos a la verificación de lectura de los logs y ver si están llegando en el archivo especificado.

```
srv-ossim:/etc/ossim/agent/plugins# tail /var/log/fwcyberoam.log -f
Nov 16 10:12:29 192.168.1.6 date=2014-11-16 time=10:12:32 timezone="ECT" device_
name="CR50iNG" device_id=C16213285432-83VU3H log_id=062009517505 log_type="Event
" log_component="GUI" log_subtype="Admin" status="Successful" priority=Notice us
er_name="LOCAL" src_ip=127.0.0.1 message="Registration information of 'WAF' were
updated by 'LOCAL' from '127.0.0.1' using 'LOCAL'"
```

Figura 3.18 Verificación de la Lectura de los Logs

✓ **Configurando Rsyslog para un Switch cisco SF-200:**

Siguiendo el procedimiento anterior del cyberoam, ahora procedemos a establecer un archivo donde se almacenaran los logs generados en el equipo cisco: “/etc/rsyslog.d/sw-cisco1.conf”

```
GNU nano 2.2.4 File: /etc/rsyslog.d/sw-cisco1.conf
if ($fromhost-ip == '172.16.1.5') then /var/log/sw-cisco1.log
& ~
```

Figura 3.19 Configuración Rsyslogs Para Switch Cisco

A continuación procedemos a reiniciar el servicio rsyslog “/etc/init.d/rsyslog restart”, y no olvidar la importancia de configurar un script de rotation de archivos, lo creamos en “/etc/logrotate.d/sw-cisco1”

```
GNU nano 2.2.4 File: /etc/logrotate.d/sw-cisco1
/var/log/sw-cisco1.log
{
rotate 4 # save 4 days of logs
daily # rotate files daily
missingok
notifempty
compress
delaycompress
sharedscripts
postrotate
invoke-rc.d rsyslog reload > /dev/null
endscript
}
```

Figura 3.20 Reiniciar el Rsyslog

Finalmente para terminar con la configuración del Switch procedemos a la verificación de lectura de los logs y ver si están llegando en el archivo especificado.

```
srv-ossim:/etc/ossim/agent/plugins# tail /var/log/sw-cisco1.log -f
Nov 16 11:52:06 172.16.1.5 %AAA-W-REJECT: New https connection, source 192.168.20.10 destination 172.16.1.5 REJECTED
```

Figura 3.21 Verificación de Lectura de los Logs del Switch

- ✓ **Configurando syslog desde un servidor Linux:** Para poder capturar los logs desde un servidor Linux, el procedimiento a seguir es el mismo que en los equipos anteriores, por ende la creación de un archivo personalizado es importante y lo haremos en la siguiente ruta “/etc/rsyslog.d/centralpbx.conf” y agregar el código respectivo.

```
if ($fromhost-ip == '172.16.1.160') then -/var/log/centralpbx.log
& ~
```

Figura 3.22 Configuración Syslog Linux

Finalmente para terminar con la configuración del servidor Linux procedemos a la verificación de lectura de los logs y ver si están llegando en el archivo especificado.

```
srv-ossim:/var/log# tail -f centralpbx.log
Oct 16 14:33:46 172.16.1.160 sudo:      root : TTY=pts/3 ; PWD=/home/abravo ; USER=root ; COMMAND=/bin/su
Oct 16 14:33:46 172.16.1.160 su: pam_unix(su:session): session opened for user root by abravo(uid=0)
```

Figura 3.23 Verificación de lectura de los Logs desde Linux

- ✓ **Configuración de disponibilidad con Nagios:** Para poder configurar la disponibilidad en los servidores, dispositivos de red o host y poder realizar el monitoreo es muy importante habilitar el Plugin NAGIOS que OSSIM trae incorporado, debemos seguir el siguiente procedimiento.

Seleccionamos el plugin Nagios.

```
Configure Data Source Plugins
Select Data Sources
lqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqq
x          [ ]  motorola-firewall
x          [ ]  mwcollect
x          [*]  nagios
x          [ ]  nepenthes
```

Figura 3.24 Configuración Plugin Nagios

A continuación realizamos una búsqueda de los Hosts desde ASSET en la consola web de OSSIM.



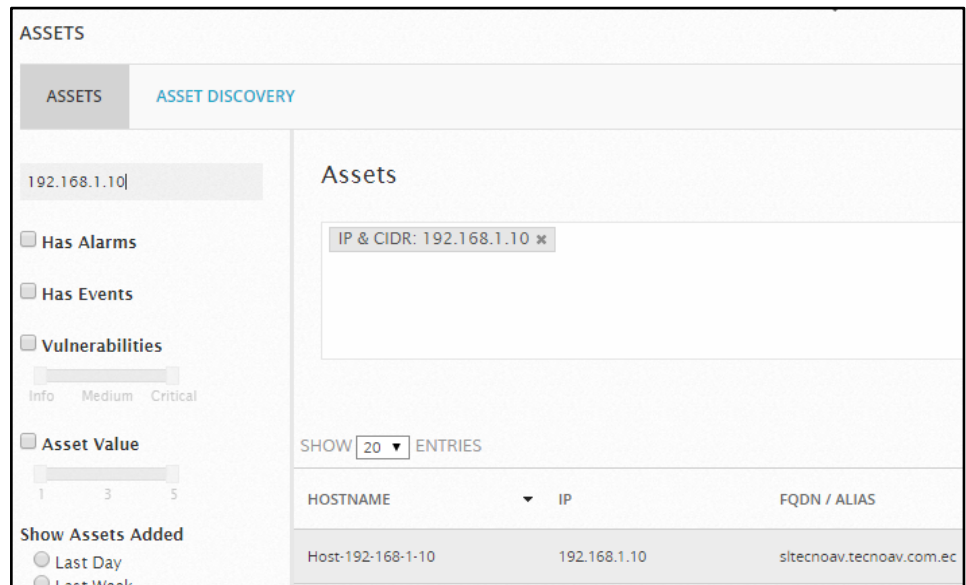


Figura 3.25 Búsqueda de Host desde ASSETT

Seleccionamos el Host y procedemos a la edición personalizada en donde habilitamos la configuración de disponibilidad (Availability Monitoring)

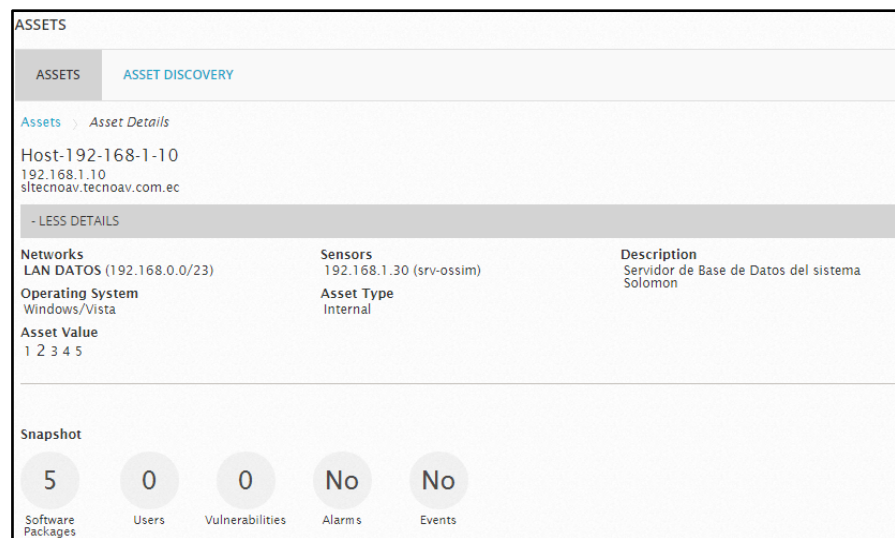


Figura 3.26 Configuración de Disponibilidad

EDIT

Name \*  
SRV-SOLOMON

IP Address \*  
192.168.1.10

FQDN/Aliases  
siltecnov.tecnov.com.ec

Asset Value \*  
2

External Asset \*  
Yes No

Sensors \*  
 192.168.1.30 (srv-ossim)

Description  
Servidor de Base de Datos del sistema Solomon

Thresholds \*  
C: 30 A: 30

Scan options  
 Availability Monitoring

Icon Allowed format: 16x16 png | jpg | gif image  
 Choose file ...

Location  
Guayaquil, Ecuador

Latitude/Longitud  
2.171 -79.9224

Devices Types  
Server HTTP Server ADD  
Server:HTTP Server

Figura 3.27 Activando Parámetros de Disponibilidad

Finalmente para dejar habilitado el monitoreo de Disponibilidad procedemos a guardar los cambios y nuestro servidor estará habilitado para ser monitoreado.

### 3.1.5.3 Configuración de los plugins CFG y SQL

Los plugins son los encargados de recibir toda la información que viene desde los dispositivos y servidores configurados para enviar logs, es importante activar los plugins necesarios como clientes recolectores existan.

- ✓ **Creando Plugin CFG:** La configuración de estos plugins se realizan en la ruta “etc/ossim/agent/plugins/”, se recomienda

hacer uso de los existentes y para nuestro ejemplo procedemos a realizar una copia del plugin ssh “cp ssh.cfg centralpbxssh.cfg” y a la configuración del mismo. Es en este plugin donde se relaciona los logs enviados desde el servidor Linux a la base de datos de OSSIM.

Los parámetros a editar en el plugin son: “plugin\_id=8001 y location=/var/log/centralpbx.log”, terminando la edición es importante reiniciar el servicio ssh.

```
[DEFAULT]
plugin_id=8001
dst_ip=_CFG(plugin-defaults,sensor)
dst_port=22

[config]
type=detector
enable=true
source=log
location=/var/log/centralpbx.log
create_file=true
```

Figura 3.28 Creación de Plugins CFG Central PBX

```
[DEFAULT]bash: c: command not found
plugin_id=8002

[config]
type=detector
enable=yes
source=log
location=/var/log/fwcyberoam.log
create_file=true
```

Figura 3.29 Creación de Plugins CFG Firewall

```
[DEFAULT]
plugin_id=8003

[config]
type=detector
enable=yes

source=log
location=/var/log/sw-cisco1.log

create_file=true
```

Figura 3.30 Creación de Plugins CFG Switch Cisco

- ✓ **Creando Plugin SQL:** La configuración de estos plugins se realiza en la ruta “/usr/share/doc/ossim-mysql/contrib/plugins/”, normalmente están en formato zip, y para poder utilizarlos se procede a descomprimir el paquete deseado con el comando “gunzip ssh.sql.gz” y después se procede a realizar una copia en la misma ruta, para nuestro ejemplo usamos el siguiente paquete “cp ssh.sql centralpbxssh.sql”. Es muy importante modificar las sentencias SQL para que tenga el mismo ID que tiene el archivo del “Plugin CFG” y la información se pueda relacionar.

```

-- SSHd
-- plugin_id: 8001

DELETE FROM plugin WHERE id = "8001";
DELETE FROM plugin_sid where plugin_id = "8001";

$('centralpbxsshd', 'SSHd: Secure Shell daemon');

INSERT IGNORE INTO plugin_sid (plugin_id, sid, category_id, class_id, name, pri$
INSERT IGNORE INTO plugin_sid (plugin_id, sid, category_id, class_id, name, pri$
INSERT IGNORE INTO plugin_sid (plugin_id, sid, category_id, class_id, name, pri$
INSERT IGNORE INTO plugin_sid (plugin_id, sid, category_id, class_id, name, pri$

```

Figura 3.31 Creación de Plugin SQL

Después de la modificación del archivo sql, procedemos a asignar el archivo a la base de datos de ossim utilizando el siguiente comando “ossim-db < centralpbxssh.sql” y verificamos que se haya insertado con éxito.

```

mysql> select * from plugin where id = 8001;
+-----+-----+-----+-----+-----+
| ctx          | id  | type | name          | description          |
| product_type | vendor |
+-----+-----+-----+-----+-----+
|              | 8001 | 1    | Central-pbx  | Elastix-SSH: Secure Shell daemon |
|              | 0    | NULL |              |              |
+-----+-----+-----+-----+-----+

```

Figura 3.32 Verificación de Logs de la Central PBX

```

mysql> select * from plugin where id = 8002;
+-----+-----+-----+-----+-----+-----+-----+
| ctx          | id  | type | name          | description          | product_type | vendor |
+-----+-----+-----+-----+-----+-----+-----+
|              | 8002 | 1    | Cyberoam     | Fw-50-iNG           |              | 0    | NULL |
+-----+-----+-----+-----+-----+-----+-----+

```

Figura 3.33 Verificación de Logs del Firewall





### 3.1.6 Instalación del cliente recolector de registros

Para recolectar los registros desde los servidores Windows se hace uso de un cliente cuyo nombre es OSSEC, este cliente ya fue especificado anteriormente y existen versiones para Linux y para Windows.

#### 3.1.6.1 Instalación del Cliente ossec en Windows.

Para instalar el agente es importante descargarse la versión para Windows desde el sitio oficial de OSSEC completamente gratis en el siguiente [link](#), a continuación ejecutar el setup descargado y seguir el proceso de instalación por default que se presenta, de la siguiente forma:



Figura 3.40 Instalación de Ossec en Windows



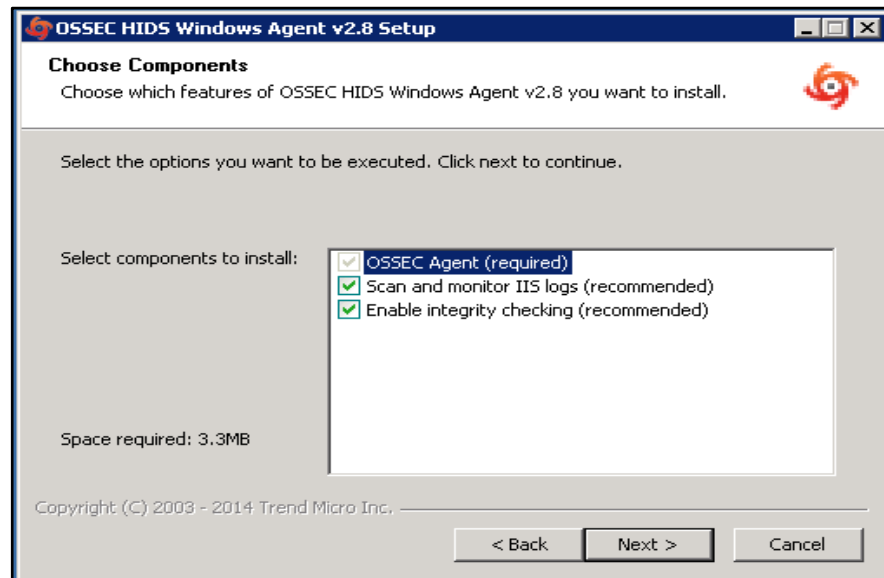


Figura 3.41 Selección de la Versión de Ossec

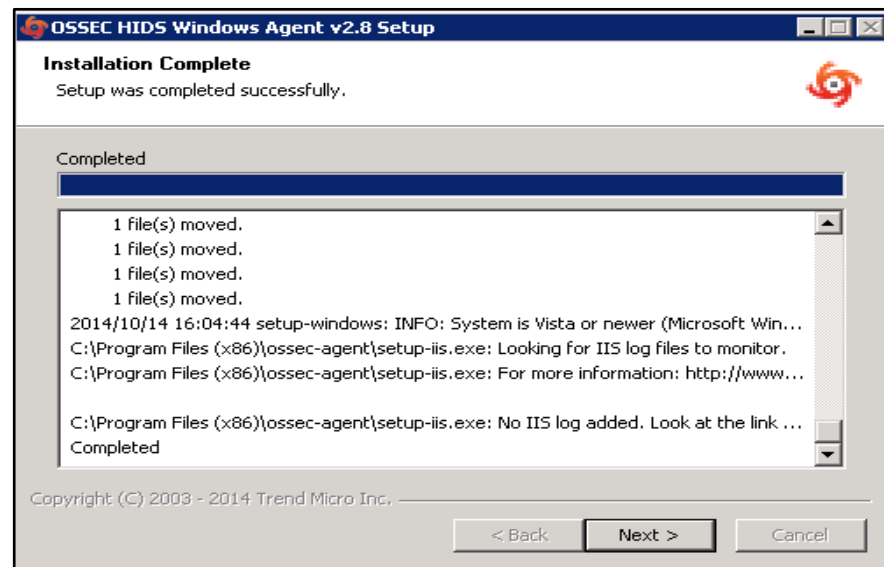


Figura 3.42 Instalación en curso Ossec

### 3.1.6.2 Configuración del cliente Rsyslog en Linux

Para poder reenviar los logs generados por los servicios que están rsyslog de Linux, para nuestro ejemplo haremos uso de nuestra Central PBX.

La configuración se la realiza en la ruta predeterminada de Linux en donde se establece el reenvío de todos los eventos generados por los diferentes servicios que está en “/etc/rsyslog.conf”, esta ruta puede cambiar dependiendo la distribución de Linux que esté utilizando y en otras ocasiones se tiene que instalar el paquete rsyslog con el siguiente comando “yum install rsyslog”.

A continuación hay que re-direccionar los registros del Linux a nuestro servidor OSSIM, esto se hace en el archivo syslog.conf o se puede crear un nuevo archivo personalizado y guardar los logs de determinados servicios y especificar la ruta adecuada en el syslog.conf con el comando “nano /etc/syslog.conf”.

```
local2.*                /var/log/sangoma_mgd.log

# Sangoma BRI Daemon (smg_bri) log
local3.*                /var/log/sangoma_bri.log

#REENVIO DE LOGS AL OSSIM
authpriv.* @192.168.1.30
```

Figura 3.43 Redireccionando los registros de Linux a Ossim

### 3.1.6.3 Configuración del Cliente Syslog en un Firewall Cyberoam.

Para poder reenviar logs a nuestro servidor OSSIM, es indispensable que el firewall soporte la configuración de un servidor externo rsyslog, el proceso de la configuración consiste en activar el rsyslog externo y reenviar determinada información a nuestro servidor.

.Los pasos empiezan por el inicio de sesión en el firewall.

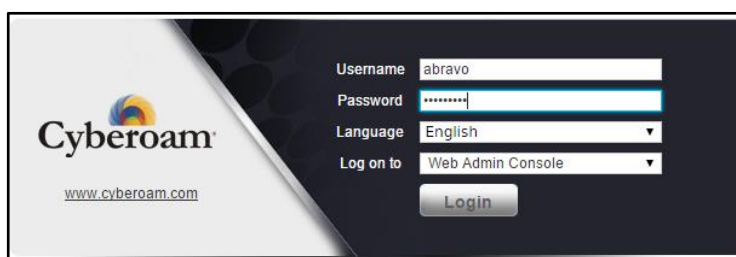


Figura 3.44 Configuración de Syslog en Cyberoam

A continuación crear un nuevo servidor syslog en donde se especifica la dirección Ip del server, el puerto 514 que es por default, se selecciona el tipo de log, el nivel y finalmente presionamos en "OK".

Figura 3.45 Creación de Nuevo Syslog en Cyberoam

#### 3.1.6.4 Configuración del Cliente Syslog en un Switch Cisco

Para poder reenviar logs a nuestro servidor OSSIM, es indispensable que el Switch soporte la configuración de un servidor externo rsyslog. El proceso de la configuración consiste en activar el rsyslog externo y reenviar determinada información a nuestro servidor.

Los pasos empiezan por el inicio de sesión al Switch.

Figura 3.46 Configuración del cliente Syslog en el Switch

Después ir a “Administration”, “System Log” y seleccionamos “Remoto Log Servers”, es aquí donde procedemos a agregar a nuestro servidor OSSIM.

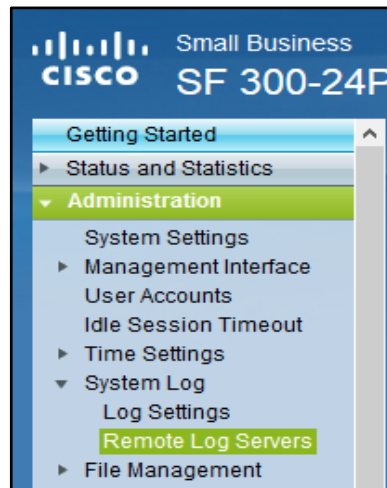


Figura 3.47 Accediendo al Rsyslog de Cisco

A continuación agregamos nuestro servidor en donde se especifica la dirección Ip del server, el puerto 514 que es por default, se selecciona el tipo de log, una descripción general, la severidad y finalmente presionamos en “Apply”.

The image shows a configuration form for adding a new Rsyslog server. The fields are: 'Log Server IP Address' with a dropdown menu showing '192.168.1.30'; 'UDP Port' with a text input field containing '514' and a note '(Range: 1 - 65535, Default: 514)'; 'Facility' with a dropdown menu showing 'Local 7'; 'Description' with a text input field containing 'Servidor OSSIM'; and 'Minimum Severity' with a dropdown menu showing 'Debug'. At the bottom, there are 'Apply' and 'Close' buttons.

Figura 3.48 Creando Nuevo Rsyslog en Cisco

### 3.1.7 Parámetros de configuración del cliente

Independientemente del cliente que se utilice, los parámetros generales de configuración en dispositivos de red y en los servidores son los siguientes:

- ✓ **Dirección IP del syslog server:** La dirección IP que se configura en esta sección es la de nuestro servidor OSSIM “192.168.1.30”
- ✓ **Puerto:** El puerto que se configura en esta parte es el 514 porque es en este puerto por donde recibe información nuestro servidor OSSIM
- ✓ **Facility:** Este campo se refiere al loggin facility tag que tiene el equipo, puede ser “daemon, Local7, kernel, etc”
- ✓ **Severity:** Este campo se refiere el tipo de severidad que se generó en el evento, se puede especificar tipos como “error, critical, warning, etc”
- ✓ **Authentication key:** Este parámetro adicional solo está presente en clientes como OSSEC que se instalan en servidores Windows o Linux, se utiliza una clave generada por el Plugin ossec de OSSIM.



Figura 3.49 Configurando Autenticación en Ossec

### 3.2 Funcionabilidad y desempeño

La funcionalidad se la puede verificar una vez que hemos finalizado con la configuración del servidor y la configuración de los respectivos clientes encargados de recolectar los registros, la verificación de la información que presenta OSSIM se la puede realizar mediante registros y por gráficos estadísticos, estas dos formas son válidas y muy útiles para obtener una mejor comprensión. Además, OSSIM otorga una gran ayuda en sus reportes presentando gráficos estadísticos resumidos con TOP 10 de las principales amenazas o anomalías encontradas en la red. Entre los principales reportes generados por OSSIM tenemos los siguientes:

### 3.2.1 Generación de informes de los eventos de la red

Cuando hablamos de eventos de la red nos referimos específicamente a los computadores que están activos y están siendo censados por OSSIM, el escaneo se lo realiza a la red o redes que tenga acceso el servidor OSSIM y para nuestro ejemplo haremos uso de la “red de voz y la red de datos”.

Este informe representa la red a la que tenemos acceso a través de nuestro servidor OSSIM para realizar el escaneo respectivo de los equipos que están activos.

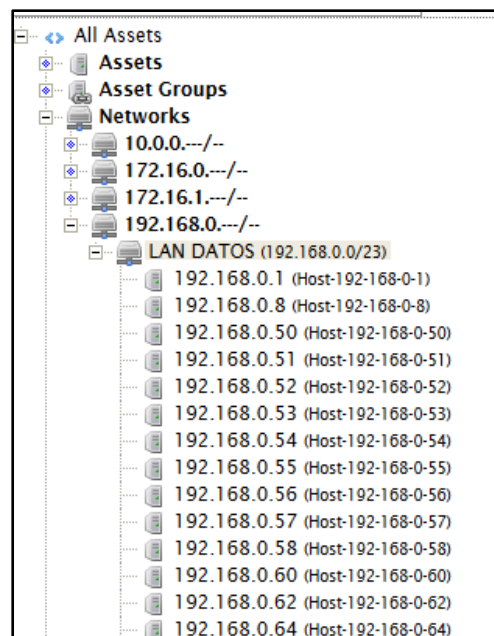


Figura 3.50 Informe de la red en OSSIM



El presente informe es el resultado del escaneo realizado y también permite visualizar todos los equipos que están activos en la red, a la vez en este reporte se puede observar una columna donde presenta la existencia de alarmas, de vulnerabilidades o eventos específicos en cada host de forma general.

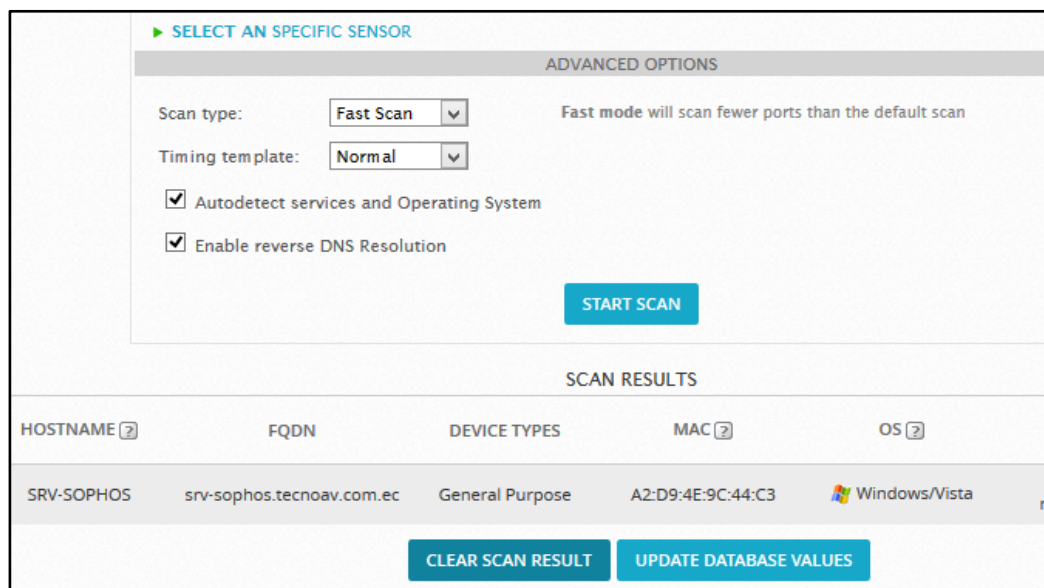
SHOW <input type="text" value="20"/> ENTRIES				
HOSTNAME	▲ IP	FQDN / ALIAS	ALARMS	VULNERABILITIES
SRV-SOPHOS	192.168.1.14		-	-
SRV-SOLOMON	192.168.1.10	sittecnoav.tecnoav.com.ec	-	-
srv-ossim	192.168.1.30		-	-
SRV-DOMAIN	192.168.1.12	srv-dctecnoav.tecnoav.com.ec	-	-
SRV-BIOMERICO-QUITO	192.168.1.100		-	-
SRV-BIOMERICO	192.168.1.8		-	-
Host-192-168-20-10	192.168.20.10		-	-

Figura 3.51 Escaneo realizado de la Red

### 3.2.2 Generación de informes de los eventos del S.O Windows

Al referirnos de eventos del sistema operativo Windows en esencial estamos enfatizando los problemas o anomalías que presentan los servicios que están configurados en los diferentes servidores, las fallas en la autenticación y alarmas desconocidas por aplicaciones que afectan directamente al sistema operativo.

En este informe podemos visualizar un escaneo realizado a un servidor específico y la información general que presenta a nivel de la seguridad se resume en puertos abiertos, servicios que se ejecutan, eventos generados, vulnerabilidades y alarmas detectadas, localización del servidor en el mapa siendo muy útil cuando se tiene diferentes sucursales remota por todo el mundo y las actividades realizadas.



The screenshot displays a web-based interface for configuring and viewing scan results. The top section, titled "SELECT AN SPECIFIC SENSOR", contains an "ADVANCED OPTIONS" panel with the following settings:

- Scan type: Fast Scan (dropdown menu)
- Timing template: Normal (dropdown menu)
- Autodetect services and Operating System:
- Enable reverse DNS Resolution:

A "START SCAN" button is located below these options. The "SCAN RESULTS" section below features a table with the following data:

HOSTNAME ?	FQDN	DEVICE TYPES	MAC ?	OS ?
SRV-SOPHOS	srv-sophos.tecnoav.com.ec	General Purpose	A2:D9:4E:9C:44:C3	Windows/Vista

At the bottom of the results section, there are two buttons: "CLEAR SCAN RESULT" and "UPDATE DATABASE VALUES".

Figura 3.52 Escaneo Realizado a un Servidor Windows

Assets > Asset Details

SRV-SOPHOS  
192.168.1.14

+ MORE DETAILS

Snapshot

5 Software Packages   0 Users   0 Vulnerabilities   No Alarms   No Events

GENERAL   ACTIVITY   LOCATION   NOTES

SOFTWARE | USERS | PROPERTIES | PLUGINS

EDIT AVAILABILITY MONITORING

Search:

IP ADDRESS	PORT	NAME	VULNERABLE	AVAILABLE
192.168.1.14	80	http	No	● No
192.168.1.14	135	msrpc	No	● No
192.168.1.14	139	netbios-ssn	No	● No

Figura 3.53 Escaneo General en Hosts Windows

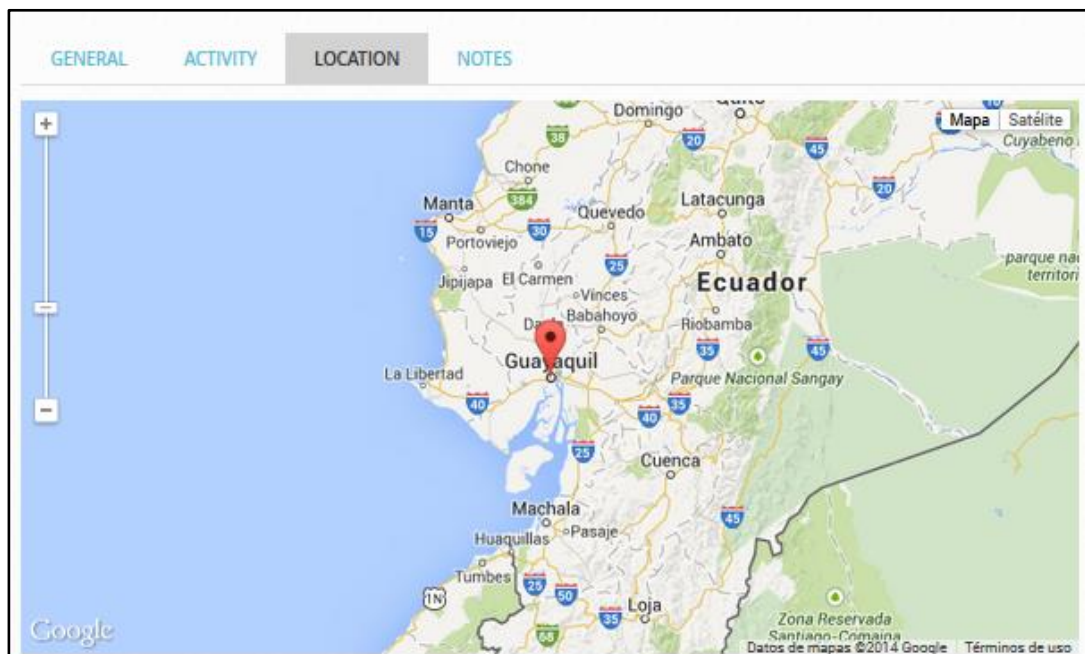


Figura 3.54 Sucursales remotas ubicadas en el mapa

### 3.2.3 Generación de informes de los eventos del S.O Linux

Los eventos que estamos analizando del servidor Linux son específicamente las autenticaciones y accesos a través de la interface web o por conexiones ssh, también estamos verificando el funcionamiento de determinados servicios. En este informe presentamos datos específicos solo de nuestro servidor OSSIM y el de nuestra central telefónica.

#### ✓ Informe del Servidor OSSIM.

alienvault  
192.168.1.30

- LESS DETAILS

Networks  
LAN DATOS (192.168.0.0/23)

Sensors  
192.168.1.30 (srv-ossim)

Description  
none

Operating System  
unknown:unknown

Asset Type  
Internal

Asset Value  
1 2 3 4 5

EDIT

Snapshot

4 Software Packages

0 Users

0 Vulnerabilities

No Alarms

No Events

GENERAL | ACTIVITY | LOCATION | NOTES

SOFTWARE | USERS | PROPERTIES | PLUGINS

EDIT AVAILABILITY MONITORING

Search:

IP ADDRESS	PORT	NAME	VULNERABLE	AVAILABLE
192.168.1.7	22	ssh	No	● No
192.168.1.30	22	ssh	No	● No
192.168.1.30	443	ssl	No	● No
192.168.1.30	3128	http	No	● No

Figura 3.55 Informe del Servidor Ossim

### ✓ Informe del Servidor Linux - Central PBX IP

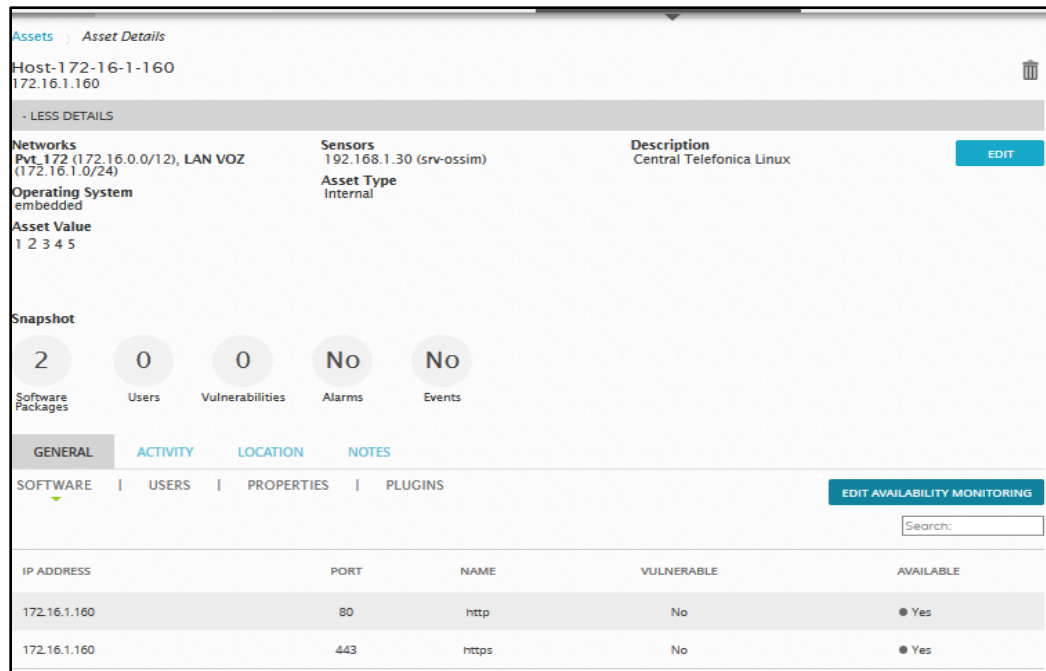


Figura 3.56 Informe del Servidor Linux PBX

### 3.2.4 Informes de vulnerabilidades y alarmas en general

Los informes de las vulnerabilidades se realizan a través de los host que están siendo monitoreados por OSSIM, en esta sección podemos presentar muchos gráficos estadísticos en forma de TOP de vulnerabilidades, ordenados por los servicios o TOP Services que se han generado en los servidores o hosts.

En el presente informe no tenemos vulnerabilidades, por tal razón se muestra completamente vacío, recalcamos que OSSIM está implementado en una empresa real con dispositivos y servidores en producción por tal razón no podemos generar simulaciones para presentar información.

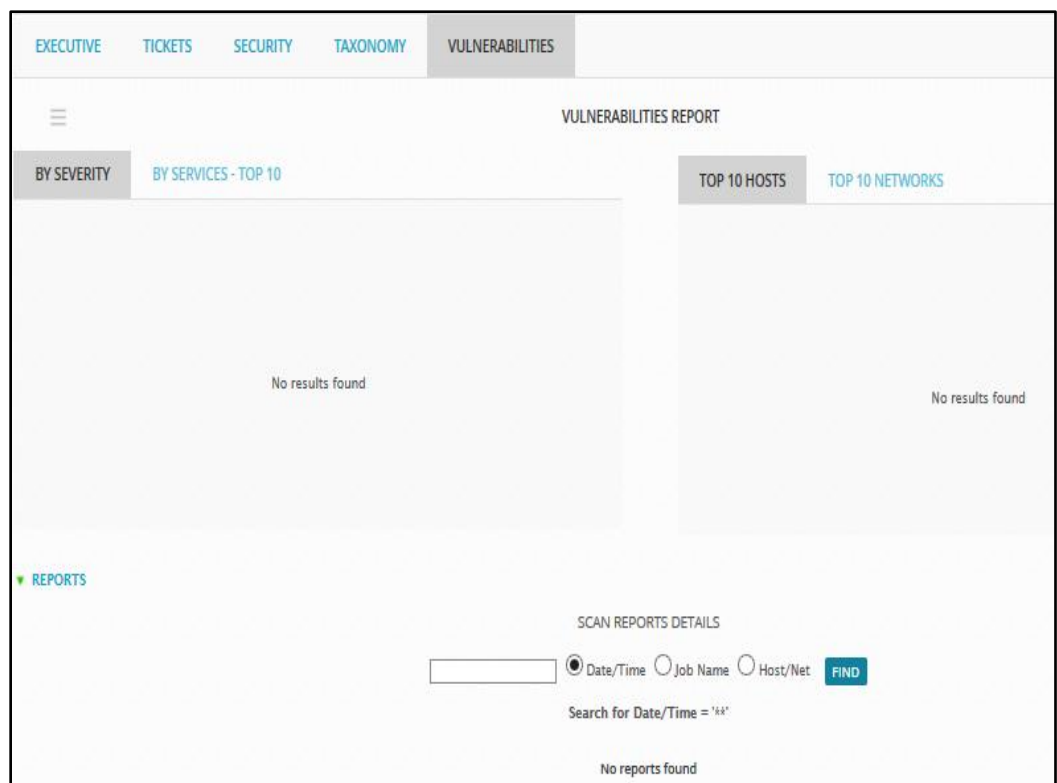


Figura 3.57 Análisis de Vulnerabilidad

El presente Gráfico nos da un análisis estadístico de los últimos eventos generados por los diferentes servicios en nuestro servidor Linux OSSIM.

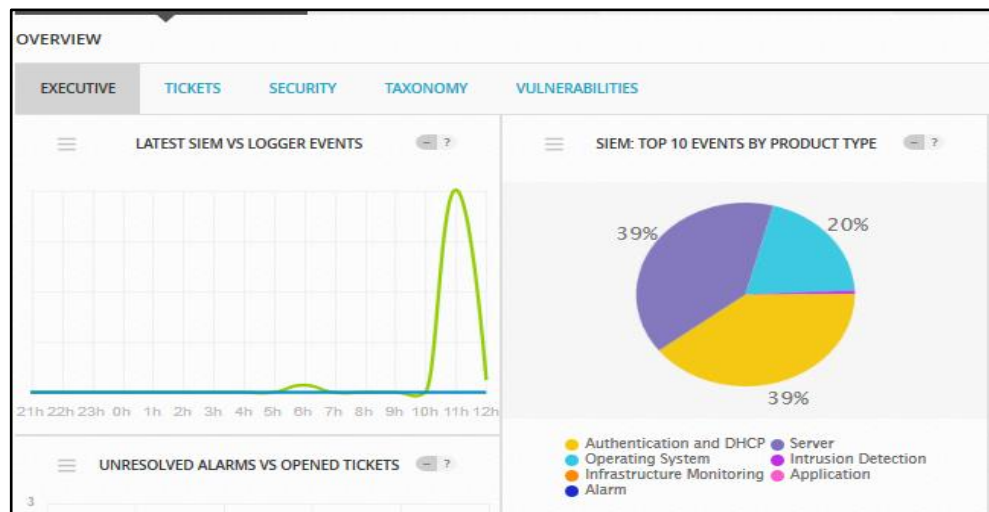


Figura 3.58 Análisis Estadístico de los últimos Eventos

Este informe presenta una estadística resumida de todos los sensores o plugins que tenemos configurados para recolectar la información.

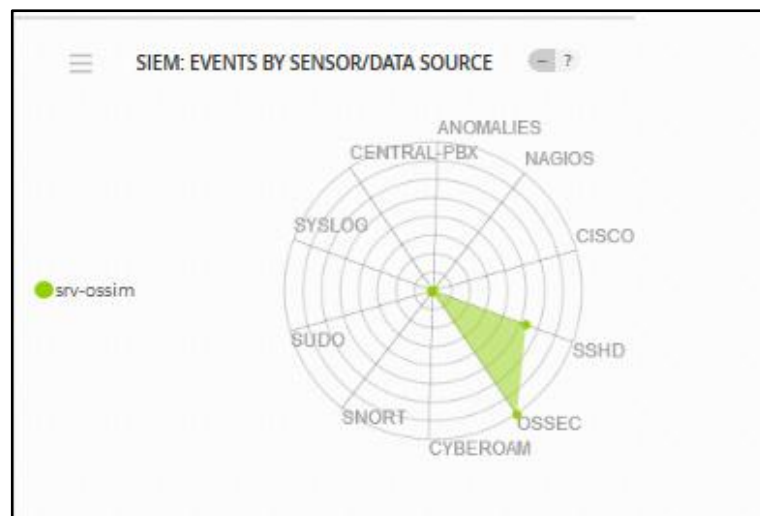


Figura 3.59 Análisis resumido de los Sensores

En este gráfico presentamos los diferentes servicios, políticas y las actividades que se ejecutan en tiempo real desde OSSIM hacia la red.

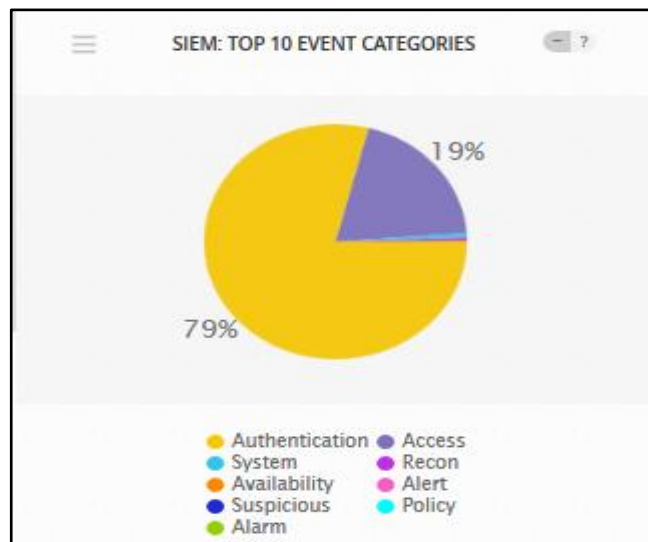


Figura 3.60 Políticas Ejecutadas en Tiempo Real

### 3.2.5 Generación de informes de la disponibilidad de la red

Cuando mencionamos disponibilidad se relaciona con el estado en tiempo real de los host y servidores de la red corporativa, OSSIM ofrece dos informes que nos presenta esta información, el informe general que presenta un reporte de los host que están en la red y un informe personalizado que se genera habilitando la opción de monitoreo con Nagios y es utilizado esencialmente para verificar el estado de los servidores.



Assets Clear All Filters

Last Updated: Last Day x

ADD ASSETS +

Results: 7

SAVE GROUP

SHOW 20 ENTRIES

HOSTNAME	IP	FQDN / ALIAS	ALARMS	VULNERABILITIES	EVENTS
FIREWALL-50ING	192.168.1.6		-	-	-
Host-172-16-1-160	172.16.1.160		-	-	-
SRV-BIOMERICO	192.168.1.8		-	-	-
SRV-BIOMERICO-QUITO	192.168.1.100		-	-	-

Figura 3.61 Reporte de Equipos Activos en la Red

Informe personalizado de los servidores principales de la empresa donde se monitorea la disponibilidad.

**Host Status Totals**

Up	Down	Unreachable	Pending
7	1	0	0

**Service Status Totals**

Ok	Warning	Unknown	Critical	Pending
22	0	0	1	0

**Service Overview For All Host Groups**

**SERVIDORES (SERVIDORES)**

Host	Status	Services	Actions
SRV-SOPHOS	UP	No matching services	

**All Servers (all)**

Host	Status	Services	Actions
FIREWALL-50ING	UP	No matching services	
Host-172-16-1-160	DOWN	1 OK 1 CRITICAL	
SRV-BIOMERICO	UP	No matching services	
SRV-BIOMERICO-QUITO	UP	4 OK	
SRV-DOMAIN	UP	6 OK	
SRV-SOLOMON	UP	5 OK	
SRV-SOPHOS	UP	No matching services	
localhost	UP	6 OK	

Figura 3.62 Monitoreo Personalizado de Disponibilidad




DISPOSITIVOS (DISPOSITIVOS)			
Host	Status	Services	Actions
FIREWALL-50iNG	UP	No matching services	  

Figura 3.63 Monitoreo del Firewall




Debian GNU/Linux Servers (debian-servers)			
Host	Status	Services	Actions
localhost	UP	6 OK	  

Figura 3.64 Monitoreo del Servidor Linux

### 3.2.6 Generación de informes de seguridad de la red.

OSSIM es una herramienta potente, referente a los informes de seguridad, nos presenta las principales áreas de seguridad en gráficos estadísticos de TOP 10 como los siguientes ejemplos.

Informe de los hosts que más alarmas y amenazas han tenido y atentan a la seguridad de la red interna.

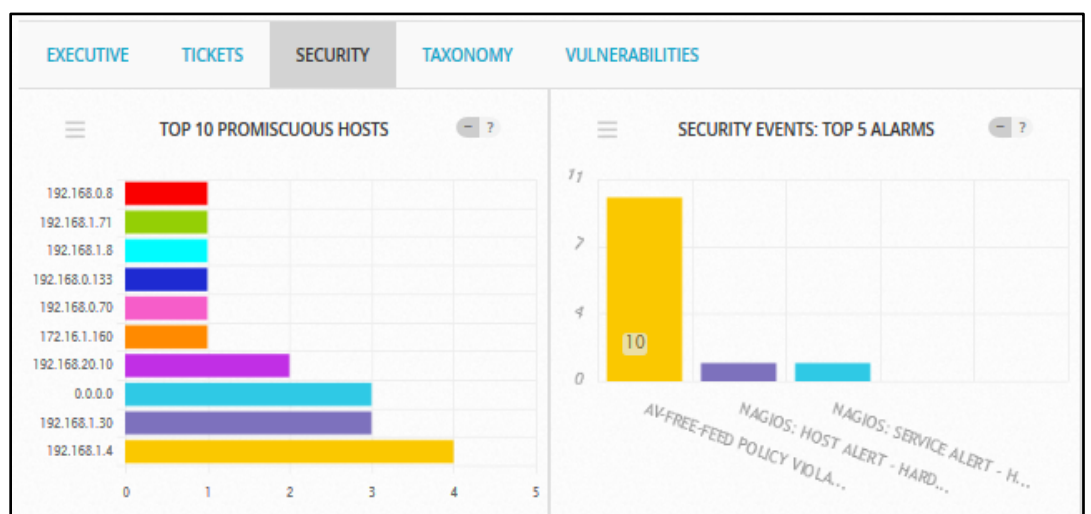


Figura 3.65 Informe de Amenazas de Seguridad

Informe de los host que han generado múltiples eventos.

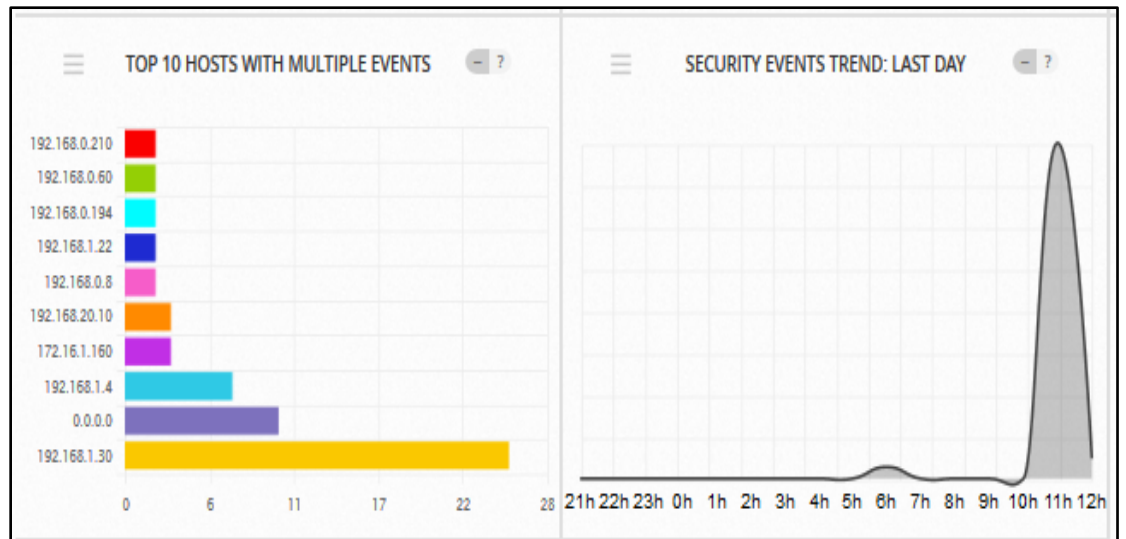


Figura 3.66 Informe de Múltiples Eventos

Informe estadístico de los puertos de Capa 4 con más tráfico.

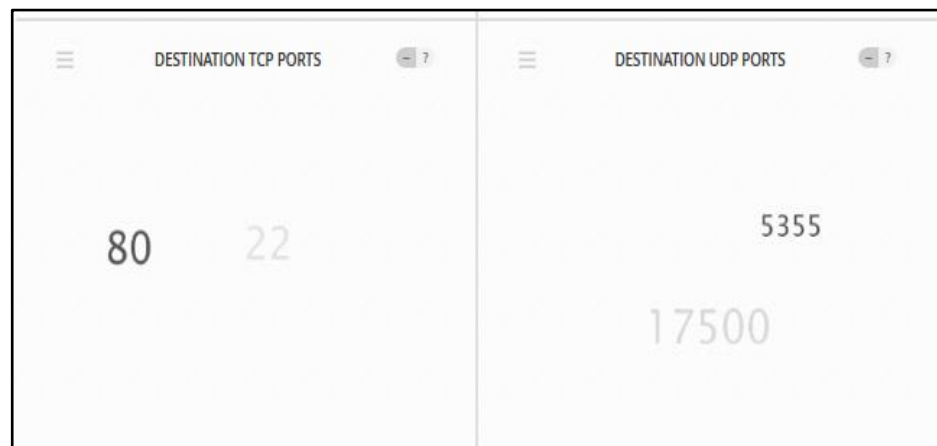


Figura 3.67 Trafico de Puertos de Capa 4

Reporte de los eventos que ha tenido un host específico, aquí se detalla el acceso al servidor 172.16.1.160 y se registra todo el comportamiento del host.

The screenshot shows a security dashboard with the following elements:

- SHOW EVENTS:** Radio buttons for 'Last Day', 'Last Week', 'Last Month', and 'Date Range' (selected). A date range is set from 14-11-08 to 14-11-15.
- FILTERS:** Dropdown menus for 'DATA SOURCES', 'RISK', 'TAXONOMY: PRODUCT TYPE', 'TAXONOMY: EVENT CATEGORY', 'IP REPUTATION ACTIVITY', and 'IP REPUTATION SEVERITY'. A 'SENSORS' field is also present.
- Buttons:** '+ MORE FILTERS' and 'ADVANCED SEARCH'.
- View Options:** 'EVENTS' (selected), 'GROUPED', and 'TIMELINE'.
- Graphs:** 'SHOW TREND GRAPH' is set to 'Off'.
- Table:** Displays 1-14 of about 14 matching events. The table has columns: SIGNATURE, DATE GMT-8:00, SENSOR, SOURCE, and DESTINATION.

SIGNATURE	DATE GMT-8:00	SENSOR	SOURCE	DESTINATION
SSH: Login successful, Accepted password	2014-11-13 15:30:29	srv-ossim	192.168.1.22:53580	172.16.1.160:22
SSH: Login successful, Accepted password	2014-11-13 14:54:45	srv-ossim	192.168.1.22:56580	172.16.1.160:22
SSH: Received disconnect	2014-11-13 13:07:21	srv-ossim	192.168.1.22	172.16.1.160:22

Figura 3.68 Reporte de un Host Específico

En este informe se detalla como un host intento acceder a varios servidores y se registra los intentos fallidos.

The screenshot shows a security dashboard with the following elements:

- SHOW EVENTS:** Radio buttons for 'Last Day', 'Last Week', 'Last Month', and 'Date Range' (selected). A date range is set from 14-11-08 to 14-11-15.
- FILTERS:** Dropdown menus for 'DATA SOURCES', 'RISK', 'TAXONOMY: PRODUCT TYPE', 'TAXONOMY: EVENT CATEGORY', 'IP REPUTATION ACTIVITY', and 'IP REPUTATION SEVERITY'. A 'SENSORS' field is also present.
- Buttons:** '+ MORE FILTERS' and 'ADVANCED SEARCH'.
- View Options:** 'EVENTS' (selected), 'GROUPED', and 'TIMELINE'.
- Graphs:** 'SHOW TREND GRAPH' is set to 'Off'.
- Table:** Displays 1-31 of about 31 matching events. The table has columns: SIGNATURE, DATE GMT-8:00, SENSOR, SOURCE, and DESTINATION.

SIGNATURE	DATE GMT-8:00	SENSOR	SOURCE	DESTINATION
SSHd: Login successful, Accepted password	2014-11-14 09:54:21	srv-ossim	192.168.1.4:10664	192.168.1.30:22
SSHd: Login successful, Accepted password	2014-11-14 08:04:18	srv-ossim	192.168.1.4:6425	192.168.1.30:22
SSHd: Login successful, Accepted password	2014-11-13 09:36:31	srv-ossim	192.168.1.4:8687	192.168.1.30:22

Figura 3.69 Intento Fallido de Autenticación

Este informe presenta información de quienes acceden a los switches cisco.

The screenshot shows a security dashboard with the following filters and data:

- SHOW EVENTS:** Radio buttons for Last Day, Last Week, Last Month, and Date Range.
- DATA SOURCES:** Cisco-switch
- TAXONOMY: PRODUCT TYPE:** (Empty)
- TAXONOMY: EVENT CATEGORY:** (Empty)
- IP REPUTATION ACTIVITY:** (Empty)
- IP REPUTATION SEVERITY:** (Empty)
- RISK:** (Empty)
- SENSORS:** (Empty)
- Buttons:** + MORE FILTERS, ADVANCED SEARCH
- View Modes:** EVENTS (selected), GROUPED, TIMELINE
- SHOW TREND GRAPH:** Off
- DISPLAYING EVENTS:** 1-4 OF ABOUT 4 MATCHING YOUR SELECTION.

<input type="checkbox"/>	SIGNATURE	▼ DATE GMT-8:00 ▲	SENSOR	SOURCE	DESTINATION
<input type="checkbox"/>	Cisco-AAA: Authentication, authorization, and accounting Emergency Event	2014-11-12 14:33:22	srv-ossim	172.16.1.5	0.0.0.0
<input type="checkbox"/>	Cisco-AAA: Authentication, authorization, and accounting Emergency Event	2014-11-12 14:28:22	srv-ossim	172.16.1.5	0.0.0.0
<input type="checkbox"/>	Cisco-AAA: Authentication, authorization, and accounting Emergency Event	2014-11-12 13:32:02	srv-ossim	172.16.1.5	0.0.0.0

Figura 3.70 Informe de Accesos al Switcho cisco

Este informe presenta eventos del Firewall

The screenshot shows a security dashboard with the following filters and data:

- SHOW EVENTS:** Radio buttons for Last Day, Last Week, Last Month, and Date Range.
- DATA SOURCES:** Cyberoam
- TAXONOMY: PRODUCT TYPE:** (Empty)
- TAXONOMY: EVENT CATEGORY:** (Empty)
- IP REPUTATION ACTIVITY:** (Empty)
- IP REPUTATION SEVERITY:** (Empty)
- RISK:** (Empty)
- SENSORS:** (Empty)
- Buttons:** + MORE FILTERS, ADVANCED SEARCH
- View Modes:** EVENTS (selected), GROUPED, TIMELINE
- SHOW TREND GRAPH:** Off
- DISPLAYING EVENTS:** 1-50 OF ABOUT A HUNDRED THOUSAND MATCHING YOUR SELECTION.

<input type="checkbox"/>	SIGNATURE	▼ DATE GMT-8:00 ▲	SENSOR	SOURCE	DESTINATION
<input type="checkbox"/>	Cyberoam: Unknown event	2014-11-14 11:48:45	srv-ossim	192.168.1.6	0.0.0.0
<input type="checkbox"/>	Cyberoam: Unknown event	2014-11-14 11:23:57	srv-ossim	192.168.1.6	0.0.0.0
<input type="checkbox"/>	Cyberoam: Unknown event	2014-11-14 11:11:57	srv-ossim	192.168.1.6	0.0.0.0

Figura 3.71 Eventos del Firewall

Informe detallado de los accesos a nuestra Central PBX.

The screenshot displays the OSSIM interface with the following components:

- SHOW EVENTS:** Radio buttons for 'Last Day', 'Last Week', 'Last Month', and 'Date Range'. A date range selector is present below.
- DATA SOURCES:** A dropdown menu set to 'Central-pbx'.
- RISK:** A dropdown menu.
- SENSORS:** A dropdown menu.
- TAXONOMY: PRODUCT TYPE:** A dropdown menu.
- TAXONOMY: EVENT CATEGORY:** A dropdown menu.
- IP REPUTATION ACTIVITY:** A dropdown menu.
- IP REPUTATION SEVERITY:** A dropdown menu.
- Buttons:** '+ MORE FILTERS' and 'ADVANCED SEARCH'.
- View Modes:** 'EVENTS' (selected), 'GROUPED', and 'TIMELINE'.
- SHOW TREND GRAPH:** A toggle switch set to 'Off'.
- DISPLAYING EVENTS:** 1-37 OF ABOUT 37 MATCHING YOUR SELECTION.
- Event Table:**

<input type="checkbox"/>	SIGNATURE	▼ DATE GMT-8:00 ▲	SENSOR	SOURCE	DESTINATION
<input type="checkbox"/>	SSH: Login successful, Accepted password	2014-11-13 15:30:29	srv-ossim	192.168.1.22:53580	172.16.1.160:22
<input type="checkbox"/>	SSH: Login successful, Accepted password	2014-11-13 14:54:45	srv-ossim	192.168.1.22:56580	172.16.1.160:22
<input type="checkbox"/>	SSH: Received disconnect	2014-11-13 13:07:21	srv-ossim	192.168.1.22	172.16.1.160:22

Figura 3.72 Acceso a la Central PBX

### 3.3 Análisis de resultados

Al no utilizar encuestas o valores cuantitativos no se puede analizar en función de estos datos, los parámetros que se podría analizar son la forma de configurar ossim, el funcionamiento con la activación de los diferentes plugins y los resultados proporcionados por los informes que genera ossim en producción.

El análisis e interpretación de resultados se presenta según la etapa de investigación e implementación realizada de la herramienta OSSIM y enfocándonos al cumplimiento de los objetivos planteados inicialmente.

La instalación de la herramienta OSSIM se realizó con éxito en un servidor que cumple con los requerimientos mínimos de hardware y podemos estipular que es muy sencilla la instalación respectiva.

Los plugins utilizados encontramos que funcionan a cabalidad para el uso específico en nuestra empresa, cabe recalcar que OSSIM tiene muchos plugins o servicios adicionales que no están implementados ni mencionados en este proyecto pero la eficiencia de cada uno es aceptable.

Los resultados esperados con los logs enviados desde los diferentes servidores y dispositivos de red se cumple a cabalidad, excepto que **es importante mencionar que tenemos un problema al leer los logs con el firewall Cyberoam, este firewall emite un formato de log propietario y OSSIM no puede adaptar el formato, por ende sale la información del evento como desconocida al momento de presentarlo en la interface Web, pero si el log se analiza a nivel de consola o directamente en el archivo ubicado en “/var/log/” es legible e interpretable con normalidad.**

El monitoreo de los host que están activos en la red es muy eficiente, con respecto al análisis de vulnerabilidades y alarmas se lo realiza en base al

escaneo de puertos y protocolos, dando como resultado información desde las aplicaciones y servicios que se ejecutan en los sistemas operativos de los hosts.



## CAPÍTULO 4

### 4 ANÁLISIS FINANCIERO, VIABILIDAD Y FACTIBILIDAD

#### 4.1 Viabilidad del proyecto.

Cuando analizamos los objetivos planteados inicialmente sobre la cobertura general del proyecto, tenemos un escenario un poco difícil para implementarlo con éxito y por tal razón el análisis de los factores para la viabilidad se centraron en la parte técnica profesional y en la parte financiera de la empresa que pueda cubrir los gastos necesarios para la implementación.

- ✓ **Viabilidad técnica:** Este factor comprende específicamente el conocimiento profesional de como instalar y configurar la herramienta OSSIM, se enfoca en la capacidad de análisis que debe

- ✓ tener un profesional en el área de seguridades en redes informáticas para poder realizar la configuración de los clientes recolectores de logs estratégicamente en diferente puntos de la red y en los servidores de la empresa, la importancia de tener profesionales con mayor experiencia es para garantizar que el proyecto tenga el impacto requerido.
  
- ✓ **Viabilidad Financiera:** La herramienta presentada en este proyecto requiere de una inversión en la parte profesional y en la parte de hardware en donde se tiene que instalar físicamente el servidor OSSIM, el punto financiero también se considera de vital importancia para medir el grado de viabilidad del proyecto, porque si la empresa que será la futura beneficiaria no cuenta con el recurso financiero no se podrá implementar y poner en marcha el proyecto.

Ahora analizando la propuesta inicial de implementar el proyecto en una empresa privada, para nuestro caso podemos afirmar que si se pudo concretar y podemos enfatizar que el proyecto es viable porque contamos con los recursos profesionales y, los recursos financieros necesarios fueron otorgados por la empresa favorecida para ponerlo en marcha, además al estar latente esta necesidad en las empresas medianas, podemos decir que si es factible la viabilidad del proyecto,

dada la importancia que se genera al nivel de la seguridad informática en el ámbito corporativo y por la característica de OSSIM que puede cubrir algunos puntos de mayor importancia en el monitoreo general en el cual nos hemos enfocados a lo largo del proyecto.

#### **4.2 Estudio de Factibilidad.**

La factibilidad de Ossim se destaca por tener una amplia gama de recursos que podemos utilizar y cubrir un mayor control, acorde a lo analizado anteriormente en las instalaciones y funcionabilidad de la herramienta, podemos recalcar que es factible la instalación y la puesta en marcha de Ossim en cualquier empresa privada o pública dado que no representa una carga mayor al administrador de red y al ser una herramienta libre tampoco tiene una mayor carga económica para la empresa.

Teniendo a ossec embebido en Ossim, este nos brinda una mayor eficacia a la hora de realizar el monitoreo en tiempo real y al momento de conocer los hosts que están operativos en la red, analizando vulnerabilidades y riesgos, mostrando un resumen completo de la red. Además también está el Arpwatch que se encuentra realizando un

monitoreo continuo para saber si hay una Mac duplicada en la red por un posible ataque que estemos siendo víctima.

Este proyecto tendrá mucho éxito si lo empezamos a expandir dado que es una herramienta no muy conocida aun en nuestro medio local y hay pocos usuarios que la utilizan, pero al mismo tiempo es una herramienta muy famosa por todas su funcionalidades y características que trae incorporado, no requiere de un estudio amplio para el administrador de red y las ventajas que ofrece a la organización son muy provechosas.

### **4.3 Recursos Humanos**

Cuando hablamos de las personas involucradas en la implementación de OSSIM, esta es una gran ventaja, porque no se necesita la contratación de varios especialistas en la herramienta, otorgando una preocupación menos a la empresa a la hora de contratar personal nuevo para hacerse cargo del funcionamiento. Los recursos humanos principales que se necesitaría para la implementación eficiente son:

- ✓ Consultor externo en seguridad informática para levantamiento de información
- ✓ Profesional en la implementación de la herramienta OSSIM.

- ✓ Administrador de Red de la empresa
- ✓ Administrador de servidores Windows de la empresa
- ✓ Administrador de servidores Linux de la empresa.

#### **4.4 Recursos Materiales**

Entre los recursos materiales principales utilizados durante la implementación de OSSIM además de los mencionados anteriormente como el servidor y una red operativa, es indispensable tener en cuenta materiales que en si no son parte de la herramienta pero son muy importantes antes y durante el proceso de instalación, dado que sin estos materiales no se llevaría a cabo una implementación exitosa.

Los materiales a considerar son los siguientes:

- ✓ Laptops
- ✓ Cables de red
- ✓ Plumas
- ✓ Libretas de notas
- ✓ Impresiones
- ✓ Memory flash

Antes de la implementación de OSSIM, es muy importante realizar un levantamiento de información y estudio de factibilidad en la empresa

involucrada y poder tener el mayor porcentaje de efectividad al momento de la ejecución del proyecto.

## 4.5 Recursos Financieros

### 4.5.1 Costo de implementación

Acorde a lo mencionado anteriormente con respecto al licenciamiento de OSSIM, reiteramos que no tiene costo en licenciamiento pero si es necesario un servidor físico para su instalación cumpliendo los requerimientos mínimos en el hardware acorde a lo detallado en el capítulo anterior.

También es indispensable un profesional que configure y supervise el adecuado funcionamiento de la herramienta OSSIM, basándonos en estos términos presentamos a continuación un detalle general de costos en la siguiente tabla.

<b>COSTO DE IMPLEMENTACIÓN</b>	
Licenciamiento	Herramienta libre
Administrador de la red interna	Personal de empresa
Servidor mínimo requerido para la instalación.	\$800
Consultor externo en seguridad informática para levantamiento de información	\$800
Ingeniero encargado de instalar Ossim	\$800
Movilización	\$80
Alimentación	\$150

Tabla 4 Costo de Implementación del Proyecto

#### 4.5.2 Costo de mantenimiento

Analizando que Ossim es una herramienta no muy compleja y teniendo presente que existe material en la web que facilita su mantenimiento, entonces podemos decir que el costo de manteniendo es cero, porque el mantenimiento lo dará el mismo administrador de red de la empresa, si es una configuración que amerita un profesional experto en OSSIM se puede hacer un contrato mensual o anual y brindar el soporte requerido de la siguiente forma:

COSTO DE MANTENIMIENTO	HORA / TECNICA
Configuración y Mantenimiento general	\$50
Solución de errores y reparación	\$50
Consultorías de seguridad	\$50
Consultorías de mejoras (Updates)	\$0

Tabla 5 Costo de Mantenimiento de OSSIM

#### 4.6 Recursos Legales.

Tomando en cuenta que la aplicación que presentamos en el proyecto es de libre comercialización y se distribuye bajo licencia LGPL (libertad de usar, compartir y estudiar el software), entonces no es necesario de comprar algún tipo de licencia o de realizar pagos mensuales y anuales, la herramienta OSSIM se la puede obtener directamente desde la página oficial sin ningún problema o recargo alguno, lo que sí debemos tener en cuenta que está prohibido bajo la licencia LGPL la modificación del código y no publicarlo en la página principal de OSSIM,

además que cada mejora que se realice se publica con una nueva versión del producto.

También está prohibida totalmente la venta en general de la herramienta OSSIM, pero si se puede comercializar o vender los servicios profesionales de las configuraciones y la implementación a terceros.

Como conocimiento adicional de los recursos legales es importante aclarar que el nombre de Ossim fue lanzada como una rama de AlienVault pero de forma gratuita, tomando en cuenta que AlienVault es una forma mejorada, ofreciendo aplicaciones y mayores recursos en la seguridad de la red que Ossim y esta distribución si es pagada.

Es importante resaltar que en la página Oficial de Ossim usted puede registrarse para pertenecer a la comunidad de Alienvault-Ossim y así tener una participación activa a las nuevas mejoras, un punto importante es que Alienvault hace muchas mejoras a Ossim retroalimentándose así mismo con las mejoras que se hacen a Ossim y luego estas mejoras son añadidas a la herramienta Alienvault que si es licenciada y la venden a un precio muy alto.



## CONCLUSIONES Y RECOMENDACIONES

Concluimos que en nuestro análisis destacamos que OSSIM no solo es una herramienta que recolecta logs de diferentes dispositivos, también es un SIEM (Security Information and Event Management) y trae incorporado diversas formas para gestión de seguridad como un antivirus que se encarga de detectar y eliminar software malicioso de un sistema informático, cuenta con detectores de intrusos basados en host (HIDS, Host-based Intrusion Detection Systems) encargado de monitorear procesos y archivos críticos del sistema bajo análisis, cuenta con Detectores de intrusos basados en red (NIDS, Network-based Intrusion Detection Systems) responsables de la revisión de los datos que circulan por la red, y avisan cuando observan tráfico que evidencia un ataque, detectores de vulnerabilidades que hacen un análisis detallado y arrojan como resultado las vulnerabilidades que existen en el sistema operativo y el software instalado.

Concluimos que OSSIM otorga un aporte invaluable al administrador de red, brindándole información útil para la toma de decisiones en el campo de la seguridad y que enfocados en la visión principal hemos logrado integrar varios dispositivos de red de diferentes marcas y diferentes servidores Windows y Linux en la misma consola, logrando obtener un resultado confiable en la solución implementada. OSSIM al tener la filosofía de código

abierto y libre distribución, permite la implementación de una consola centralizada a un costo relativamente bajo.

Concluimos que este trabajo representa un aporte profesional y el potencial de los estudiantes politécnicos para el desarrollo de servicios de consultoría en seguridades informáticas empleando herramientas de código abierto, y se convierte en un excelente ejemplo de colaboración entre la universidad y empresa privada en nuestro entorno.

Recomendamos a Ossim como una herramienta muy poderosa al momento de visualizar la disponibilidad de los servidores y dispositivos de red, porque es de gran ayuda y eficaz en el momento oportuno de riesgos y amenazas generados en la red interna por los diferentes hosts, al mismo tiempo presenta una gran cantidad de información que puede ser analizada detalladamente.

Se recomienda al administrador profundizar sus conocimientos en el campo de seguridades informáticas y administración de Linux para aprovechar al máximo el funcionamiento de OSSIM.

Se recomienda que Ossim sea implementado a partir de empresas medianas para optimizar su gestión y el control de una gran cantidad de hosts, previo a esto se recomienda tener una administración organizada de equipos de Red

y Servidores tanto en Netbios y su direccionamiento lógico IP para poder tener establecidas los parámetros de cada usuario antes de Instalar la herramienta

## Bibliografía

- [1] «Alien Vault,» [En línea]. Available: <https://www.alienvault.com/open-threat-exchange/projects>. [Último acceso: 26 septiembre 2014].
- [2] A. Ossim, «AlienVault OSSIM,» 15 Septiembre 2014. [En línea]. Available: <https://www.alienvault.com/open-threat-exchange/projects>. [Último acceso: 15 Septiembre 2014].
- [3] W. BLOG, «Wolfant's BLOG,» 15 Octubre 2014. [En línea]. Available: <http://wolfant.insuasti.ec/?p=29>. [Último acceso: 15 Octubre 2014].
- [4] A. Vault, «Wikipedia,» 2014. [En línea]. Available: [http://es.wikipedia.org/wiki/Open\\_Source\\_Security\\_Information\\_Management](http://es.wikipedia.org/wiki/Open_Source_Security_Information_Management). [Último acceso: 10 12 2014].
- [5] L. Martinez, «SecurityByDefault.com,» 03 Mayo 2013. [En línea]. Available: <http://www.securitybydefault.com/2013/05/mi-analisis-de-alienvaultossim-421.html>. [Último acceso: Septiembre 2014].
- [6] A. A. Parriza, «angelalonzo.ec,» [En línea]. Available: <http://www.angelalonzo.es/doc-presentaciones/ossim-hakin9.pdf>.
- [7] N. C. L. M. JOSE ALVAREZ OROZCO, «Blogdiario,» 12 08 2012. [En línea]. Available: <http://networkadmin.blogspot.es/>. [Último acceso: 18 08 2013].
- [8] K. Makino, «kinomakino.blogspot,» 18 03 2014. [En línea]. Available: <http://kinomakino.blogspot.com/2014/03/ossim-pentesting-continuo-como-si.html>. [Último acceso: 17 12 2014].
- [9] V3ktor, «itfreakzone.blogspot,» 15 06 2010. [En línea]. Available: <http://itfreakzone.blogspot.com/2010/06/monitoreo-de-red-ossim-review-parte-i.html>. [Último acceso: 07 11 2013].
- [10] S. c. S.A, «sifra.net.mx,» 2009. [En línea]. Available: <http://www.sifra.net.mx/metodolog%C3%ADa/ppdioo.aspx>. [Último acceso: 05 12 2014].
- [11] Admin, «todoit.com.ve,» 16 05 2011. [En línea]. Available: <http://todoit.com.ve/blog/2011/sobre-metodologia-de-gestion-de-redes/>.
- [12] M. M. Tenorio, «hermeschavez.,» 14 08 2009. [En línea]. Available: <http://hermeschavez.files.wordpress.com/2010/11/manual-super-de-ossim.pdf>.
- [13] Bumiga, «xmind,» 18 08 2010. [En línea]. Available: <http://www.xmind.net/m/CseF/>.
- [14] Hector, «inforleon,» 14 09 2010. [En línea]. Available: <http://inforleon.blogspot.com/2010/09/ossim.html>. [Último acceso: 02 11 2014].
- [15] C. E. B., «coberturadigital,» 16 05 2014. [En línea]. Available:

<http://www.coberturadigital.com/2014/05/16/internet-en-ecuador-el-acceso-paso-del-3-al-404-en-10-anos/#comments>.

- [16] «Bajolared,» 16 05 2014. [En línea]. Available:  
<http://www.bajolared.com/wordpress/ossim-como-plataforma-de-monitorizacion-y-gestion-de-informacion-de-seguridad/>. [Último acceso: 28 10 2014].
- [17] D. R. M. S. H. A. A. H. S. VanDyke, Security Information And Event Management (Siem) Implementation, 2010 ed., New York: McGraw-Hill Education, 2010.
- [18] SUPERTEL, «Aeprovi,» 08 10 2008. [En línea]. Available:  
[http://www.aeprovi.org.ec/index.php?option=com\\_content&task=view&id=299&Itemid=34](http://www.aeprovi.org.ec/index.php?option=com_content&task=view&id=299&Itemid=34).