UNIVERSIDAD POLITÉCNICA SALESIANA
SEDE QUITO

CARRERA
INGENIERÍA DE SISTEMAS

Trabajo de titulación previo a la obtención del título de:
INGENIEROS DE SISTEMAS

TEMA:

ANÁLISIS, DISEÑO, DESARROLLO E IMPLEMENTACIÓN DE POLÍTICAS Y PROCEDIMIENTOS PARA LA GESTIÓN DE LOS SERVIDORES. CASO DE ESTUDIO: CENTRO DE INVESTIGACIÓN IDE-IA-GEOCA.

AUTORES:

DARWIN RAMIRO JIMÉNEZ ERAZO
MARCELO PAÚL OSORIO DUQUE

TUTOR:

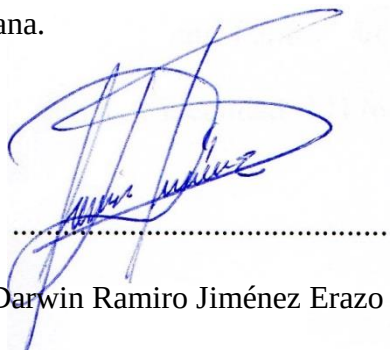
RODRIGO EFRAÍN TUFIÑO CÁRDENAS

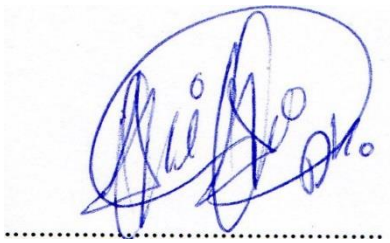
Quito, agosto del 2016

CESIÓN DE DERECHOS DE AUTOR

Nosotros Darwin Ramiro Jiménez Erazo, con documento de identificación N° 1720470499 y Marcelo Paúl Osorio Duque, con documento de identificación N° 1715274492, manifiesto nuestra voluntad y cedemos a la Universidad Politécnica Salesiana la titularidad sobre los derechos patrimoniales en virtud de que somos autores del trabajo de titulación intitulado: ANÁLISIS, DISEÑO, DESARROLLO E IMPLEMENTACIÓN DE POLÍTICAS Y PROCEDIMIENTOS PARA LA GESTIÓN DE LOS SERVIDORES. CASO DE ESTUDIO: CENTRO DE INVESTIGACIÓN IDE-IA-GEOCA, mismo que ha sido desarrollado para optar por el título de: Ingenieros de Sistemas, en la Universidad Politécnica Salesiana, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente.

En aplicación a lo determinado en la Ley de Propiedad Intelectual, en nuestra condición de autores nos reservamos los derechos morales de la obra antes citada. En concordancia, suscribo este documento en el momento que hago entrega del trabajo final en formato impreso y digital a la Biblioteca de la Universidad Politécnica Salesiana.





.....	.....
Darwin Ramiro Jiménez Erazo	Marcelo Paúl Osorio Duque
1720470499	1715274492

Quito, agosto de 2016

DECLARATORIA DE COAUTORÍA DEL DOCENTE TUTOR

Yo, declaro que bajo mi dirección y asesoría fue desarrollado el trabajo de titulación ANÁLISIS, DISEÑO, DESARROLLO E IMPLEMENTACIÓN DE POLÍTICAS Y PROCEDIMIENTOS PARA LA GESTIÓN DE LOS SERVIDORES. CASO DE ESTUDIO: CENTRO DE INVESTIGACIÓN IDE-IA-GEOCA, realizado por Darwin Ramiro Jiménez Erazo y Marcelo Paúl Osorio Duque, obteniendo un producto que cumple con todos los requisitos estipulados por la Universidad Politécnica Salesiana para ser considerados como trabajo final de titulación.

Quito, agosto de 2016

Rodrigo Efraín Tufiño Cárdenas

Cédula de identidad: 171764639-0

ÍNDICE

ÍNDICE DE FIGURAS

ÍNDICE DE TABLA

ÍNDICE DE ANEXOS

RESUMEN

El presente proyecto, es un caso de estudio, donde realizamos un análisis de seguridad informática mediante herramientas opensource, aplicando metodología OSSTMM y ethical hacking, permitiendo identificar las vulnerabilidades presentes en la infraestructura y mostrando las mitigaciones correspondientes para cada una de ellas, definiendo un esquema base para la implantación de políticas de seguridad informática para el centro de investigación IDE-IA–GEOCA.

ABSTRACT

This project is a case study, where we do an analysis of security by opensource tools, applying OSSTMM and ethical hacking methodology, allowing to identify vulnerabilities in the infrastructure and showing corresponding to each mitigations, defining a scheme basis for the implementation of security policies for the IDE-IA-GEOCA research center.

INTRODUCCIÓN

Antecedente

Análisis, diseño, desarrollo e implementación de políticas y procedimientos para la gestión de los servidores. Caso de Estudio: Centro de Investigación IDE-IA-GEOCA.

La Seguridad informática, cada día se ve amenazada en el entorno físico y lógico, existen varios factores que deben ser cubiertos, se centra en mantener la integridad de los datos e infraestructura, manteniendo la confidencialidad corporativa; los métodos tradicionales de seguridad se quedan varios pasos detrás de los nuevos tipos de ataque y riesgos inmersos en las redes informáticas, mucho más si esta incluyen sistemas interconectados al mundo por internet, existen amenazas directas que ponen en riesgo toda la organización, si existe un hueco de seguridad tan solo en uno de sus equipos, puede llegar a filtrarse información sensible y poner en riesgo su información financiera organizativa, que puede llegar a generar pérdidas económicas considerables.

Las organizaciones se esfuerzan por mantener sus sistemas seguros, implementando firewalls, Anti-DoS, Ips entre otros elementos de mitigación generan una capa de protección que ayuda a mantener el perímetro de red seguro, al interno elementos de seguridad como antivirus, host dlp, proxys y otros para control de cada PC y servidores integrados a la red, como menciona Kevin Mitnick “Las organizaciones gastan millones de dólares en firewalls y dispositivos de seguridad, pero tiran el dinero porque ninguna de estas medidas cubre el eslabón más débil de la cadena de seguridad: la gente que usa y administra los ordenadores.” (Wilding, 2006), es justamente lo que las organizaciones deben tener claro, que existen varios niveles de amenazas, Mitnik en el Campus Party de Octubre del 2011 en Ecuador, le realizaron una pregunta: Que sistema es el más seguro? y el respondió “El sistema más seguro es el que esta

desconectado de la toma eléctrica y sin información almacenada en su hardware" (Mitnik, 2011)

El ciber-espionaje también es un mercado en auge, ya que el valor de la información digital es incalculable.

"Los ataques de ciber-espionaje serán cada vez más frecuentes. Los delincuentes establecidos se convertirán en avezados cazadores furtivos de la información y los que empiecen a delinquir buscarán formas de robar dinero y fastidiar a sus adversarios (IntelSecurity, 2014).

Justificación del proyecto

El elemento más importante de una organización es la información que contiene y la operatividad y downtime de las plataformas implementadas, esto genera la necesidad de mantener la integridad y disponibilidad de la mismas, esta debe mantener un balance entre accesibilidad y seguridad, por esta razón se observa la necesidad de plantear un modelo de seguridad para el IDE-IA-GEOCA, el cual ha generado varios proyectos interesantes para la universidad en el georreferenciación y temas académicos, al realizar estas actividades, se ha generado una brecha de seguridad, al entregar el acceso al equipamiento a los tesistas que han desarrollado sus proyectos sobre los servidores disponibles de producción del grupo, todos los proyectos que han sido añadidos a esta plataforma no tienen lineamientos ni estándares de seguridad que garanticen la integridad de la información y de acceso a los recursos de red.

Se propone un análisis de vulnerabilidades para los elementos que componen la infraestructura, en esta revisión se planea recopilar información actual de seguridad y

generar el respectivo análisis de la misma para determinar fallos y poder sugerir los correctivos e implementar una capa perimetral de protección, que logre mitigar las posibles amenazas a las que está expuesta la plataforma.

En la infraestructura informática del Grupo de Investigación IDE-IA-GEOCA existen riegos asociados a los proyectos implementados y para la propia plataforma de virtualización ya que no existe un documento de buenas prácticas para cargar nuevos proyectos, ni se dispone de una política de seguridad para que cada proyecto nuevo pueda ser implementado, cerrando vulnerabilidades, tanto desde su implementación y de la administración de proyectos existentes, cabe mencionar que la infraestructura informática, están publicados sin restricciones hacia el internet y esto es un grave riesgo para la seguridad de la plataforma y la infraestructura.

Por esta razón se plantea un análisis integral para la aplicación de políticas de seguridad y la generación de procedimientos elementales, para la administración y carga de proyectos en la infraestructura informática del Grupo de Investigación IDE-IA-GEOCA, como una base referencial para su ejecución.

Objetivos del proyecto

Objetivo general.

- Auditar e implementar seguridades informáticas y buenas prácticas en la administración, implementación y manteniendo de la infraestructura informática del grupo de investigación IDE-IA-GEOCA.

Objetivos específicos.

- Recolectar y analizar información mediante las herramientas de monitoreo el estado actual de la infraestructura informática del grupo de investigación.
- Implementar el esquema de seguridad perimetral para los servicios instalado en la infraestructura.
- Generar políticas y procedimientos elementales para la administración, implementación y mantenimiento de la infraestructura informática del Grupo IDE-GEOCA

CAPÍTULO 1

ESTADO DEL ARTE

1.1 Marco referencial

1.1.1 OSSTMM

"Open Source Securiy Testing Methodology Manual", es la metodología abierta y colaborativa realizada por ISECOM "Institute for Security and Open Methodologies", convertida en pilar fundamental para el análisis y test de seguridad de las Tecnologías de la información, esta metodología tiene 3 principios fundamentales que son: Confidencialidad, integridad y disponibilidad.

OSSTMM es una metodología científica con enfoque a la seguridad informática, su objetivo es adaptarse a cualquier tipo de auditoria informática, para esto plantea categorizaciones estándar, definiendo el alcance de cada una de ellas.

La metodología sigue un proceso para determinar el nivel de seguridad según se explica en la siguiente gráfica

Proceso de la Metodología OSSTMM

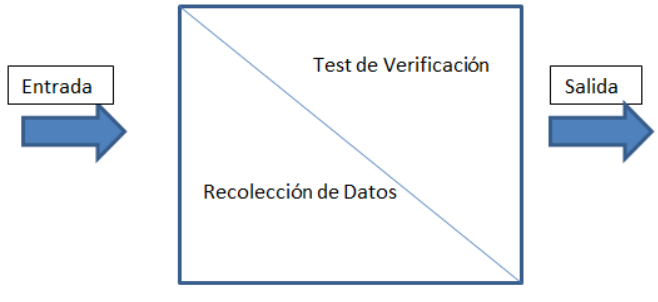


Figura 1. Flujo OSSTMM
Fuente: Metodología OSSTMM, Herzog 2003

“La metodología fluye desde el proceso inicial “Entrada” hasta completar el modulo final “Salida”. La metodología permite la separación entre recolección de datos y test de verificación de y sobre los datos recolectados. El flujo también determina los puntos precisos de cuando extraer e insertar estos datos.” (Herzog, 2003)

La recolección de información da la pauta para el análisis y determinar que secciones serán utilizadas de la metodología, ya que, al ser abierta y flexible, se adapta a las necesidades del análisis. Los ítems disponibles son los siguientes:

1.1.2 Seguridad de la información.

Se refiere a la información privada y pública que puede ser divulgada por cualquier medio, en ella se valida:

- Revisión de la Inteligencia Competitiva
- Revisión de Privacidad
- Recolección de Documentos

1.1.3 Seguridad de los procesos.

Los procesos implantados en una organización son el medio por el cual se pude llegar a determinar problemas de se seguridad, aquí se considera:

- Testeo de Solicitud
- Testeo de Sugerencia Dirigida
- Testeo de las Personas Confiables

1.1.4 Seguridad en las tecnologías de internet y comunicaciones.

Se analiza toda la información disponible a través del internet como buscadores, blogs, wikis, ftp y escaneo de protocolos disponibles a través de internet.

- Logística y Controles
- Sondeo de Red
- Identificación de los Servicios de Sistemas
- Búsqueda de Información Competitiva
- Revisión de Privacidad
- Obtención de Documentos
- Búsqueda y Verificación de Vulnerabilidades
- Testeo de Aplicaciones de Internet
- Enrutamiento
- Testeo de Sistemas Confiados
- Testeo de Control de Acceso
- Testeo de Sistema de Detección de Intrusos
- Testeo de Medidas de Contingencia
- Descifrado de Contraseña
- Testeo de Denegación de Servicios
- Evaluación de Políticas de Seguridad

Los enfoques aplicables se entrelazan para dar un resultado y evaluar cuantitativamente el estado de seguridad de un sistema, en el siguiente gráfico se puede ver la relación de los mismos.

Parámetros de convergencia

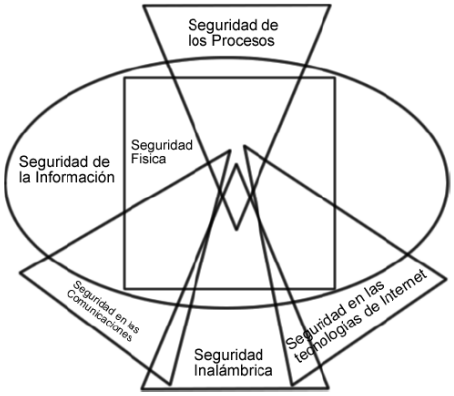


Figura 2. Vista global de parámetros

Fuente: Manual de la metodología abierta de testeo de Seguridad, pág23

1.2 Políticas de seguridad

"Una política de seguridad puede ser simplemente un uso aceptable de los recursos de red o puede ser cientos de páginas que indique cada uno de los elementos asociados de la red y sus políticas individuales. De acuerdo al documento Site Securty Handbook (RFC2196, 1997), "Una Política de seguridad es un documento formal de reglas para las personas que requieren acceso a la red en una organización tanto a los recursos tecnológicos como la información" Una política de seguridad actualmente es el centro de la seguridad." (Cisco, 2005)

1.2.1 Importancia de la política de seguridad

La política de seguridad provee varios beneficios y requiere tiempo y esfuerzo para implementarlo. Las políticas de seguridad son importantes en las organizaciones por varias razones, incluyendo los siguientes:

- Crea una línea base de la seguridad actual
- Plantea una base para la implementación de seguridades
- Define comportamientos permitidos o no
- Ayuda a determinar herramientas y procedimientos
- Genera consensos y define roles
- Define el manejo de incidentes

Según se define en el libro Network Security Fundamentals (Cisco, 2005, pág. 81)

1.3 Marco teórico

1.3.1 Hacking ético

Para Definir un Hacker ético, se debe empezar definiendo el termino hacker, un hacker en si es un experto en materia de seguridad y operación de los sistemas, el cual es capaz de determinar el funcionamiento completo de una plataforma y explorar puntos débiles que tenga posibles vulnerabilidades, que puedan ser explotadas, definiendo esto podemos definir el termino hacking, que es la acción que realiza el hacker al efectuar su actividad analizando puntos débiles de la infraestructura y como complemento definiendo la ética de una actividad es el manejo profesional de la actividad que se realiza apegándose a las normas y leyes aplicables, para realizar el hacking ético se requiere la autorización expresa de la organización a la cual requiere la actividad, en los últimos años firmas importantes de auditoria respaldan esta actividad y la ofrecen dentro de su portafolio de servicios, dando un respaldo e impulso a esta actividad.

El hacker ético debe tener habilidades de ingeniería social, programación, ingenio, etc. habilidades mínimas que cualquier hacker debe manejar.

En la actualidad varias empresas que requieren seguridad en sus procesos contratan estos servicios, para asegurar su infraestructura, a través de diversas metodologías y herramientas, que permiten valorar los puntos vulnerables a ataques informáticos, con el fin de defensa y protección de los datos de la organización, esto finaliza con un informe final que es entregado formalmente con un acuerdo de confidencialidad, para que con esta información la organización sea capaz de mitigar las amenazas reportadas en el mismo, de darse el caso la empresa o experto que auditó puede cubrir los servicios de aseguramiento, implementación, mitigación de los eventos de seguridad reportados.

Las pruebas generadas en la auditoría informáticas, se las denomina pruebas de penetración, o pruebas de pen test que son efectuadas con el consentimiento del titular de los datos en la infraestructura de la organización.

1.3.2 Hacking malicioso

A la vez que el hacking ético existe su contraparte el hacking malicioso. Hoy en día las amenazas son más sofisticadas y con las mismas oportunidades que antes. Todo tipo de información es amenazada, más y más ataques se generan a diario afectando sin distinción a las organizaciones, por ejemplo:

- Comodo: En marzo de 2011, un intruso comprometió a un socio de negocios de Comodo, consiguiendo 9 certificados digitales ilegalmente concedidos, afectando a varios sitios operados por Google, Microsoft, Skype y Yahoo, esto muestra el potencial de los atacantes y de la información sensibles a la que pueden llegar a tener acceso

- RSA: En marzo de 2011, RSA Security, EMC Corporation fue infiltrada por un atacante que envió un email de phising con un archivo adjunto de Microsoft Excel. Este archivo contenía una amenaza de día cero de Adobe Flash Player, que mediante una puerta trasera permite el control remoto de los equipos, obtener passwords y acceso a información sensible.
- Sony PlayStation: En abril 2011, hackers lograron obtener acceso a la red de Sony, obteniendo información de tarjetas de crédito, información personal, incluido nombres, fechas de nacimiento, direcciones, emails, online, de alrededor de 100 millones de clientes, toda esta información está valorada en el mercado negro hasta por un millón de dólares. (Lawrence C. Miller, 2014, págs. 6, 7)

1.3.3 Pentesting

Es el procedimiento metodológico y sistemático de la ejecución de un ataque simulado en la red informática, con el propósito de identificar, evaluar y resolver vulnerabilidades de seguridad.

1.3.4 Pentesting en la actualidad

- Se considera como un recurso más para las tareas comunes en la seguridad corporativa.
- En algunas organizaciones se vuelve un elemento formal (Ej.: Normas PCI, ISO27001)

- Existen varios tipos de análisis diferentes, por esto se vuelve importante conocerlos para un uso adecuado.
- Las actualizaciones automáticas han sido un hito importante en el control de la seguridad, pero estas tienen sus limitantes, y se vuelven escasas para mitigar problemas con sitios web de aplicaciones, que presentan problemas graves.
- Cada una de ellas puede aportar diferente visión de las amenazas, por es esto es importante la elección adecuada ya que puede afectar significativamente las pruebas.

1.3.5 Variantes pentesting.

- BlackBox: EL consultor no dispone de información de Red o sistemas
- WhiteBox: El consultor tiene disponible toda la información de red, accesos, passwords, códigos fuente, etc. del sistema o red a analizar.
- GrayBox: Si el consultor dispone información parcial (Ips Publicas, Accesos, pero no códigos fuente)

1.4 Herramientas de análisis

Las herramientas de análisis son parte fundamental de la auditoría de seguridad ya que a través de ellas se logra una visibilidad global del nivel de exposición de los sistemas informáticos sean estos externos o internos.

1.4.1 OpenVas

Open Vulnerability Assessment System es un conjunto de diversos servicios y herramientas que contemplan el escaneo y el análisis de vulnerabilidades, tanto en sistemas operativos, servicios como y equipos en red.

OpenVAS utiliza distintos protocolos para crear solicitudes que permiten establecer las vulnerabilidades que se están ejecutando en servidores o equipo de red; Adicional, el eje de la arquitectura de OpenVAS está orientado a servicios protegidos por SSL y la utilización de actualizaciones de pruebas de vulnerabilidades de red (NVTs), que contiene más de 35.000 registros de análisis. Las actualizaciones NVT están configuradas como predeterminadas para OpenVAS desde el repositorio global en internet.

1.4.1.1 Características

OpenVAS opera principalmente con 3 servicios:

- OpenVAS Scanner. Es el servicio encargado de ejecutar las pruebas de vulnerabilidad (NVT - Network Vulnerability Test) contra los objetivos fijados.
- OpenVAS Manager. Es el servicio central que contiene toda la inteligencia del sistema, gestionando las planificaciones, ejecuciones e informes de las distintas evaluaciones.
- OpenVAS Administrador. El servicio permite el manejo de distintos usuarios y vista sincronizadas.

1.4.1.2 Arquitectura

Arquitectura OpenVas

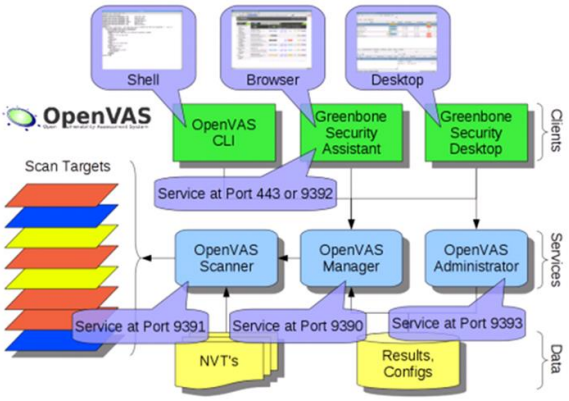


Figura 3. Detalle arquitectura OpenVas
Fuente: http://www.openvas.org/about-software.html

1.4.1.3 Proceso de evaluación

El proceso que utiliza OpenVAS para la evaluación de vulnerabilidades, se divide en siete actividades que permiten realizar eficientes análisis de vulnerabilidades.

- Detectar los Sistemas en Funcionamiento
- Identificar los Sistemas en Funcionamiento
- Enumerar los Servicios
- Identificar los Servicios
- Identificar las Aplicaciones
- Identificar las Vulnerabilidades
- Reportar las Vulnerabilidades

1.4.1.4 Vulnerabilidades y amenazas

La vulnerabilidad es el punto débil o falible de la infraestructura informática que es susceptible a ataques de la seguridad del mismo, dando como respuesta perdida de confidencialidad de la información de la organización. Es decir, los elementos que componen la infraestructura informática tienen un punto frágil, que es posible que alguien ataque en los elementos de la infraestructura informática, aprovechando ese punto débil.

Las debilidades pueden aparecer en cualquiera de los elementos que componen la infraestructura informática, tanto en hardware o software.

Las vulnerabilidades se clasifican mediante cinco aspectos fundamentales:

- **Producto.** Se refiere a la vulnerabilidad que tiene el producto en su versión.
- **Donde.** La vulnerabilidad se presenta en módulos o configuraciones que son parte del sistema.
- **Causas y consecuencias.** Desarrollo de aplicaciones sin tener manejo de buenas prácticas de desarrollo, que da origen a nuevas vulnerabilidades. Como resultado se presentan desbordamientos de memoria o uso excesivo de la misma, dando pautas para análisis avanzados de vulnerabilidades de personas no son parte del equipo de desarrollo u organización.
- **Impacto.** Se define la gravedad de ejecutar código arbitrario (malware, virus, etc.), pudiendo conseguir información confidencial o denegación de servicios del sistema.

- **Vector de ataque.** Es el envío de información especialmente manipulada a la víctima (usuario o sistema), dando como resultado, que el atacante direccione a la víctima a lugares donde puede explotar vulnerabilidades.

Tipos de vulnerabilidades.

A continuación, se mencionan algunos ataques más comunes para la infraestructura que está expuesta a internet, algunas de ellas están presentes en los informes de seguridad que se muestran en el punto 2.4 Análisis y Mitigación de vulnerabilidades.

- Ataque por la fuerza.

  El atacante genera todas combinaciones de caracteres de formar combinaciones hasta obtener la contraseña correcta.

- Ataque de hombre en medio.

  El atacante adquiere la capacidad de leer, insertar y modificar los mensajes entre dos partes sin que ninguna de ellas conozca que el enlace ha sido vulnerado. El atacante debe tener la capacidad de observar e interceptar los mensajes entre las víctimas.

- Negación de servicio.

  El ataque se enfoca a los servicios, tienen por objetivo colapsar del sistema o red para evitar que los servicios y recursos puedan ser utilizados por los usuarios.

- SQL injection.

  El ataque se genera cuando introducen datos suministrados por el usuario como parte de una consulta SQL. Una inyección SQL sucede cuando se inserta código SQL invasor dentro de otro código SQL para perturbar su funcionamiento normal.

- Cross Site Scripting (XSS).

  Se trata de una vulnerabilidad que compromete especialmente la seguridad del usuario que navega por internet y no la seguridad del servidor. Es una vulnerabilidad relativamente fácil de explotar ya que no requiere de importantes conocimientos de algún complicado lenguaje de programación ni nada similar, basta con tener idea de las etiquetas HTML y conocer algún lenguaje de scripting. Estas se dividen en 3 grupos: Tipo0 cuando se utiliza código remoto con permisos de otro usuario; Tipo 1, cuando es un ataque no persistente utilizado en páginas no estáticas; Tipo 2, Ataque persistente, donde se inyecta código en páginas estáticas (Destripa la Red Hacking Practico, 2008, págs. 490-491).

- Spoofing.

  Es una técnica donde un intruso logra conseguir acceso no autorizado alterando los paquetes haciéndolos aparecer como tráfico seguro originado desde una red valida y de privilegios elevados (Checkpoint Software Tecnologies, 2009).

1.4.2 Gestión de vulnerabilidades.

En la actualizad la gestión de vulnerabilidades se ha estandarizado mediante organización MITRE que es un aliado en el área de tecnología e investigación del gobierno de EEUU. La organización MITRE desarrollo de un sistema que permite conocer su gravedad de la vulnerabilidad de forma objetiva, permitiendo responder a todos los parámetros definidos de las vulnerabilidades con los estándares CVE, CVSS, NVT.

1.4.3 CVE (Common Vulnerabilities and Exposures).

El proyecto CVE, provee referencias de seguridad estandarizadas que permite a los consumidores desarrollar proceso de gestión del sistema vulnerabilidades con CVE.

El CVE proporciona una base de datos que contiene nombres estandarizados para las vulnerabilidades y las exposiciones de seguridad, permitiendo que productos de seguridad informática tengan un punto de referencia para la evaluación de vulnerabilidades en las infraestructuras informáticas. Adicional, a medida que se van encontrando nuevas vulnerabilidades, la organización MITE realiza la asignación del identificado, manteniendo actualizado la base de vulnerabilidades.

El manejo de la notación del estándar CVE, se basa en 3 parámetros.

- Nombre de la estándar (CVE).
- El año de asignación del código CVE (2014)
- Numero de cuatro cifras, que identifica a la vulnerabilidad (2983).

1.4.4 CVSS (Common Vulnerability Scoring System)

El CVSS es un estándar abierto que establece los grados de severidad, clasifica la facilidad de aprovechar un fallo y el impacto del problema, a través de fórmulas establecida por la organización MITRE y mediante la utilización de una escala del 0 a 10, donde se considera baja si la puntuación obtenida esta entre 0.0 y 3.9, medio si se ubica entre 4.0 y 6.9 y alto cuando el puntaje cae dentro del rango 7.0 y 10.0.

El objetivo del estándar CVSS, permite a los administradores de tecnología conocer de manera puntual el riesgo o nivel de compromiso de la confidencialidad, integridad y disponibilidad de los datos.

Las ventajas de utilizar CVSS:

- **Puntuaciones estandarizadas de la vulnerabilidad.** cuando una Organización estandariza las puntuaciones de vulnerabilidad, y se ve reflejada en una política se puede aprovechar dicha política de gestión, estableciendo la rapidez con la que la vulnerabilidad debe ser validada y remediada.
- **Marco abierto**. Dentro de la utilización del estándar CVSS, proporciona al usuario los detalles sobre los parámetros usados en la generación de la puntuación de la vulnerabilidad analizada, permitiendo al usuario comprender el razonamiento que sustenta la puntuación.
- **Riesgo priorizado**. Al establecer la puntuación de la vulnerabilidad, el estándar CVSS permite conocer el nivel de riesgo de la vulnerabilidad con su respectiva solución, permitiendo al usuario conocer la importancia la vulnerabilidad en relación con otra en su arquitectura, se puede identificar como riesgo bajo, medio y alto.

1.4.4.1 Impacto

El impacto de vulnerabilidad se refiere a las propiedades (confidencialidad, integridad y disponibilidad) del componente afectado. Donde, sí la vulnerabilidad es explotada con éxito en unos de los componentes (hardware, software), los indicadores de impacto se calificarán de acuerdo al componente que sufre el peor resultado, asociado a un ataque con éxito. Es decir, las métricas de impacto deben reflejar el impacto de la CIA (confidencialidad, integridad y disponibilidad)

- **Impacto confidencialidad.** La confidencialidad es la limitación de acceso a la información de una organización a usuarios no autorizados. Esta métrica mide el grado de confidencialidad de la información que gestiona un aplicativo debido a una vulnerabilidad. Mediante la utilización de la escala alta, baja y ninguna, donde se considera a un impacto de confidencialidad alto cuando existe acceso total a la información contenida, lo que resulta que toda la información dentro del componente afectado se divulgue al atacante, se considera a un impacto de confidencialidad baja donde existe cierta pérdida de confidencialidad y se obtiene acceso a cierta información restringida, pero el atacante no tiene control sobre lo que se obtiene de la información; un impacto de confidencialidad ninguno, se considera cuando no hay pérdida de confidencialidad dentro del componente afectado
- **Disponibilidad de impacto.** Este indicador se refiere a la perdida de la disponibilidad del componente afectado, tales como un servicio en red (por ejemplo, web, bases de datos, correo electrónico). Dado que la disponibilidad se refiere a la accesibilidad de los recursos de información, ataques que consumen ancho de banda, ciclos de procesador, o espacio en disco todo el

impacto de la disponibilidad de un componente afectado, también se define en los siguientes grupos:

-Alta (High) Hay una pérdida total de la disponibilidad, lo que resulta en que el atacante es capaz de negar completamente el acceso a los recursos en el componente afectado

-Baja (Low) hay una reducción en el rendimiento o interrupciones en la disponibilidad de recursos. Incluso si la explotación repetida de la vulnerabilidad es posible, el atacante no tiene la capacidad de negar por completo el servicio a los usuarios legítimos.

- Ninguno (None) No hay ningún impacto a la disponibilidad dentro del componente impactado

- **Integridad de impacto.** Esta mide el impacto de la integridad de una vulnerabilidad explotada con éxito. La integridad se refiere a la fiabilidad y veracidad de la información. La lista de posibles valores se presenta como alta, media, baja. Esta métrica valor aumenta con el impacto del componente afectado definiendo niveles:
- Alta (H) Hay una pérdida total de la integridad , o una pérdida completa de la protección. Por ejemplo, el atacante es capaz de modificar cualquier o todos los archivos protegidos por el componente afectado.
- - Bajo (Low) Modificación de los datos es posible, pero el atacante no tener control sobre la consecuencia de una modificación, o está limitada la cantidad de modificación.

- Ninguno (None) No hay ningún impacto a la disponibilidad dentro del componente impactado

A continuación, se fórmula la ecuación de CVSS para calcular el impacto de una vulnerabilidad, con sus variables definidas, (www.first.org/cvss).

```
Impacto = 10,41 * (1- (1-ConfImpact) * (1-IntegImpact) * (1-
AvailImpact))
ConfImpact = caso de ConfidentialityImpact
                        Ninguno: 0.0
                        parcial: 0.275
                        completar: 0.660

IntegImpact = caso de IntegrityImpact
                        Ninguno: 0.0
                        parcial: 0.275
                        completar: 0.660

AvailImpact = caso de AvailabilityImpact
                        Ninguno: 0.0
                        parcial: 0.275
                        completar: 0.660
```

1.4.4.2 Explotabilidad

Cuantifica el nivel de riegos que pueden vulnerarse en la infraestructura, se puede valorar los siguientes aspectos:

- **Autenticación.** Mide el número de veces que un atacante debe autenticarse en un objetivo con el fin de aprovechar una vulnerabilidad.
- **Vector de acceso.** Medida que refleja cómo se explota una vulnerabilidad. Cuanto más compleja para un usuario malintencionado y esta le permita atacar a un host, mayor será la puntuación de vulnerabilidad.

- **Acceso complejo.** Mide la complejidad del ataque requerido para explotar la vulnerabilidad una vez que un atacante ha ganado acceso al sistema de destino.

A continuación, se fórmula ecuación de CVSS para calcular el explotabilidad de una vulnerabilidad, con sus variables definidas.

```
explotabilidad = 20 * AccessVector * AccessComplexity * autenticación
```

```
AccessVector = caso AccessVector del
                        Requiere acceso local: 0,395
                        Red adyacente accesible: 0,646
                        Red accesible: 1.0

AccessComplexity = caso AccessComplexity de
                        Alta: 0,35
                        Mediano: 0,61
                        Bajo: 0,71

autenticación = caso de autenticación del
                        Requiere varias instancias de autenticación:
0.45
                        Requiere sola instancia de autenticación: 0,56
                        No requiere autenticación: 0,704
```

1.4.4.3 Base de puntuación CVSS

La ecuación de base es la plataforma de la puntuación CVSS.

A continuación, se fórmula ecuación de CVSS para calcular el explotabilidad de una vulnerabilidad, con sus variables definidas.

```
BaseScore = round_to_1_decimal(((0.6*Impact)+(0.4*Exploitability)-
1.5)*f(Impact))

f(Impact) = 0 if Impact=0; 1.176 otherwise
```

Las funciones mencionadas nos proporcionan la información cuantificada en el análisis realizado por Openvas, este software permite facilitar la tarea de cuantificar los riegos, impactos y explotabilidad asociados de la infraestructura ya que procesa cada uno de los valores entregando los resultados listos para su uso mediante el estándar CVSS.

1.5 Organizaciones

1.5.1 Red Cedia

RED CEDIA, la Fundación Consorcio Ecuatoriano para el Desarrollo de Internet Avanzado, es la Red Nacional de Investigación y Educación Ecuatoriana – RNIE (NREN por sus siglas en inglés).

Creada para estimular, promover y coordinar el desarrollo de las tecnologías de información y las redes de telecomunicaciones e informática, enfocadas al desarrollo científico, tecnológico, innovador y educativo en el Ecuador, por medio del Proyecto de Redes Avanzadas.

RED CEDIA está encabezada por un Directorio que autoriza la celebración de convenios, contratos y operaciones económicas al Director Ejecutivo. Las labores cotidianas de RED CEDIA están a cargo del equipo de trabajo bajo la Dirección Ejecutiva.

Cada institución miembro presenta ante RED CEDIA un representante principal que es el/la Rector/a más dos representantes técnicos, a los cuales se les informa de todo evento y acontecimiento.

RED CEDIA es parte de Red CLARA que es la Cooperación Latinoamericana de Redes Avanzadas, formada por redes de instituciones pares de RED CEDIA en Latinoamérica conocidas como Redes Nacionales de Investigación y Educación. Red CLARA, a su vez, interconecta a las RNIEs latinoamericanas con las redes avanzadas internacionales en distin - tos continentes: Norte América, Europa, Asia y África. Entre estas redes se encuentran Intenet2, GEANT2, CANARI, APAN, UbuntuNet, ESNET y NLR, Adicional a esto, la red Cedia tiene su CSIRT (Computer Emergency Response Team) y sus objetivos son:

- Apoyar a los miembros de la comunidad del CEDIA a implementar medidas proactivas con el objetivo de reducir los riesgos de incidentes de seguridad informáticos
- Apoyar a la comunidad del CEDIA a responder a estos incidentes cuando ocurran. (CEDIA).

CAPÍTULO 2

MARCO METODOLÓGICO

2.1 Análisis

De acuerdo a la metodología planteada OSSTMM, se ha recolectado información que es valiosa para la medición de la seguridad de la información.

2.2 Proceso inicial

El proyecto usa herramientas de Pentesting, estas herramientas requieren una infraestructura para implementarlas, mediante esta infraestructura, se permitirá generar el análisis de los servidores del grupo IDEIA-GEOCA. La plataforma en este estudio se generó a nivel de la red LAN (interno) y WAN (externo).

2.2.1 Recursos de infraestructura

En base a las reuniones mantenidas con el administrador de la plataforma se define que la infraestructura del IDEGEOCA, no cuenta con protecciones adecuadas y que cada servidor esta publicado directamente con la ip publica en la interfaz Wan del equipamiento, sin contar con ACLs de restricción de tráfico, con este preámbulo se define que se requiere realizar un análisis de la situación actual de la seguridad y riesgo expuestos, al mantener la arquitectura directamente publicada hacia el internet, con este fin los autores del documento implementaron la infraestructura externamente (cloud privada), para que desde el internet se haga un escaneo de vulnerabilidades.

Para este fin se dispone de los siguientes recursos contratados temporalmente, mientras dure la culminación del presente proyecto a un costo de 50 dólares mensuales.

Hardware:

- 1 Servidor HP DL380G8
- 48 GB de RAM
- 2TB de disco

Para el tema de implementación de software de escaneo de vulnerabilidades, se defino que debe realizarse con software libre, cumpliendo con una de las políticas establecidas por el centro de investigación IDE-IA-GEOCA, por lo tanto, se propuso el uso de las siguientes herramientas, de las más comunes dentro de la auditoria de seguridad en el mundo opensource, se selecciona herramientas, tanto de virtualización para aprovechar los recursos del servidor como Vmware, marca reconocida en el mundo de virtualización usando el licenciamiento sin costo que para la aplicación de test ejecuta sin problemas y para el análisis usamos la herramienta OpenVas por su trayectoria de desarrollo desde el año 2008 en sus inicios conocida como Nessus y usamos como sistema operativo base Kali Linux por su trayectoria como suite de auditoria de seguridad informática antes conocido como Backtrack. Nmap parte de la suite Kali y Vmware Workstation Trial, para replicar el escenario externo al interno de Centro de investigación.

Software:

- VMware ESXi 5.5 Free Edition
- Kali Linux
- OpenVas
- Nmap
- VMWare Workstation

Para el análisis usamos la infraestructura del ISP TEUNO, quien nos provee el datacenter housing del servidor y su acceso internet de 80 megas tanto de subida como bajada.

2.2.2 Implementación

2.2.2.1 Kali Linux

La implementación de este sistema operativo, consiste en descargar el iso de la página web oficial:

http://cdimage.kali.org/kali-2016.1/kali-linux-2016.1-amd64.iso

Una vez descargado, procedemos crear la máquina virtual y cargar el iso a la plataforma de VMware.

Seguimos los sencillos pasos del asistente en modo gráfico:

Proceso de instalación KALI Linux

Figura 4. Instalación Kali
Elaborado por: Darwin Jiménez y Marcelo Osorio

2.2.2.2 OpenVas

La implementación de OpenVas, se la realiza sobre el Sistema operativo levantado, se requiere descargar el paquete correspondiente desde la página oficial. www.kali.org/download o mediante los comandos de instalación apt-get o yum en algunos sistemas Operativos

Comandos de instalación:

Se actualiza el sistema operativo y se procede a instalar openvas

```
root@testide:~# apt-get update
:~# apt-get dist-upgrade
```

Posteriormente se inicializa openvas

```
root@testide:~# apt-get install openvas
root@testide:~# openvas-setup
```

Salida donde indica que las bases de datos de openvas ha sido actualizada y se genera un password aleatorio para el usuario gsad:

```
[i] This script synchronizes an NVT collection with the 'OpenVAS
NVT Feed'.
[i] Online information about this feed:
'http://www.openvas.org/openvas-nvt-feed
...
sent 1143 bytes received 681741238 bytes 1736923.26 bytes/sec
total size is 681654050 speedup is 1.00
[i] Initializing scap database
[i] Updating CPEs
[i] Updating /var/lib/openvas/scap-data/nvdcve-2.0-2002.xml
[i] Updating /var/lib/openvas/scap-data/nvdcve-2.0-2003.xml
...
Write out database with 1 new entries
Data Base Updated
Restarting Greenbone Security Assistant: gsad.
User created with password '6062d074-0a4c-4de1-a26a-
5f9f055b7c88'.
```

Una vez implementado validamos si los servicios de manager, scanner y GSAD estén ejecutándose en los puertos:

```
root@testide:~# netstat -antp

Active Internet connections (servers and established)

Proto Recv-Q Send-Q Local Address Foreign Address State

PID/Program name

tcp 0 0 127.0.0.1:9390 0.0.0.0:* LISTEN 9583/openvasmd

tcp 0 0 127.0.0.1:9391 0.0.0.0:* LISTEN 9570/openvassd: Wai

tcp 0 0 127.0.0.1:9392 0.0.0.0:* LISTEN 9596/gsad
```

Inicio de servicios:

```
root@testide:~# openvas-start

Starting OpenVas Services

Starting Greenbone Security Assistant: gsad.

Starting OpenVAS Scanner: openvassd.

Starting OpenVAS Manager: openvasmd.
```

2.2.2.3 Zenmap

La instalación de Zenmap, es muy simple, tanto en Windows como en Linux para instalar en Linux Centos se requiere ejecutar el comando ***su*** *-c "yum install nmap-frontend"* o el comando *sudo apt-get install Zenmap* para otros sistemas Linux, en Windows únicamente es necesario obtener el instalador desde la página y ejecutar el ejecutable y seguir los pasos del asistente de instalación.

Pantalla Principal NMAP

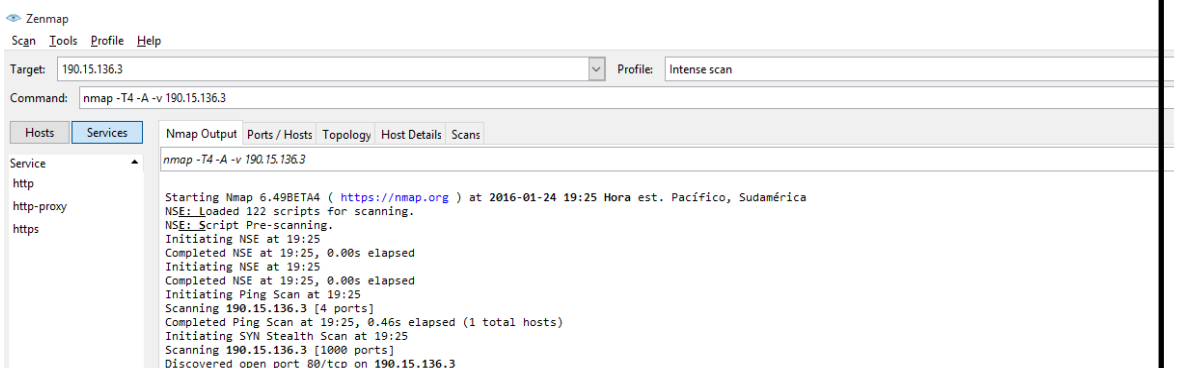


Figura 5. NMAP
Elaborado por: Darwin Jiménez y Marcelo Osorio

2.3 Información general.

Recopilando la información se genera 3 gráficos descriptivos de la infraestructura, aquí se detallan los puertos, ips , nombres de cada uno de los equipos objetos de estudio de esta revisión, esta información fue entregada por el administrador de la plataforma como punto de partida del estudio.

2.3.1 Servicios 190.15.136.3

Este Servidor se encuentra operando con los siguientes servicios:

- Postgres 9.0
- Tomcat
- Mysql
- Joomla - http https
- VNC
- SSH
- FTP

Este servidor actúa como Servidor Web y sirve de repositorio a los proyectos de Geoportales desarrollado por los estudiantes y el portal actual y anterior ide.ups.edu.ec.

Diagrama de servicios 190.15.136.3

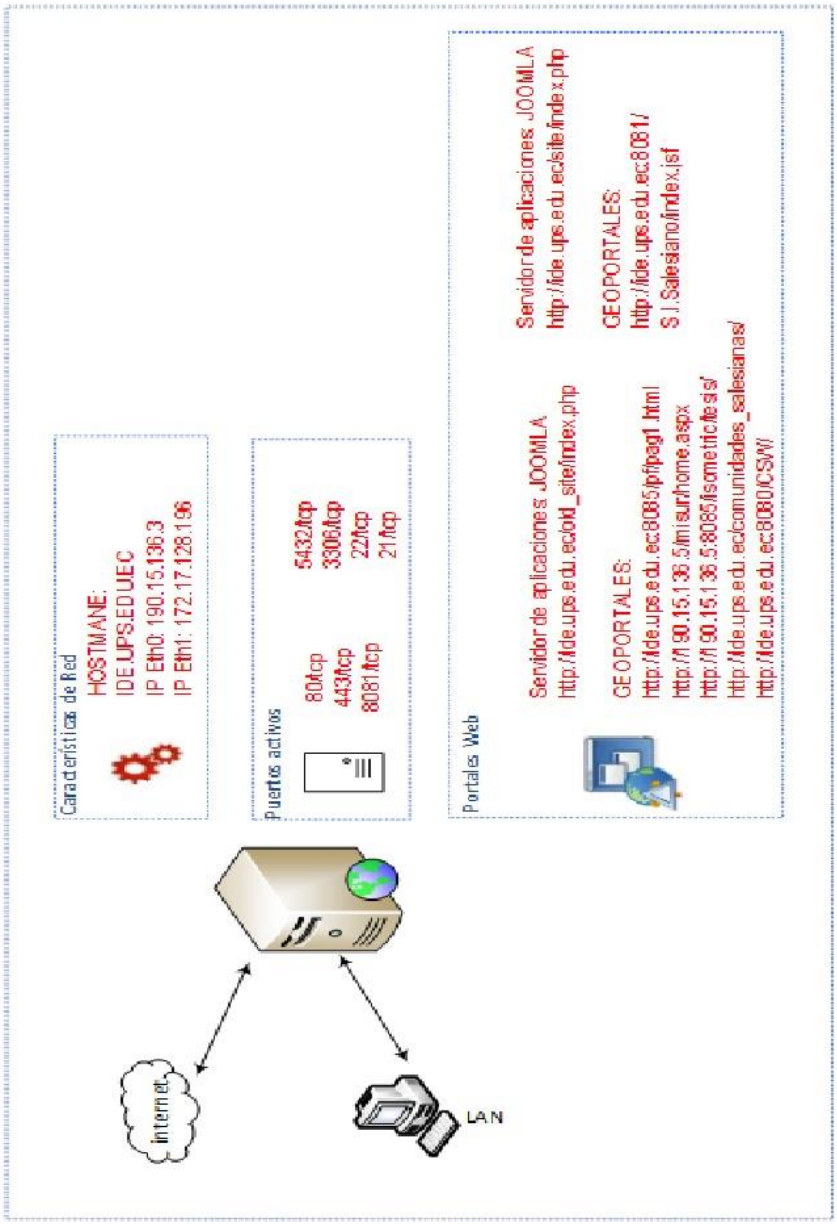


Figura 6. Servicios ide.ups.edu.ec 190.15.136.3
Elaborado por: Darwin Jiménez y Marcelo Osorio

2.3.2 Servicios 190.15.136.4

Este Servidor se encuentra operando con los siguientes servicios:

- Tomcat http – https
- Jboss
- Mysql
- Postgress
- VNC
- SMTP

Este servidor esta designado para el monitoreo de enlaces de la infraestructura, corriendo la herramienta Cacti y Munin

Diagrama de servicios 190.15.136.4

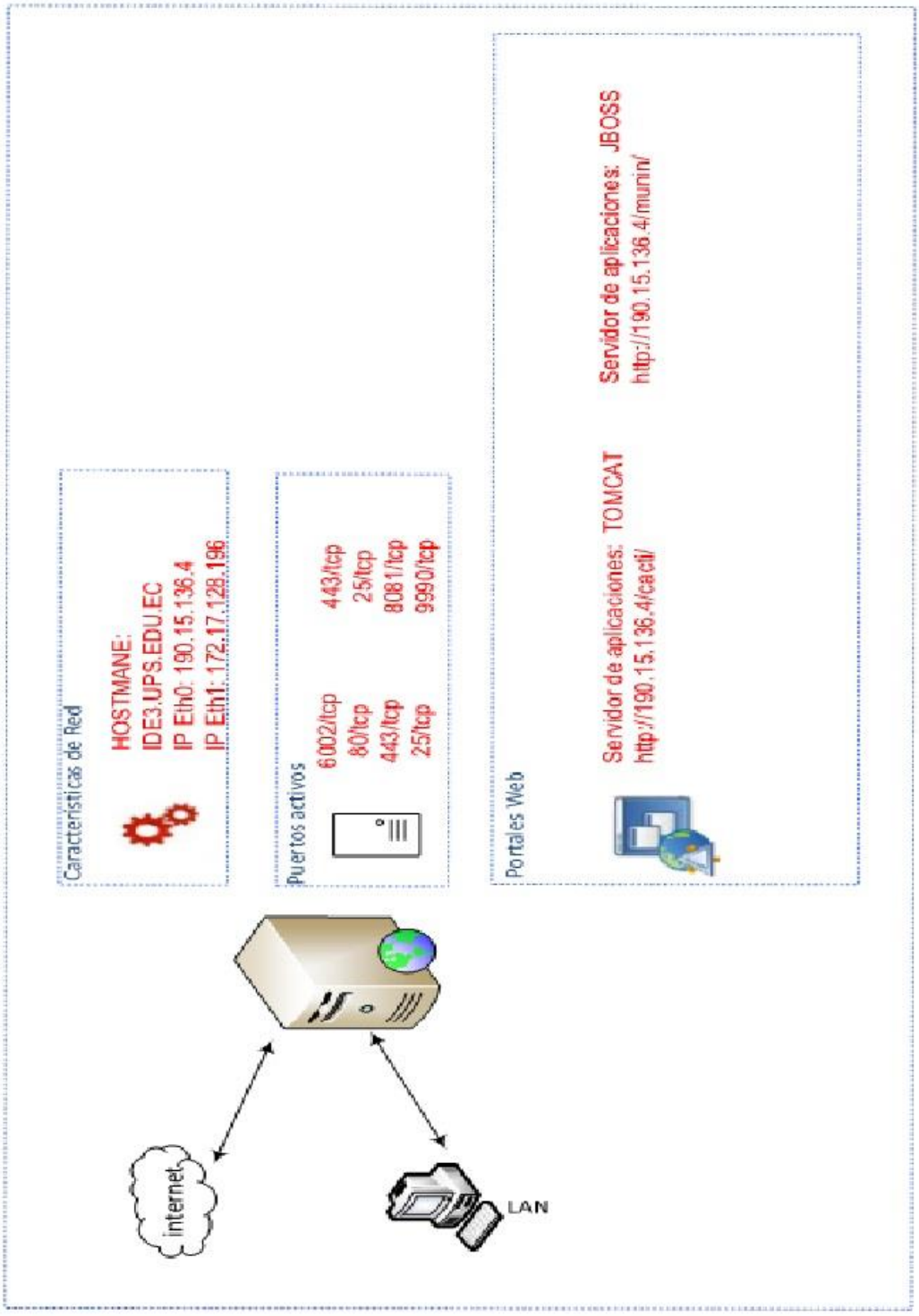


Figura 7. Servicios Ide3.ups.edu.ec
Elaborado por: Darwin Jiménez y Marcelo Osorio

2.3.3 Servicios 190.15.136.10

Este Servidor se encuentra operando con los siguientes servicios:

- Tomcat http – https
- Mysql
- GlassPhish
- VNC
- Postgress

Este servidor esta designado para tesis y tareas administrativas

Diagrama de servicios 190.15.136.10

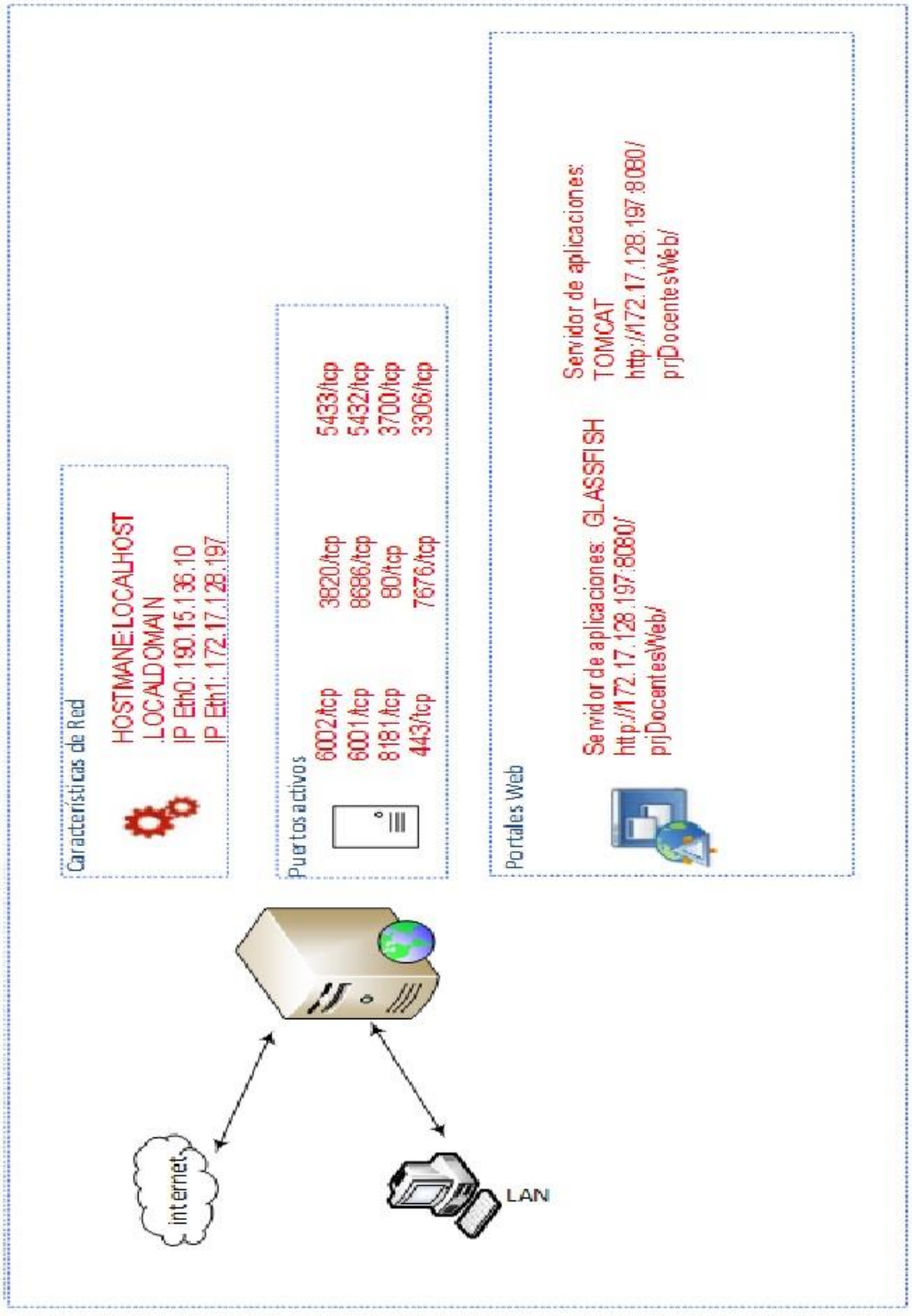


Figura 8. Servicios localhost.local 190.15.136.10
Elaborado por: Darwin Jiménez y Marcelo Osorio

2.4 Análisis y mitigación de vulnerabilidades.

Los resultados del análisis de seguridad en la infraestructura del Grupo de investigación IDE-IA-GEOCA han arrojado datos que se representan en el siguiente resumen de resultados.

El análisis se basa en datos recopilados con la herramienta OpenVAS con las siguientes características:

Tabla 1. Características de Análisis

Fecha de análisis de vulnerabilidad:	6/06/2015	**Duración del análisis:**	3 días
Tipo de organización:	Educación/ investigación	**País:**	Ecuador
Servidores analizados:	IDE1, IDE3 y IDE5	**Redes analizadas:**	WAN - LAN
Herramienta de análisis:	OpenVas /kali Linux	**Modo análisis:**	Reporte WAN - LAN

Nota. Información del análisis realizado
Elaborado por: Darwin Jiménez y Marcelo Osorio

El presente análisis de vulnerabilidades de la infraestructura IDE-IA-GEOCA se ha clasificado en función del segmento testeado de la red.

La infraestructura comprende el análisis WAN y LAN en base a la Figura 9:

Diagrama de Red de Análisis

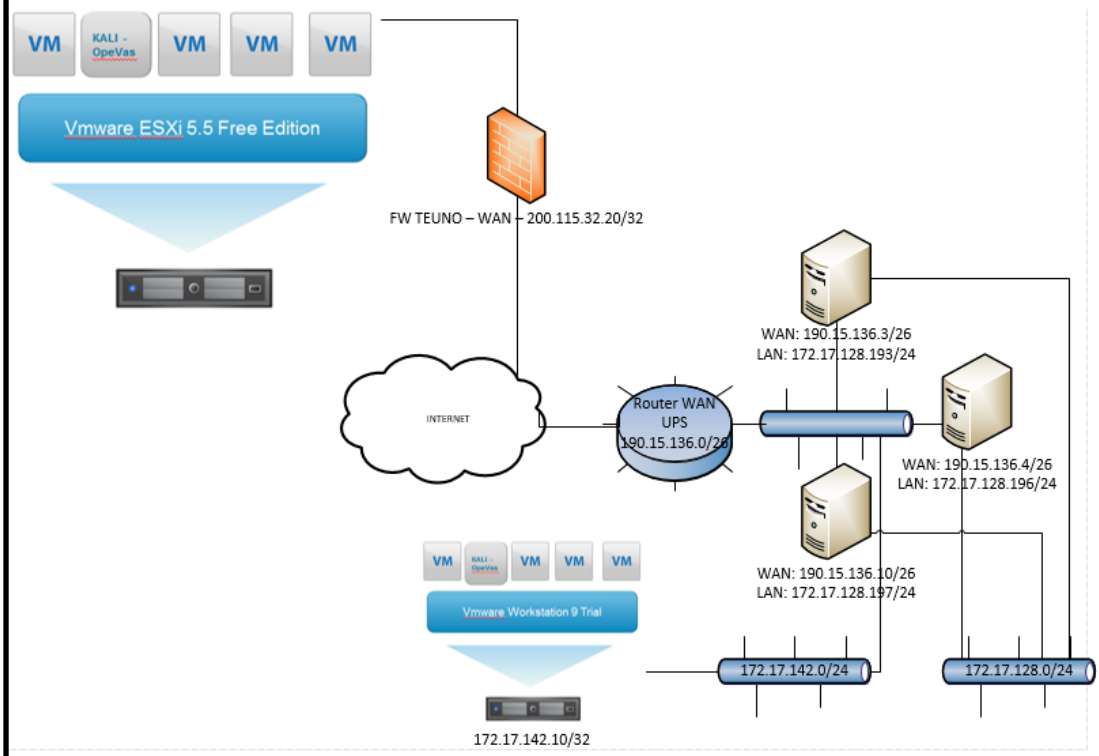


Figura 9. Topología de red
Elaborado por: Darwin Jiménez y Marcelo Osorio

En la siguiente tabla se presentan un informe cualitativo del riesgo de las vulnerabilidades a nivel WAN en los servidores IDE-IA-GEOCA:

Tabla 2. Resumen de amenazas perimetrales internet

Nombre	**Host / Servidor**	**Alta**	**Media**	**Baja**	**Log**	**Falso Positivos**
Ide.ups.edu.ec	190.15.136.3	1	3	1	29	0
Ide3.ups.edu.ec	190.15.136.4	6	7	2	59	0
Localhost.localdomain	190.15.136.10	3	9	1	43	0
	Total: 3	10	19	4	131	0

Nota. Describe el riesgo de las amenazas perimetrales de la arquitectura de IDE-IA-GEOCA
Elaborado por: Darwin Jiménez y Marcelo Osorio

En la siguiente tabla se presentan un informe cualitativo del riesgo de las vulnerabilidades a nivel LAN en los servidores IDE-IA-GEOCA:

Tabla 3. Resumen de amenazas internas LAN

	Host / Servidor	**Alta**	**Media**	**Baja**	**Log**	**Falso Positivos**
Ide.ups.edu.ec	172.17.128.193	2	6	2	43	0
Ide3.ups.edu.ec	172.17.128.196	1	3	1	29	0
Localhost.localdomain	172.17.128.197	3	7	1	43	0
	Total: 3	6	18	4	115	0

Nota. Describe el riesgo de las amenazas en la red LAN de la arquitectura de IDE-IA-GEOCA
Elaborado por: Darwin Jiménez y Marcelo Osorio

2.4.1 Análisis de vulnerabilidades de los segmentos WAN y LAN.

A continuación, se detalla las características del servidor con sus respectivos puertos, su nivel de vulnerabilidades e impactos que generan en los servicios de red LAN como WAN para los servidores del IDE-IA-GEOCA.

2.4.1.1 Impacto servidor ide.ups.edu.ec - 190.15.136.3

EL servidor ide.ups.edu.ec, es accesible desde el internet por ende está expuesto a riesgo los cuales, en la tabla 4 se hace referencia a información general del servidor el cual será objeto de estudio y revisión.

Tabla 4. Características técnicas ide.ups.edu.ec

Características técnicas			
Hostname	IDE.UPS.EDU.EC	**Virtualizador**	VMware
Sistema Operativo	Centos Plus 64 bits	**Interfaces de red**	Eth0 y Eth1
Versión	5.9	**IP Eth0**	190.15.136.3
Kernel	2.6.18-348.3.1.EL5	**IP Eth1**	172.17.128.193
Procesador	Intel Xeon X5650	**UpTime**	179 días
Core	Dual		
RAM	5 GB		
Disco Duro	250 GB		

Nota. Describe las características de la arquitectura de IDE-IA-GEOCA
Elaborado por: Darwin Jiménez y Marcelo Osorio

Luego del análisis sobre la red WAN del servidor 190.15.136.3, se puede observar que existen varias amenazas o vulnerabilidades explotables, cada una de ellas tiene un nivel de riesgo, clasificado dentro del impacto como Alto (rojo), Medio (naranja), Bajo (amarillo).

Tabla 5. Impacto de vulnerabilidades y ataques - ide.ups.edu.ec

	Vulnerabilidades Altas - WAN - ide.ups.edu.ec		
	Puerto	**Vulnerabilidad**	**Efecto**
	80/tcp	Phpinfo() CVSS: 7,5	Localhost/phpinfo divulga la información potencialmente sensible.
	Vulnerabilidades Altas - LAN - ide.ups.edu.ec		
	6002 /tcp	X Server CVSS: 10	Atacante puede enviar datos basura y ralentizar su sesión “X” o incluso colgar el servidor.
	80/tcp 443/tcp	phpinfo() output accesible	El archivo phpinfo divulga la información potencialmente sensible. CVSS:7,5
	Ataques – Sistema Operativo - ide.ups.edu.ec		
	SSH2	Brute force attack (PAM 2 authentication) - Analysis LOG secure Jul-2015	Se realiza ataque de fuerza bruta con las IPs 43.229.53.40, 218.65.30.217, 43.229.53.36, 218.87.111.116, 218.65.30.23, 59.45.79.117, 218.87.111.118, 218.87.111.108, 43.229.53.36 y 43.255.189.85 al usuario Root del sistema operativo.
	FTP	Brute force attack - Analysis Log VSFTP Jul-2015	Las IPs 81.31.240.56, 52.2.140.58, 87.139.125.232, 5.39.216.121, 61.240.144.65, 141.212.122.146, 188.138.1.218, 141.212.122.50, 182.118.53.91, 201.15.106.130 realizan ataque de fuerza bruta al servicio FTP.

	MySQL	Exploit Mysql_db – Analysis log Mysql Jul-2015	Las IPs 173.254.230.5, 101.36.82.176, 122.226.102.9, 173.254.230.5, 198.55.106.137 y 173.254.230.5 realizan conexiones de testeo al puerto 3306 de MySQL.

	Vulnerabilidades MEDIAS – WAN - ide.ups.edu.ec		
	Puerto	**Vulnerabilidad**	**Efecto**
	443/tcp	SSL Certification Expired CVSS:5 Check for SSL Weak Ciphers CVSS:4,3 POODLE SSLv3 Protocol CBC ciphers Information Disclosure Vulnerability CVSS:4,3	El certificado SSL en el servicio remoto expiró el 04/01/2012. Permite a un atacante acceder como hombre de medio y acceder al flujo de datos.

	Vulnerabilidades BAJAS – WAN – ide.ups.edu.ec		
	Puerto	**Vulnerabilidad**	**Efecto**
	Gerente/tcp * Referencia a todos los puertos en TCP.	TCP timestamps CVSS:2,6	El host remoto implementa marcas de tiempo TCP y por lo tanto permite calcular el tiempo de actividad del servidor.
	22/tcp	SSH CVSS:2	Se detecta el tipo y la versión del servidor SSH mediante la conexión con el servidor y el procesamiento de la memoria intermedia recibida. Esta información da a los atacantes potenciales información adicional sobre el sistema que están atacando. Versiones y Tipos deben omitirse cuando sea posible.
	80/tcp	Cacti Detection CVSS:1,5	El atacante puedo visualizar el servicio, nombre de la aplicación, versión y localización.
	21/tcp	FTP Banner Detection CVSS:1,3	Se detecta la Bandera Servidor FTP: 220 Bienvenido al servidor FTP del CIMA.

Nota: Descripción del impacto de las vulnerabilidades y ataques al servidor ide.ups.edu.ec
Elaborado por: Darwin Jiménez y Marcelo Osorio

2.4.1.2 Impacto servidor ide3.ups.edu.ec - 190.15.136.4

EL servidor ide3.ups.edu.ec, es accesible desde el internet por ende está expuesto a riesgo los cuales, en la tabla 6 se hace referencia a información general del servidor el cual será objeto de estudio y revisión.

Tabla 6. Características técnicas ide.ups3.edu.ec

Características técnicas			
Hostname	Ide3.ups.edu.ec	Virtualizador	VMware
Sistema Operativo	Centos Plus 64 bits	Interfaces de red	Eth0 y Eth1
Versión	6.6	IP Eth0	190.15.136.4
Kernel	2.6.32-331.17.1.el6	IP Eth1	172.17.128.196
Procesador	Intel Xeon X5650 2.67 GHz	UpTime	239 días
Core	Dual		
RAM	4 GB		
Disco Duro	250 GB		

Nota: Descripción de las características técnicas del servidor ide.ups3.edu.ec
Elaborado por: Darwin Jiménez y Marcelo Osorio

Luego del análisis sobre la red WAN del servidor 190.15.136.4, se puede observar que existen varias amenazas o vulnerabilidades explotables, cada una de ellas tiene un nivel de riesgo, clasificado dentro del impacto como Alto (rojo), Medio (naranja), Bajo (amarillo).

Tabla 7. Impacto de vulnerabilidades y ataques – ide3.ups.edu.ec

	Vulnerabilidades Altas – WAN –ide3.ups.edu.ec		
	Puerto	**Vulnerabilidad**	**Efecto**
	6002 /tcp	X Server CVSS:10	Atacante puede enviar datos basura y ralentizar su sesión "X" o incluso colgar el servidor.
	80/tcp	Php-cgi-based CVSS:7,5 Phpinfo() CVSS:7,5	EL archivo localhost/phpinfo divulga la información potencialmente sensible.
	443/tcp	Php-cgi-based CVSS:7,5	Concede al atacante remoto observar código fuente de los archivos y obtener información sensible.
	25/tcp	SMTP too long line CVSS:7,5 SMTP antivirus scanner DoS CVSS:7,2	Algunos escáneres de antivirus mueren cuando procesan un correo electrónico con una cadena demasiado tiempo sin saltos de línea. Dicho mensaje fue enviado.
	Vulnerabilidades Altas – LAN –ide3.ups.edu.ec		
	80/tcp 443/tcp	phpinfo() output accesible CVSS: 7,5	El archivo phpinfo divulga la información potencialmente sensible.

			Provee información de que usuario instalo el php, ip host, directorio root, versión de web server y del sistema operativo Linux.
	Ataques – Sistema Operativo –ide3.ups.edu.ec		
	SSH2	Brute force attack (PAM 2 authientication) - Analysis LOG secure Jul-2015	Se realiza ataque de fuerza bruta con las IPs 43.229.53.40, 43.255.189.85, 182.100.67.102 y 43.229.53.36 al usuario Root del sistema operativo.

	Vulnerabilidades Medias – WAN –ide3.ups.edu.ec		
	Puerto	Vulnerabilidad	Impacto
	443/tcp	Check for SSL Weak Ciphers CVSS:4,3 Deprecated SSLv2 and SSLv3 Protocol Detection Poodle SSL CVSS:4,3	Un atacante podría ser capaz de utilizar las fallas criptográficas conocidas para espiar la conexión entre los clientes y el servicio.
	25/tcp	Check if Mail server answer to VRFY and EXPN requests CVSS:4,3	El servidor de correo electrónico responde a VRFY y EXPN, donde responde información de la cuenta.
	8081/tcp	Apache Tomcat servlet/JSP container default files CVSS:6,8	Un atacante puede determinar la versión exacta del Apache Tomcat y explotar sus vulnerabilidades.
	9990/tcp	Infinite HTTP request CVSS:5	El servidor web acepta peticiones ilimitadas. Puede ser vulnerable al ataque WWW solicitud infinita, saturando la memorita y matando al servidor.
	4848/tcp	SSL Certification Expired CVSS:5 DCShop exposes sensitive files CVSS:5	El certificado SSL del servidor remoto ya ha expirado. Se detectado la versión CGI DCShop vulnerable. Esta versión no protege adecuadamente la información del usuario y tarjeta de crédito. Es posible acceder a los archivos que contienen las contraseñas administrativas, actuales y transacciones pendientes y la información de tarjeta de crédito.
	Vulnerabilidades Medias – LAN –ide3.ups.edu.ec		
	443/tcp	OpenSSL CCS Man in the Middle Security Bypass Vulnerability Poodle CVSS: 4,3 SSL Certification Expired CVSS: 5 Check for SSL Weak Ciphers CVSS:4,3	Permite a un atacante acceder como hombre de medio y acceder al flujo de datos. El servidor tiene el certificado SSL.

	Vulnerabilidades BAJAS – WAN – ide3.ups.edu.ec		
	Puerto	Vulnerabilidad	Efecto
	8181/tcp	Fingerprint web server with favicon.ico CVSS:2,1	El servidor web remoto contiene una imagen gráfica que es propenso a la divulgación de información.
	General/tcp	TCP timestamps CVSS:2,6	El host remoto implementa marcas de tiempo TCP y por lo tanto permite calcular el tiempo de actividad del servidor.
	Vulnerabilidades BAJAS – LAN – ide3.ups.edu.ec		
	443/tcp	TCP timestamps CVSS:2,6	El host remoto implementa marcas de tiempo TCP y por lo tanto permite calcular el tiempo de actividad del servidor.

Nota: Descripción del impacto de las vulnerabilidades y ataques al servidor ide3.ups.edu.ec

Elaborado por: Darwin Jiménez y Marcelo Osorio

2.4.1.3 Impacto servidor localhost.localdomain - 190.15.136.10

EL servidor 190.15.136.10, es accesible desde el internet por ende está expuesto a riesgo los cuales, en la tabla 8 se hace referencia a información general del servidor el cual será objeto de estudio y revisión

Tabla 8. Características técnicas servidor Localhost.localdomain

Características técnicas			
Hostname	LOCALHOST.LOCALDOMAIN	**Virtualizador**	VMware
Sistema Operativo	Centos Plus 64 bits	**Interfaces de red**	Eth0 y Eth1
Versión	6.6	**IP Eth0**	190.15.136.10
Kernel	2.6.32-431.3.1.el6	**IP Eth1**	172.17.128.197
Procesador	Intel Xeon X5650 2.67 GHz	**UpTime**	223 días
Core	Dual		
RAM	4 GB		
Disco Duro	250 GB		

Nota: Descripción de características técnicas del servidor localhost.localdomain
Elaborado por: Darwin Jiménez y Marcelo Osorio

Luego del análisis sobre la red WAN del servidor 190.15.136.4, se puede observar que existen varias amenazas o vulnerabilidades explotables, cada una de ellas tiene un nivel de riesgo, clasificado dentro del impacto como Alto (rojo), Medio (naranja), Bajo (amarillo).

Tabla 9. Impacto de vulnerabilidades y ataques – localhost.localdomain

	Vulnerabilidad ALTA – LAN/WAN - localhost.localdomain		
	Puerto	Vulnerabilidad	Efecto
	6002/tcp 6001/tcp	X Server CVSS: 10	Atacante puede enviar datos basura y ralentizar su sesión "X" o incluso colgar el servidor.
	8181/tcp	Oracle GlassFish/System Application Server Web Container DOS Vulnerability CVSS: 7,8	Permite al atacante causar la DOS (denegación del servicio)
	Ataques – Sistema Operativo		
	SSH2	Brute force attack (PAM 2 authientication) - Analysis LOG secure Jul-2015	Se realiza ataque de fuerza bruta con las IPs 43.229.53.40 y 43.255.189.85 al usuario Root del sistema operativo.

	Vulnerabilidades MEDIAS – localhost.localdomain – WAN		
	Puerto	**Vulnerabilidad**	**Efecto**

	8181/tcp	Oracle GlassFish Server Multiple XSS and CSRF Vulnerabilities. CVSS:6,8 Oracle GlassFish Server Expression Evaluation Security Bypass Vulnerability. CVSS:6,4 SSL Certification Expired CVSS:5 Oracle GlassFish Server Hash Collision Denial of Service Vulnerability CVSS:5 Oracle GlassFish Server Multiple Unspecified Vulnerabilities CVSS:5	El atacante puede ingresar código arbitrario en el HTML y Script El atacante puede ejecutar sobre el browser. El certificado SSL en el servicio remoto expiró el 2014-12-13 El atarante puede utilizar el HTTP Post y generar la denegación del servicio, El certificado SSL en el servicio remoto expiró el 13/12/2014
	443/tcp	Check for SSL Weak Ciphers CVSS:4,3 Deprecated SSLv2 and SSLv3 Protocol Detection CVSS: 4,3 POODLE SSLv3 Protocol CBC ciphers Information Disclosure Vulnerability CVSS:4,3	Cifrados débiles que ofrece del servicio SSL3 y TLS1. Un atacante podría ser capaz de utilizar las fallas criptográficas conocidas para espiar la conexión entre los clientes y el servicio para tener acceso a los datos confidenciales transferidos dentro de la conexión segura. El atacante puede usar el fallo de seguridad y acceder a datos sensibles. Permite a un atacante acceder como hombre de medio y acceder al flujo de datos.
	3820/tcp	Check for SSL Weak Ciphers CVSS:4,3	Cifrados débiles que ofrece del servicio SSL3 y TLS1. Un atacante podría ser capaz de utilizar las fallas criptográficas conocidas para espiar la conexión entre los clientes y el servicio para tener acceso a los datos confidenciales transferidos dentro de la conexión segura.
	Vulnerabilidades MEDIAS – localhost.localdomain – LAN		

	8181/tcp	Oracle GlassFish Server Multiple XSS and CSRF Vulnerabilities CVSS:6,8	El atacante puede insertar código arbitrario HTML y Script. Afectando al sitio web
	443/tcp	Check for SSL Weak Ciphers CVSS: 4,3 Deprecated SSLv2 and SSLv3 Protocol Detection Poodle CVSS: 4,3	SSL contiene cifrados débiles. El atacante puedo acceder mediante una criptografía conocida, donde intercepta la comunicación entre servicio y cliente.

	Vulnerabilidad BAJA – localhost.localdomain – WAN		
	Puerto	Vulnerabilidad	Efecto
	22/tcp	SSH Protocol Versions Supported CVSS:2	Se detecta el tipo y la versión del servidor SSH mediante la conexión con el servidor y el procesamiento de la memoria intermedia recibida. Esta información da a los atacantes potenciales
	21/tcp	FTP Banner Detection CVSS:2	Se detecta la Bandera Servidor FTP: 220 Bienvenido al servidor Centos de Patsy Prieto
	General/tcp * Referencia a todos los puertos en TCP.	TCP timestamps CVSS:2,6	El host remoto implementa marcas de tiempo TCP y por lo tanto permite calcular el tiempo de actividad. Un efecto secundario de esta característica es que el tiempo de funcionamiento de la máquina remota a veces puede ser calculado.
	Vulnerabilidad BAJA – localhost.localdomain – LAN		
	General/tcp * Referencia a todos los puertos en TCP.	TCP timestamps CVSS:2,6	El host remoto implementa marcas de tiempo TCP, por lo tanto, permite calcular el tiempo de actividad del servidor.

Nota: Descripción del impacto de las vulnerabilidades y ataques al servidor localhost.localdomain
Elaborado por: Darwin Jiménez y Marcelo Osorio

2.4.2 Mitigación de vulnerabilidades de los segmentos WAN y LAN

A continuación, se detalla la solución a las vulnerabilidades que presenta en el análisis de los servidores de IDE-IA-GEOCA.

2.4.2.1 Mitigación servidor ide.ups.edu.ec - 190.15.136.3

Tabla 10. Mitigación vulnerabilidades – ide.ups.edu.ec

	Vulnerabilidades Alta - ide.ups.edu.ec – WAN		
	Puerto	Vulnerabilidad	Solución
	80/tcp	Phpinfo()	Eliminar o limitar el acceso archivo phpinfo. CVE-2012-1823 /2311/2336/2335
	Vulnerabilidad Alta - ide.ups.edu.ec – LAN		
	6002 /tcp	X Server	Recomienda filtrar las conexiones entrantes entre el rango 6000-6009. CVE-1999-0526.
	80/tcp 443/tcp	phpinfo() output accesible	Eliminar o limitar el acceso archivo phpinfo
	Ataques – Sistema Operativo – ide.ups.edu.ec		
	SSH2	Brute force attack (PAM 2 authientication) - Analysis LOG secure Jul-2015	Bloquear el servicio ssh puerto 22 desde la red WAN
	FTP	Brute force attack - Analysis Log VSFTP Jul-2015	Bloquear el servicio el servicio ftp y ftps puerto 21 y 22
	MySQL	Exploit Mysql_db – Analysis log Mysql Jul-2015	Bloquear el puerto 3306 del servicio mysql.

	Vulnerabilidades Media - ide.ups.edu.ec –WAN		
	Puerto	Vulnerabilidad	Solución
	443/tcp	SSL Certification Expired Check for SSL Weak Ciphers POODLE SSLv3 Protocol CBC ciphers Information Disclosure Vulnerability	Generar y cargar nuevas certificado SSL. La configuración de estos servicios no admite permitir cifrados débiles. Actualizar el Open SSL CVE-2014-3566

	Vulnerabilidades BAJA – ide.ups.edu.ec – WAN		
	Puerto	Vulnerabilidad	Solución
	General/tcp	TCP timestamps	Desactivar las marcas de tiempo TCP en Linux agregar la línea 'net.ipv4.tcp_timestamps = 0 ' a /etc/sysctl.conf.
	22/tcp	SSH	Aplicar el filtrado para no permitir el acceso a este puerto desde hosts no confiables
	21/tcp	FTP Banner Detection	Cambiar el número de puerto, deshabilitar accesos anónimos y generar contraseñas complicadas de vulnerar.
	Vulnerabilidades BAJA – ide.ups.edu.ec – LAN		
	80/tcp	Cacti Detection	Cerrar el puerto o restringir el acceso a los usuarios.

Nota: Descripción de las mitigaciones de las vulnerabilidades presentadas en el servidor ide.ups.edu.ec
Elaborado por: Darwin Jiménez y Marcelo Osorio

2.4.2.2 Mitigación servidor ide3.ups.edu.ec - 190.15.136.4

Tabla 11. Mitigación vulnerabilidades – ide3.ups.edu.ec

	Vulnerabilidad ALTA – ide3.ups.edu.ec –WAN		
	Puerto	Vulnerabilidad	Solución
	6002 /tcp	X Server	Recomienda filtrar las conexiones entrantes entre el rango 6000-6009. CVE-1999-0526.
	80/tcp	Php-cgi-based Phpinfo()	PHP está recomendando que los usuarios actualicen a la última versión de PHP. Eliminar o limitar el acceso archivo phpinfo. CVE-2012-1823 /2311/2336/2335.
	443/tcp	Php-cgi-based	PHP ha lanzado la versión 5.4.3 y 5.3.13 para abordar esta vulnerabilidad. CVE-2012-1823 /2311/2336/2335.
	25/tcp	SMTP too long line SMTP antivirus scanner DoS	Bloquear el puerto 25 o instalar herramienta anti SPAM o actualizar el antivirus.
	Vulnerabilidad ALTA – ide3.ups.edu.ec –LAN		
	80/tcp 443/tcp	phpinfo() output accesible	Eliminar o limitar el acceso archivo phpinfo. CVE-2012-1823 /2311/2336/2335.
	Ataque – Sistema Operativo – ide3.ups.edu.ec		
	SSH2	Brute force attack (PAM 2 authentication) - Analysis LOG secure Jul-2015	Aplicar el filtrado para no permitir el acceso a este puerto desde hosts no confiables.

	Vulnerabilidad MEDIA – ide3.ups.edu.ec –WAN		
	Puerto	Vulnerabilidad	Solución
	443/tcp	Check for SSL Weak Ciphers Deprecated SSLv2 and SSLv3 Protocol Detection	Deshabilitar los protocolos SSLv2 y/o SSLv3, para no admitir cifrados débiles. Se recomienda manejar el protocolo TLSv1+.
	25/tcp	Check if Mail server answer to VRFY and EXPN requests	Deshabilitar VRFY y EXPN en el servidor de correo electrónico. URL:http://cr.yp.to/smtp/vrfy.html
	8081/tcp	Apache Tomcat servlet/JSP container default files	Eliminar archivos predeterminados JSP y servlets del contenedor Apache Tomcat.
	9990/tcp	Infinite HTTP request	Actualizar su software o protegerlo con iptables. CVE-2001-0760
	4848/tcp	SSL Certification Expired DCShop exposes sensitive files	Vuelva a colocar el certificado SSL nuevo. Cambiar el nombre de los directorios siguientes: - Data - User_carts - Orders - Auth_data Renombrar los archivos dcshop.setup y dcshop_admin.setup http://www.securiteam.com/unixfocus/5RP0N2K4KE.html CVE-2001-0821
	Vulnerabilidad MEDIA – ide3.ups.edu.ec –LAN		
	443/tcp	OpenSSL CCS Man in the Middle Security Bypass Vulnerability SSL Certification Expired Check for SSL Weak Ciphers	Generar y cargar nuevas certificado SSL. La configuración de estos servicios no admite los permitir cifrados débiles. Actualizar el Open SSL CVE-2014-3566

	Vulnerabilidad BAJA – ide3.ups.edu.ec –WAN		
	Puerto	Vulnerabilidad	Solución
	8181/tcp	Fingerprint web server with favicon.ico	Quite el archivo ' favicon.ico "o crear uno personalizado para su sitio.

	General/tcp * Referencia a todos los puertos en TCP.	TCP timestamps	Desactivar las marcas de tiempo TCP en Linux agregar la línea 'net.ipv4.tcp_timestamps = 0 ' a /etc/sysctl.conf.
	Vulnerabilidad BAJA – ide3.ups.edu.ec –LAN		
	443/tcp	TCP timestamps	Desactivar las marcas de tiempo TCP en Linux agregar la línea 'net.ipv4.tcp_timestamps = 0 ' a /etc/sysctl.conf.

Nota: Descripción de las mitigaciones de las vulnerabilidades presentadas en el servidor ide3.ups.edu.ec
Elaborado por: Darwin Jiménez y Marcelo Osorio

2.4.2.3 Mitigación servidor localhost.localdomain - 190.15.136.10

Tabla 12. Mitigación vulnerabilidades – localhost.localdomain

	Vulnerabilidad ALTA – localhost.localdomain – WAN		
	Puerto	Vulnerabilidad	Solución
	6002/tcp 6001/tcp	X Server	Recomienda filtrar las conexiones entrantes entre el rango 6000-6009. CVE-1999-0526.
	8181/tcp	Oracle GlassFish/System Application Server Web Container DOS Vulnerability	Aplicar las actualizaciones de seguridad http://www.oracle.com/technetwork/topics/security/cpuoct2011-330135.html CVE-2011-3559
	Vulnerabilidad ALTA – localhost.localdomain – LAN		
	6002 /tcp 6001/tcp	X Server	Recomienda filtrar las conexiones entrantes entre el rango 6000-6009. CVE-1999-0526.
	8181/tcp	Oracle GlassFish/System Application Server Web Container DOS Vulnerability	Aplicar las actualizaciones de Glassfish: http://www.oracle.com/technetwork/topics/security/cpuoct2011-330135.html
	Ataques – Sistema Operativo - localhost.localdomain		
	SSH2	Brute force attack (PAM 2 authentication) - Analysis LOG secure Jul-2015	Aplicar el filtrado para no permitir el acceso a este puerto desde hosts no confiables

	Vulnerabilidad MEDIA – localhost.localdomain – WAN		
	Puerto	Vulnerabilidad	Solución
	8181/tcp	Oracle GlassFish Server Multiple XSS and CSRF Vulnerabilities. Oracle GlassFish Server Expression	Aplique el parche desde abajo vínculo, http://www.oracle.com /technetwork/topics/security/cpuapr2012-366314.html CVE: CVE-2012-0550, CVE-2012-055.

		Evaluation Security Bypass Vulnerability. SSL Certification Expired Oracle GlassFish Server Hash Collision Denial of Service Vulnerability Oracle GlassFish Server Multiple Unspecified Vulnerabilities	Aplique el parche desde abajo vínculo, http://www.oracle.com/technetwork/topics/security/cpujul2012-392727.html Vuelva a colocar el certificado SSL nuevo. Aplique el parche desde abajo vínculo, http://www.oracle.com/technetwork/topics/security/cpujan2012-366304.html Aplique el parche desde abajo vínculo, http://www.oracle.com/technetwork/topics/security/cpujan2012-366304.html
	443/tcp	Check for SSL Weak Ciphers Deprecated SSLv2 and SSLv3 Protocol Detection POODLE SSLv3 Protocol CBC ciphers Information Disclosure Vulnerability	Generar y cargar nuevas certificado SSL. La configuración de estos servicios no admite los permitir cifrados débiles. Desactivar el SSLv2 y SSLv3 y remplazar por TLSv1+ Actualizar el Open SSL CVE-2014-3566
	3820/tcp	Check for SSL Weak Ciphers	Generar y cargar nuevas certificado SSL. La configuración de estos servicios no admite los permitir cifrados débiles.
	Vulnerabilidad MEDIA – localhost.localdomain- LAN		
	8181/tcp	Oracle GlassFish Server Multiple XSS and CSRF Vulnerabilities	Aplicar las actualizaciones de Glassfish: http://www.oracle.com/technetwork/topics/security/cpuapr2012-366314.html
	443/tcp	Check for SSL Weak Ciphers Deprecated SSLv2 and SSLv3 Protocol Detection	La configuración de este servicio debe ser cambiada y no usar soportes débiles. Deseabilidad la versiones SSLv2 / SSL3 y usar SSLv1+.

	Vulnerabilidad BAJA – localhost.localdomain – WAN		
	Puerto	**Vulnerabilidad**	**Solución**
	22/tcp	SSH Protocol Versions Supported	Aplicar el filtrado para no permitir el acceso a este puerto desde hosts no confiables.

	21/tcp	FTP Banner Detection	Cambiar el número de puerto, deshabilitar accesos anónimos y generar contraseñas complicadas de vulnerar.
	Gerente/tcp *Referencia a todos los puertos en TCP.		Para desactivar las marcas de tiempo TCP en Linux agregar la línea 'net.ipv4.tcp_timestamps = 0' a /etc/sysctl.conf. Ejecutar 'sysctl -p' para aplicar la configuración en tiempo de ejecución.
	Vulnerabilidad BAJA – localhost.localdomain – LAN		
	general/tcp	TCP timestamps	Desactivar las marcas de tiempo TCP en Linux agregar la línea 'net.ipv4.tcp_timestamps = 0 ' a /etc/sysctl.conf.

Nota: Descripción de las mitigaciones de las vulnerabilidades presentadas en el servidor localhost.localdomain
Elaborado por: Darwin Jiménez y Marcelo Osorio

2.4.3 Puntuación CVSS de las vulnerabilidades

Las siguientes tablas presentan un informe cuantitativo del impacto y explotabilidad de las vulnerabilidades en los servidores IDE-IA-GEOCA, basados en la información entregada por la herramienta OpenVas, con los cálculos internos entrega el valor de CVSS.

Para obtener los valores cuantificables del análisis, es necesario generar la sumatoria de todas las puntaciones de las vulnerabilidades asociadas, a los grupos alta, media y baja, definidos por el estándar CVSS, de esta manera se obtiene una matriz donde la suma de estas, nos entrega el universo de referencia, para obtención de un valor porcentual de los riesgos.

2.4.3.1 CVSS - Perimetrales internet

Tabla 13. Valores CVSS perimetrales internet

Nombre	Host / Servidor	Alta	Media	Baja	Total CVSS
Ide.ups.edu.ec	190.15.136.3	7,5	13,6	7,6	28,7
Ide3.ups.edu.ec	190.15.136.4	39,7	34,7	4,7	79,1
Localhost.localdomain	190.15.136.10	17,8	45,4	6,6	69,8

Nota: Descripción de las sumatoria de valores CVSS en el área perimetral
Elaborado por: Darwin Jiménez y Marcelo Osorio

Tabla 14. Riesgos perimetrales internet

Nombre	Host / Servidor	Alta	Media	Baja
Ide.ups.edu.ec	190.15.136.3	26%	47%	26%
Ide3.ups.edu.ec	190.15.136.4	50%	44%	6&
Localhost.localdomain	190.15.136.10	54%	41%	5%
Promedio:		**43%**	**44%**	**13%**

Nota: Descripción del riesgo perimetral de los servidores IDE-IA-GEOCA, con valores porcentual
Elaborado por: Darwin Jiménez y Marcelo Osorio

2.4.3.2 CVSS - Internas LAN

Tabla 15. Valores CVSS internas LAN

Nombre	Host / Servidor	Alta	Media	Baja	Total CVSS
Ide.ups.edu.ec	172.17.128.193	25,3	0	0	25,3
Ide3.ups.edu.ec	172.17.128.196	7,5	13,6	2,6	23,7
Localhost.localdomain	172.17.128.197	7,9	15,4	2,6	35,8

Nota: Descripción de las sumatoria de valores CVSS en la red LAN
Elaborado por: Darwin Jiménez y Marcelo Osorio

Tabla 16. Riesgos internos LAN

Nombre	Host / Servidor	Alta	Media	Baja
Ide.ups.edu.ec	172.17.128.193	100%	0	0
Ide3.ups.edu.ec	172.17.128.196	32%	57%	11%
Localhost.localdomain	172.17.128.197	50%	43%	7%
	Promedio:	**60%**	**33%**	**6%**

Nota: Descripción del riesgo de la red LAN de los servidores IDE-IA-GEOCA, con valores porcentual
Elaborado por: Darwin Jiménez y Marcelo Osorio

CAPÍTULO 3

PROTOTIPO EXPERIMENTAL

2.5 Firewall Builder

Herramienta que permite la administración grafica GUI, de uso profesional, que permite construir reglas de cortafuegos simplificadas, flexibles y sin necesidad de conocer comandos, ni sintaxis para la creación de reglas de firewall.

La metodología de Administración se basa en crear un conjunto de objetos que describen a cada servidor, redes, subredes, luego implementar su política de firewall arrastrando objetos en las reglas de política.

También puede tomar ventaja de una gran colección de objetos predefinidos que describen muchos protocolos y servicios estándar. Una vez que una política se basa en la interfaz gráfica de usuario, puede compilarlo e instalarlo en una, o varias máquinas, firewall.

Firewall Builder gestiona políticas de firewall para una serie de plataformas, incluyendo Netfilter / iptables, ipfw, PF, Cisco PIX, y otros

2.5.1 Implementación

Para iniciar el proceso de instalación, se necesita que se acepte los términos de licenciamiento del producto Firewall Builder. La herramienta Firewall Builder tiene sus políticas de aceptación de uso basados en los términos de licenciamiento GNU v2.

GNU

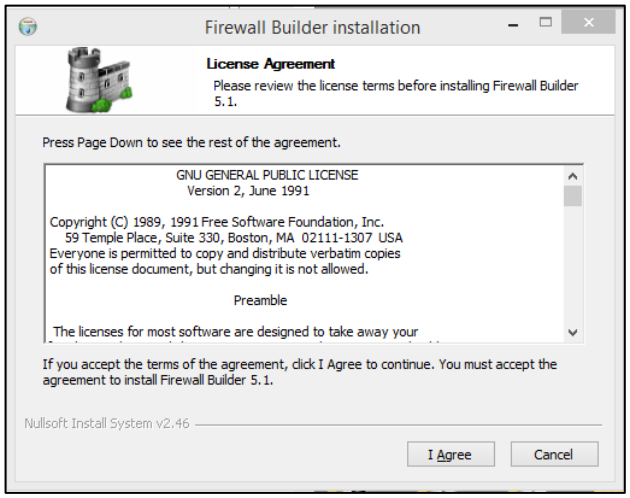


Figura 10. Acuerdo GNU
Elaborado por: Darwin Jiménez y Marcelo Osorio

Al iniciar el proceso de configuración de la herramienta Firewall Builder, se presenta una ventana de bienvenida, donde presenta la guía de configuración rápida. Se selecciona el botón Watch the guide.

Fw Builder

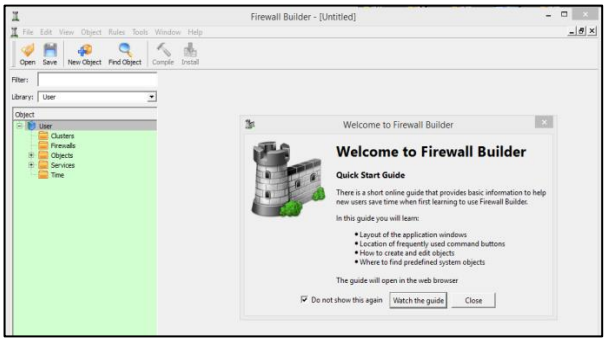


Figura 11. Watch guide FwBuilder
Elaborado por: Darwin Jiménez y Marcelo Osorio

Para continuar con el proceso de configuración se selecciona el botón Create new firewall, donde permitirá generar configuraciones nuevas del firewall.

Menú FWBuilder

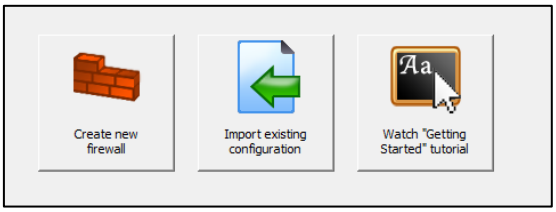


Figura 12. Create new firewall FWBuilder
Elaborado por: Darwin Jiménez y Marcelo Osorio

Se presenta una ventana básica de configuración, donde debe establecer el nombre del nuevo firewall, el tipo de firewall y la versión de sistema operativo donde se ejecuta el firewall.

Adicional, se selecciona la opción Use Preconfigured Firewall Template, donde se mostrará sugerencias de buenas prácticas de acuerdo a la configuración física, correspondiente a la arquitectura de firewall a implementar, en el caso de los servidores IDE, se toma la opción software firewall iptables y OS Linux 2.4/2.6

Firewall Object

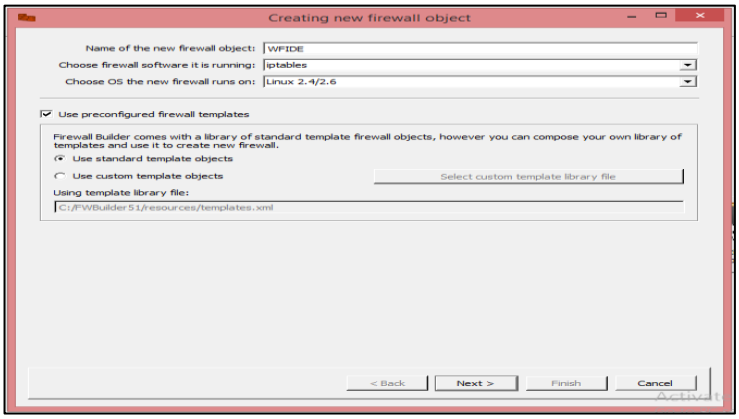


Figura 13. New object FwBuilder
Elaborado por: Darwin Jiménez y Marcelo Osorio

Para la implementación de la política de seguridad en los servidores de IDE-IA-GEOCA, se selecciona el Fw Template1, ya que cumple con el perfil de políticas acceso predeterminadas para la red WAN y LAN en dos interfaces de red tal como se especifica en el hardware para los equipos mencionados.

Templates

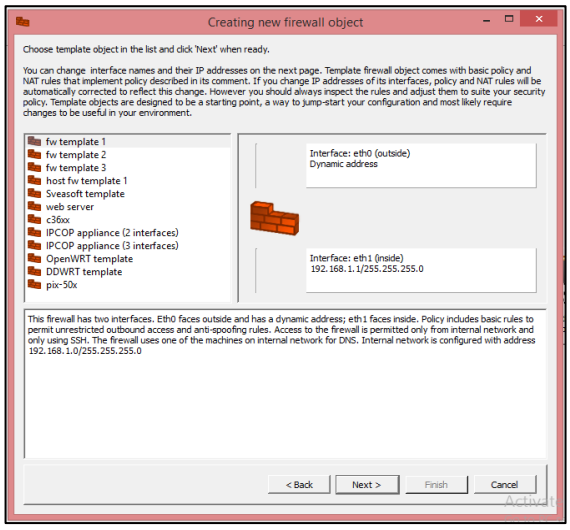


Figura 14. Template FwBuilderContinuando con la configuración del objeto firewall, se debe agregar
Elaborado por: Darwin Jiménez y Marcelo Osorio

IP address WAN, Netmask WAN y el protocolo IPv4, que es correspondiente a la interface eth0.

Nuevo objeto Eth0

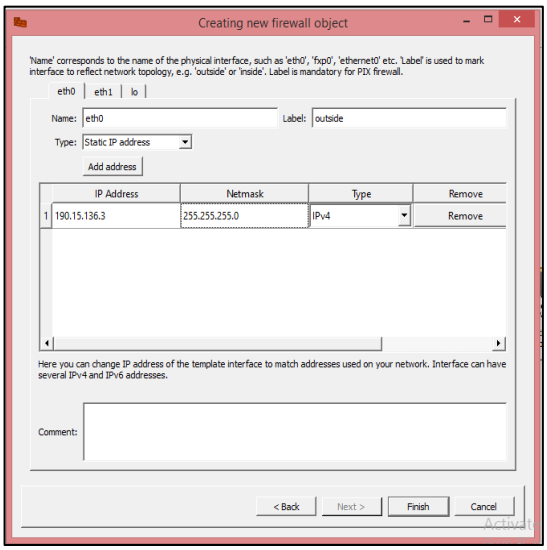


Figura 15. New object eth0 FwBuilder
Elaborado por: Darwin Jiménez y Marcelo Osorio

La configuración de los parámetros LAN se los realizan en la interface eth1, donde se ingresa la IP address LAN, Netmask LAN y el protocolo IPv4.

Nuevo Objeto Eth1

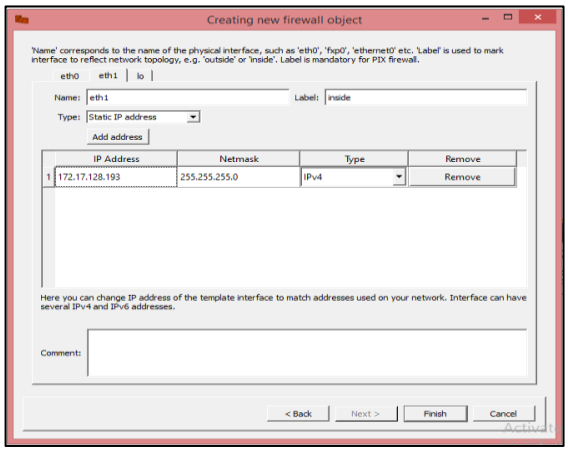


Figura 16. Create new objet Eth1
Elaborado por: Darwin Jiménez y Marcelo Osorio

La consola de administración permite manejar gráficamente la generación y administración de políticas de acceso.

Panel principal

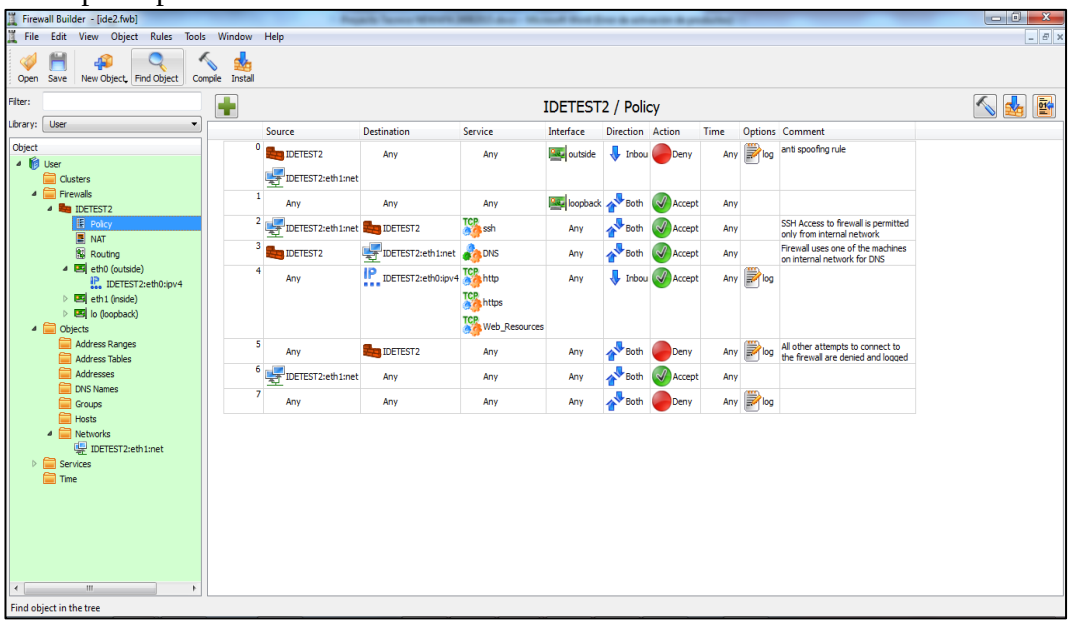


Figura 17. Panel principal de FwBuilder
Elaborado por: Darwin Jiménez y Marcelo Osorio

Las secciones de la ventana principal son los siguientes:

- **Menú y barras de herramientas.** Se encuentra en parte superior de la ventana, permite ejecutar procesos básicos de administración como son: abrir, guardar, atrás, adelante, nuevos objetos, buscar, compilar, instalar, etc.
- **El árbol de objetos.** Se muestra en la parte izquierda de la ventana, las pantallas de los árboles objeto cortafuegos, anfitriones, interfaces, servicios y otros "objetos" que va a utilizar al crear políticas de firewall.
- **El área de política.** Contiene el conjunto de reglas que está trabajando actualmente y se muestra a la derecha del árbol de objetos.
- **Editor de objetos, vistas parciales.** Realice las operaciones de buscar y reemplazar, y permite ver la salida de la regla solo compiladas.
- **Buscar y reemplazar diálogo objeto, vistas parciales.** Permite realizar búsquedas de objetos y gobernar conjuntos a través de sus archivos de objetos, además de hacer los reemplazos de los objetos
- **Salida vista, vista parcial.** Permite visualizar la compilación de las reglas y ver el estado de la conversión de la instrucción de firewall.
- **Deshacer pila.** Deshacer acción, es decir, deshace todos los cambios después de esa acción seleccionada.

Para la configuración las políticas del firewall FWIDE, se selecciona el objeto de Policy, que presenta las reglas predefinidas que pueden ser modificadas o anexas más políticas al objeto firewall FWIDE dependiendo adaptarse a la necesidad del ambiente.

Lista de objetos GUI FwBuilder

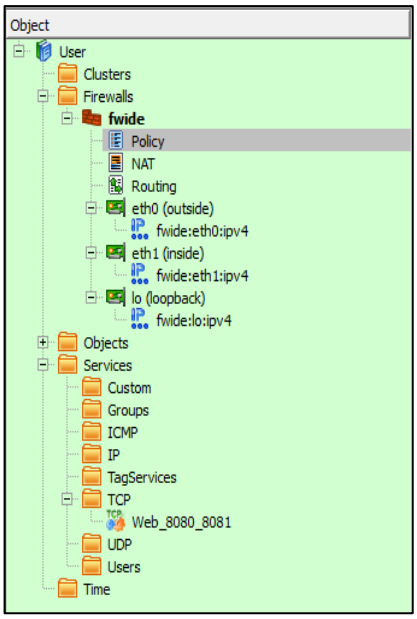


Figura 18. Listado de objetos FwBuilder
Elaborado por: Darwin Jiménez y Marcelo Osorio

CAPITULO 4

RESULTADOS

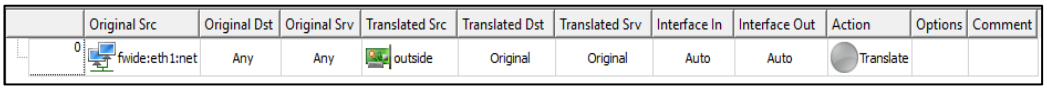
Luego de una exhaustiva revisión mediante las herramientas propuestas en el análisis, se han obtenido los siguientes resultados:

El listado de políticas de firewall, puede hacer uso de los objetos disponibles y comenzar a construir nuevas reglas de seguridad, routing y NAT.

3.1 Reglas de NAT (Network Address Translation)

Esta regla encapsula el tráfico para que desde el exterior sea la ip pública la que transacciones y gestione todo el tráfico interno.

NAT



	Original Src	Original Dst	Original Srv	Translated Src	Translated Dst	Translated Srv	Interface In	Interface Out	Action	Options	Comment
0	fwide:eth1:net	Any	Any	outside	Original	Original	Auto	Auto	Translate		

Figura 19. Regla de nateo
Elaborado por: Darwin Jiménez y Marcelo Osorio

Regla 0 NAT

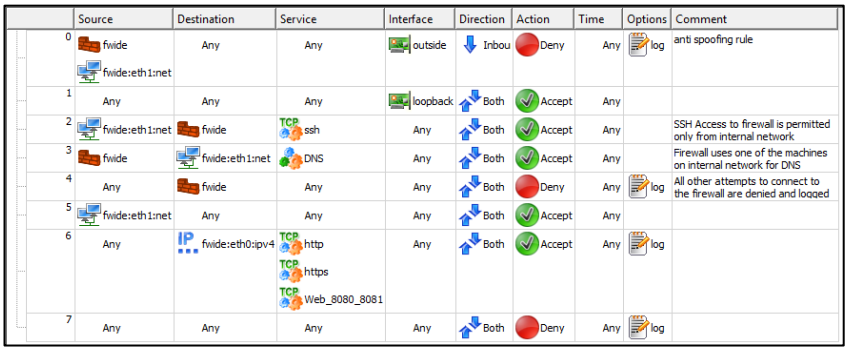
Esta regla NAT trasfiere todo el tráfico interno por la IP pública del equipo

3.2 Reglas de firewall (Policy)

La utilización del componente dashboard de firewall de la herramienta FWbuilder es potente dentro de la administración de seguridad, este es capaz generar configuraciones avanzadas las políticas basadas en objetos a través de la interfaz

gráfica, dando como resultado la generación del script que contiene las políticas que serán instaladas en el servidor a proteger, estas pueden ser implementadas directamente si necesidad de conocer su código interno, agregando las credenciales ssh a la herramienta y esta al instalar la política de seguridad se conectara automáticamente al equipo a ser configurado y aplicara el esquema de seguridad definido.

Dashboard de firewall – Reglas



	Source	Destination	Service	Interface	Direction	Action	Time	Options	Comment
0	fwide fwide:eth1:net	Any	Any	outsiou	Inbou	Deny	Any	log	anti spoofing rule
1	Any	Any	Any	loopback	Both	Accept	Any		
2	fwide:eth1:net	fwide	ssh	Any	Both	Accept	Any		SSH Access to firewall is permitted only from internal network
3	fwide	fwide:eth1:net	DNS	Any	Both	Accept	Any		Firewall uses one of the machines on internal network for DNS
4	Any	fwide	Any	Any	Both	Deny	Any	log	All other attempts to connect to the firewall are denied and logged
5	fwide:eth1:net	Any	Any	Any	Both	Accept	Any		
6	Any	fwide:eth0:ipv4	http https Web_8080_8081	Any	Both	Accept	Any	log	
7	Any	Any	Any	Any	Both	Deny	Any	log	

Figura 20. Reglas de firewall
Elaborado por: Darwin Jiménez y Marcelo Osorio

A continuación, se detalla brevemente las reglas generadas con la interface gráfica:

- Rule 0 – Anti Spoofing

  Regla de Anti Spoofing, previene que trafico externo emule una IP interna o de DMZ autorizada.

- Rule 1 – Loopback

  Permite que el tráfico interno del servidor circule libremente

- Rule 2 - Admin ssh

Permite la administración desde la red interna al protocolo tcp ssh

- Rule 3 – DNS

  Permite al firewall consultar a la red interna Resolución de Nombres DNS

- Red 4 – Acceso externo a servidor web de FWIDE

  Esta regla permite que desde cualquier origen externo alcanzar los servicios autorizados en el puerto 80, 443, 8080, 8081.

- Rule 5 – Sthealt

  Regla saludable que bloquea cualquier intento de conexión de protocolos no explícitamente permitidos hacia el objeto firewall

- Regla 6 – Acceso interno

  Permite llegar desde la red interna a través del NAT alcanzar cualquier puerto e IP desde el origen interno al destino externo

- Red 7 – Drop Total

  Esta regla bloquea y loguea toda actividad no explícitamente permitida.

Las reglas mencionadas anteriormente serán tratadas a de detalle en el punto 4.1.3 con el nombre Scripting FW Builder para cada uno de los servidores que forman parte de este estudio.

3.3 Scripting FW Builder

FWbuilder es un software muy potente dentro de la administración de firewall, este es capaz mediante las configuraciones realizadas a través de la interfaz gráfica definir políticas de seguridad robustas.

Todos los scripts fueron desarrollados en base al análisis de la información proporcionada por el administrador de la plataforma y generado de forma automática por el software FwBuilder, determinando los puertos y accesos requeridos para el funcionamiento de las plataformas de producción implementadas en cada servidor, cada regla permite o deniega el trafico explícitamente configurado en base a la política de seguridad definida.

A continuación se detalla con comentarios el código que entrega la herramienta de seguridad de Firewall, en los 3 Servidores que son el objeto de estudio de este documento.

3.3.1 Script servidor ide.ups.edu.ec

```
#Ide.ups.edu.ec / Policy / rule 0

# Anti spoofing rule evita la suplantación de ips de la red LAN
atreves de la red WAN.

# Define variable para agregar varias cadenas de filtrado.

$IPTABLES -N In_RULE_0$IPTABLES -A INPUT -i eth0 -s
172.17.128.193 -j In_RULE_0

#Se agrega en el perfil de ingreso la interface Eth0 con la ip
172.17.128.193(LAN)

$IPTABLES -A INPUT -i eth0 -s 190.15.136.3 -j In_RULE_0

#Se agrega  en el perfil de ingreso la interface Eth0 con la ip
190.15.136.3 (WAN estática)

$IPTABLES -A INPUT -i eth0 -s 172.17.128.0/24 -j In_RULE_0

#Se agrega  en el perfil de ingreso la interface Eth0 con la ip
172.17.128.0/24  (LAN)

$IPTABLES -A FORWARD -i eth0 -s 172.17.128.193 -j In_RULE_0

#Se agrega en el perfil de re-envío la interface Eth0 con la ip
172.17.128.193(LAN)

$IPTABLES -A FORWARD -i eth0 -s 190.15.136.3 -j In_RULE_0

#Se agrega  en el perfil de re-envío la interface Eth0 con la ip
190.15.136.3 (WAN estática)

$IPTABLES -A FORWARD -i eth0 -s 172.17.128.0/24 -j In_RULE_0

#Se agrega  en el perfil de re-envío la interface Eth0 con la ip
172.17.128.0/24  (LAN)

$IPTABLES -A In_RULE_0 -j LOG --log-level info --log-prefix "RULE
0 -- DENY”

#Agrega el evento al log del Sistema operativo la cadena de texto
“Rule 0--Deny” en modo informativo

$IPTABLES -A In_RULE_0 -j DROP


#Bloque el tráfico que cumpla con las condiciones anteriores
```

```
#Ide.ups.edu.ec/ Policy / rule 1

$IPTABLES -A INPUT -i lo -m state --state NEW -j ACCEPT

$IPTABLES -A OUTPUT -o lo -m state --state NEW -j ACCEPT

#Permite todo el tráfico generado de la entrada y la salida por
la interface local host
```

```
#Ide.ups.edu.ec / Policy / rule 2

$IPTABLES -A INPUT -p tcp -m tcp -s 172.17.142.0/24 --dport 22 -m
state -- NEW -j ACCEPT

# El acceso por el puerto 22 con servicio ssh desde la red
interna (LAN)
```

```
#Ide.ups.edu.ec / Policy / rule 3

$IPTABLES -A OUTPUT -p tcp -m tcp -d 172.17.142.0/24 --dport 53 -
m state --state NEW -j ACCEPT

$IPTABLES -A OUTPUT -p udp -m udp -d 172.17.142.0/24 --dport 53 -
m state --state NEW -j ACCEPT

# Permite el ingreso al servidor DNS en la red interna por el
Puerto 53 y con los protocolos  tcp y udp
```

```
#Ide.ups.edu.ec / Policy / rule 4

$IPTABLES -N In_RULE_4

# Define variable para agregar cadenas de filtrado.

$IPTABLES -A INPUT -p tcp -m tcp -d 190.15.136.3 --dport
8080:8081 -m state --state NEW -j In_RULE_4

$IPTABLES -A INPUT -p tcp -m tcp -m multiport -d 190.15.136.3 --
dports 80,443 -m state --state NEW -j In_RULE_4

# Permite el ingreso desde la ip publica (190.15.136.3) mediante
a los puertos 80,443, 8080:8081 por el protocolo tcp

$IPTABLES -A In_RULE_4 -j LOG --log-level info --log-prefix "RULE
4 -- ACCEPT"

#Agrega el evento al log del Sistema operativo la cadena de texto

"Rule 4--ACCEPT" en modo informativo


$IPTABLES -A In_RULE_4 -j ACCEPT


# Cumple con las condiciones de la regla In Rule 4 se acepta
```

```
#Ide.ups.edu.ec / Policy / rule 5

$IPTABLES -N RULE_5

# Define variable para agregar cadenas de filtrado.

$IPTABLES -A OUTPUT -d 172.17.128.193 -j RULE_5

$IPTABLES -A OUTPUT -d 190.15.136.3 -j RULE_5

$IPTABLES -A INPUT -j RULE_5

$IPTABLES -A RULE_5 -j LOG --log-level info --log-prefix "RULE 5
-- DENY”

# Bloque todas las conexiones que vengan desde la red interna
(LAN) e externa (WAN) al Firewall

$IPTABLES -A RULE_5 -j DROP

#Bloque el tráfico que cumpla con las condiciones anteriores
```

```
#Ide.ups.edu.ec / Policy / rule 6

$IPTABLES -A INPUT -s 172.17.142.0/24 -m state --state NEW -j
ACCEPT

$IPTABLES -A OUTPUT -s 172.17.142.0/24 -m state --state NEW -j
ACCEPT

$IPTABLES -A FORWARD -s 172.17.142.0/24 -m state -- NEW -j ACCEPT

# Permite llegar desde la red interna a través del NAT alcanzar
cualquier puerto e IP desde el origen interno al destino externo
```

3.3.2 Script servidor ide3.ups.edu.ec

```
#Ide3.ups.edu.ec / Policy / rule 0

# Anti spoofing rule evita la suplantación de ips de la red LAN
atreves de la red WAN.

$IPTABLES -N In_RULE_0

# Define variable para agregar varias cadenas de filtrado.

$IPTABLES -A INPUT -i eth0 -s 172.17.128.196 -j In_RULE_0

#Se agrega en el perfil de ingreso la interface Eth0 con la ip
172.17.128.196(LAN)

$IPTABLES -A INPUT -i eth0 -s 190.15.136.4 -j In_RULE_0

#Se agrega en el perfil de ingreso la interface Eth0 con la ip
190.15.136.4 (WAN estática)

$IPTABLES -A INPUT -i eth0 -s 172.17.142.0/24 -j In_RULE_0

#Se agrega en el perfil de ingreso la interface Eth0 con la ip
172.17.128.0/24 (LAN)

$IPTABLES -A FORWARD -i eth0 -s 172.17.128.196 -j In_RULE_0

#Se agrega en el perfil de re-envío la interface Eth0 con la ip
172.17.128.196(LAN)

$IPTABLES -A FORWARD -i eth0 -s 190.15.136.4 -j In_RULE_0

#Se agrega en el perfil de re-envío la interface Eth0 con la ip

190.15.136.4 (WAN estática)

$IPTABLES -A FORWARD -i eth0 -s 172.17.142.0/24 -j In_RULE_0

#Se agrega en el perfil de re-envío la interface Eth0 con la ip

172.17.128.0/24 (LAN)

$IPTABLES -A In_RULE_0 -j LOG --log-level info --log-prefix "RULE

0 -- DENY”

#Agrega el evento al log del Sistema operativo la cadena de texto

“Rule 0--Deny” en modo informativo

$IPTABLES -A In_RULE_0 -j DROP

#Bloque el tráfico que cumpla con las condiciones anteriores
```

```
# ide3.ups.edu.ec / Policy / rule 1

$IPTABLES -A INPUT -i lo -m state --state NEW -j ACCEPT

$IPTABLES -A OUTPUT -o lo -m state --state NEW -j ACCEPT

#Permite todo el tráfico generado de la entrada y la salida por
la interface local host
```

```
#ide3.ups.edu.ec / Policy / rule 2

$IPTABLES -A INPUT -p tcp -m tcp -s 172.17.142.0/24 --dport 22 -m
state --state NEW -j ACCEPT

# El acceso por el puerto 22 con servicio ssh desde la red
interna (LAN)
```

```
#ide3.ups.edu.ec / Policy / rule 3

$IPTABLES -A OUTPUT -p tcp -m tcp -d 172.17.142.0/24 --dport 53 -
m state --state NEW -j ACCEPT

$IPTABLES -A OUTPUT -p udp -m udp -d 172.17.142.0/24 --dport 53 -
m state --state NEW -j ACCEPT

# Permite el ingreso al servidor DNS en la red interna por el
Puerto 53 y con los protocolos tcp y udp
```

```
#ide3.ups.edu.ec / Policy / rule 4

$IPTABLES -N In_RULE_4

# Define variable para agregar cadenas de filtrado.

$IPTABLES -A INPUT -p tcp -m tcp -d 190.15.136.4 --dport
8080:8081 -m state --state NEW -j In_RULE_4

$IPTABLES -A INPUT -p tcp -m tcp -m multiport -d 190.15.136.4 --
dports 80,443 -m state --state NEW -j In_RULE_4

# Permite el ingreso desde la ip publica (190.15.136.4) mediante
a los puertos 80,443,

8080:8081 por el protocolo tcp

$IPTABLES -A In_RULE_4 -j LOG --log-level info --log-prefix "RULE
4 -- ACCEPT”

#Agrega el evento al log del Sistema operativo la cadena de texto
“Rule 4--ACCEPT” en modo informativo

$IPTABLES -A In_RULE_4 -j ACCEPT

# Cumple con las condiciones de la regla In_Rule_4 se acepta
```

```
# ide3.ups.edu.ec / Policy / rule 5

$IPTABLES -N RULE_5

# Define variable para agregar cadenas de filtrado.

$IPTABLES -A OUTPUT -d 172.17.128.196 -j RULE_5

$IPTABLES -A OUTPUT -d 190.15.136.4 -j RULE_5

$IPTABLES -A INPUT -j RULE_5

$IPTABLES -A RULE_5 -j LOG --log-level info --log-prefix "RULE 5
-- DENY”

# Bloque todas las conexiones que vengan desde la red interna
(LAN) e externa (WAN) al Firewall

$IPTABLES -A RULE_5 -j DROP

#Bloque el tráfico que cumpla con las condiciones anteriores
```

```
# ide3.ups.edu.ec / Policy / rule 6

$IPTABLES -A INPUT -s 172.17.142.0/24 -m state --state NEW -j
ACCEPT

$IPTABLES -A OUTPUT -s 172.17.142.0/24 -m state --state NEW -j
ACCEPT

$IPTABLES -A FORWARD -s 172.17.142.0/24 -m state --state NEW -j
ACCEPT

# Permite llegar desde la red interna a través del NAT alcanzar
cualquier puerto e IP desde el origen interno al destino externo
```

```
# ide3.ups.edu.ec / Policy / rule 7

$IPTABLES -N RULE_7

# Define variable para agregar cadenas de filtrado.

$IPTABLES -A OUTPUT -j RULE_7

$IPTABLES -A INPUT -j RULE_7

$IPTABLES -A FORWARD -j RULE_7

$IPTABLES -A RULE_7 -j LOG --log-level info --log-prefix "RULE 7
-- DENY”

#Agrega el evento al log del Sistema operativo la cadena de texto
“Rule 7-ACCEPT” en modo informativo

$IPTABLES -A RULE_7 -j DROP

# Bloquea todas conexiones no configuradas explícitamente
```

3.3.3 Script servidor localhost.localdomain

```
#localhost.localdomain / Policy / rule 0

# Anti spoofing rule evita la suplantación de ips de la red LAN
atreves de la red WAN.

$IPTABLES -N In_RULE_0

# Define variable para agregar varias cadenas de filtrado.

$IPTABLES -A INPUT -i eth0 -s 172.17.128.197 -j In_RULE_0

#Se agrega en el perfil de ingreso la interface Eth0 con la ip
172.17.128.197(LAN)

$IPTABLES -A INPUT -i eth0 -s 190.15.136.10 -j In_RULE_0

#Se agrega en el perfil de ingreso la interface Eth0 con la ip
190.15.136.10 (WAN estática)

$IPTABLES -A INPUT -i eth0 -s 172.17.142.0/24 -j In_RULE_0

#Se agrega en el perfil de ingreso la interface Eth0 con la ip
172.17.128.0/24  (LAN)

$IPTABLES -A FORWARD -i eth0 -s 172.17.128.197 -j In_RULE_0

#Se agrega en el perfil de re-envío la interface Eth0 con la ip
172.17.128.197(LAN)

$IPTABLES -A FORWARD -i eth0 -s 190.15.136.10 -j In_RULE_0

#Se agrega en el perfil de re-envío la interface Eth0 con la ip
190.15.136.10 (WAN estática)

$IPTABLES -A FORWARD -i eth0 -s 172.17.142.0/24 -j In_RULE_0

#Se agrega en el perfil de re-envío la interface Eth0 con la ip
172.17.128.0/24 (LAN)

$IPTABLES -A In_RULE_0 -j LOG --log-level info --log-prefix "RULE
0 -- DENY”

#Agrega el evento al log del Sistema operativo la cadena de texto
“Rule 0--Deny” en modo informativo

$IPTABLES -A In_RULE_0 -j DROP

#Bloque el tráfico que cumpla con las condiciones anteriores
```

```
#localhost.localdomain/ Policy / rule 1

$IPTABLES -A INPUT -i lo -m state --state NEW -j ACCEPT

$IPTABLES -A OUTPUT -o lo -m state --state NEW -j ACCEPT

#Permite todo el tráfico generado de la entrada y la salida por
la interface local host
```

```
# localhost.localdomain / Policy / rule 2

$IPTABLES -A INPUT -p tcp -m tcp -s 172.17.142.0/24 --dport 22 -m
state --state NEW -j ACCEPT

# El acceso por el puerto 22 con servicio ssh desde la red
interna (LAN)
```

```
# localhost.localdomain / Policy / rule 3

$IPTABLES -A OUTPUT -p tcp -m tcp -d 172.17.142.0/24 --dport 53 -
m state --state NEW -j ACCEPT

$IPTABLES -A OUTPUT -p udp -m udp -d 172.17.142.0/24 --dport 53 -
m state --state NEW -j ACCEPT

# Permite el ingreso al servidor DNS en la red interna por el
Puerto 53 y con los protocolos tcp y udpla redes internas (LAN)
```

```
# localhost.localdomain / Policy / rule 4

$IPTABLES -N In_RULE_4

# Define variable para agregar cadenas de filtrado.

$IPTABLES -A INPUT -p tcp -m tcp -d 190.15.136.10 --dport
8080:8081 -m state --state NEW -j In_RULE_4

$IPTABLES -A INPUT -p tcp -m tcp -m multiport -d 190.15.136.10 --
dports 80,443 -m state --state NEW -j In_RULE_4

# Permite el ingreso desde la ip publica (190.15.136.10)
mediante  a los puertos 80,443, 8080:8081 por el protocolo tcp

$IPTABLES -A In_RULE_4 -j LOG --log-level info --log-prefix "RULE
4 -- ACCEPT"

#Agrega el evento al log del Sistema operativo la cadena de texto
"Rule 4--ACCEPT" en modo informativo

$IPTABLES -A In_RULE_4 -j ACCEPT

# Cumple con las condiciones de la regla In_Rule_4 se acepta
```

```
# localhost.localdomain / Policy / rule 5

$IPTABLES -N RULE_5

# Define variable para agregar cadenas de filtrado.

$IPTABLES -A OUTPUT -d 172.17.128.197 -j RULE_5

$IPTABLES -A OUTPUT -d 190.15.136.10 -j RULE_5

$IPTABLES -A INPUT -j RULE_5

$IPTABLES -A RULE_5 -j LOG --log-level info --log-prefix "RULE 5
-- DENY”

# Bloque todas las conexiones que vengan desde la red interna
(LAN) e externa (WAN) al Firewall

$IPTABLES -A RULE_5 -j DROP

#Bloque el tráfico que cumpla con las condiciones anteriores
```

```
# localhost.localdomain / Policy / rule 6

$IPTABLES -A INPUT -s 172.17.142.0/24 -m state --state NEW -j
ACCEPT

$IPTABLES -A OUTPUT -s 172.17.142.0/24 -m state --state NEW -j
ACCEPT

$IPTABLES -A FORWARD -s 172.17.142.0/24 -m state --state NEW -j
ACCEPT

# Permite llegar desde la red interna a través del NAT alcanzar
```

```
# localhost.localdomain / Policy / rule 7

$IPTABLES -N RULE_7

# Define variable para agregar cadenas de filtrado.

$IPTABLES -A OUTPUT -j RULE_7

$IPTABLES -A INPUT -j RULE_7

$IPTABLES -A FORWARD -j RULE_7

$IPTABLES -A RULE_7 -j LOG --log-level info --log-prefix "RULE 7
-- DENY”

#Agrega el evento al log del Sistema operativo la cadena de texto
“Rule 7-ACCEPT” en modo informativo

$IPTABLES -A RULE_7 -j DROP

# Bloquea todas conexiones no configuradas explícitamente
```

3.4 Políticas y procedimiento de seguridad para IDE-IA-GEOCA

3.4.1 Introducción

La seguridad y la administración de sistemas requieren mantener un esquema organizado y para esto se han diseñado las siguientes normas básicas, que debe tomando en cuenta para todos los proyectos cargados a los sistemas de la organización, esto tiene como objetivo estandarizar la organización de la información, seguridad y administración de la plataforma.

3.4.2 Responsables

Se debe definir un responsable de la seguridad de la información, que se encargue de consensuar, desarrollar, divulgar y ejecutar las políticas de seguridad a los usuarios de la infraestructura informática de IDE-IA-GEOCA. En este estudio se determina que el

administrador de seguridades será el responsable de definir las políticas de seguridad y de la administración de la misma, que debe ser congruente con las plataformas implementadas y a su vez, periódicamente debe ser auditado por el administrador de sistema y el ingeniero de proyectos.

El criterio para designar a un administrador de seguridad, debe ser seleccionando a un profesional con un perfil de certificaciones de Ethical Hacking, Infraestructura, ISO27001, etc. y experiencia en seguridad informática comprobable.

3.4.3 Definición

En esta parte se plantea la creación de políticas de seguridad como un recurso de mitigación a los riesgos y amenazas a las que se ve expuesta la infraestructura informática de IDE-IA-GEOCA.

3.4.4 Organización

La toma de decisiones requiere de un Comité que se conformará por los siguientes colaboradores:

- Administrador de Sistemas
- Administrador de Seguridades
- Ingeniero de Proyecto

Para el estudio de factibilidad de los proyectos se tomará en cuenta los siguientes factores:

- Estudio Técnico
- Vigencia Tecnológica
- Estándares de Desarrollo e implementación
- Margen de Crecimiento.

Una vez realizado los estudios técnicos el comité será responsable de emitir periódicamente una lista de software base vigente aplicable para la ejecución y desarrollo de nuevos proyectos.

Para el desarrollo se considerarán los siguientes ítems:

- Plataforma de Sistema Operativo
- Base de Datos
- Lenguaje de Programación
- Utilitarios
- Navegadores
- Servicios y Plugins

3.4.5 Confidencialidad

El personal designado para el desarrollo y administración del proyecto, no podrá divulgar en su total o parcial de la información, que se considere como confidencial para el grupo IDE-IA-GEOCA.

3.4.6 Versionamiento

Para los proyectos deberá considerarse el uso de los últimos reléase estables, de cada uno de los ítems mencionados anteriormente, con el uso de documentación oficial y acorde a las mejores prácticas de cada producto.

3.4.7 Licenciamiento

Todo software implementado deberá contar con el licenciamiento vigente a partir de implementación y contar con las garantías necesarias para su funcionamiento, por lo que se hará énfasis en la regularización y/o eliminación de los productos que ya se encuentre actualmente en la infraestructura y no cuente con su debido licenciamiento.

Todo desarrollo deberá llevar una etapa de pruebas de compatibilidad para adaptarse a la plataforma vigente disponible, para la implementación.

3.4.8 Cambios organización/infraestructura

Si la organización se encuentra reestructurando sus procesos, sistemas y/o infraestructura se debe mantener un margen de al menos 2 meses mientras se estabilizan los cambios y se hayan realizado las correcciones necesarias, una vez realzado y de no existir errores sobre los mismos se puede empezar a implementar nuevo proyecto de desarrollo.

3.4.9 Políticas

Dentro del Centro de Investigación IDE-IA-GEOCA se requiere plantear políticas para la toma de decisiones, para que se exprese claramente el objetivo de aseguramiento de la infraestructura y definición de funciones, con la intención de resolver y minimizar riesgos asociados en la seguridad de la infraestructura.

3.4.9.1 Políticas del ambiente de desarrollo

Art. 1.1 La etapa de desarrollo requiere un análisis de factibilidad, detallando las ventajas y beneficios que tendrá la generación del proyecto, este marcará la pauta para la generación del producto final.

Art. 1.2 Todo desarrollo deberá tomar los lineamentos entregados por el comité, respetando cada uno de ellos.

Art. 1.3 Los usuarios que desarrollen sobre la plataforma deberán entregar al Comité:

- Código Fuente
- Ejecutables
- Manual Técnico Desarrollo / Instalación
- Manual de Administración

Art. 1.4 Por ninguna causa se deberá empezar la etapa de desarrollo del proyecto, sin antes haber concluido la etapa de análisis y diseño.

Art. 1.5 La fase de análisis y diseño de proyecto deberá alinearse a la metodología que el comité disponga pertinente para la implementación del proyecto.

Art. 1.6 En caso de que se realice cambios al diseño del proyecto de desarrollo, el mismo debe ser documentado y con autorización, revisión, aprobación del comité, elaborando el respectivo documento de control de cambios.

3.4.9.2 Políticas del ambiente de pruebas

Art. 2.1 Una vez que el proyecto termina su fase desarrollo, pasará a la fase de pruebas, en la cual recibirá la certificación de uso de parte de los usuarios que recibirán la plataforma.

Art. 2.2 Antes de que el proyecto se pase ambiente de producción, es necesario realizar las pruebas pertinentes con datos reales.

Art. 2.3 Cuando se realice actualización del proyecto, es necesario que se precise un tiempo en el cual el proyecto nuevo y viejo se encuentre en funcionamiento, permitiendo buscar errores y optimizaciones.

3.4.9.3 Políticas del ambiente de producción

Art. 3.1 Para iniciar la etapa de producción todas las bases de datos deben ser depuradas y contener la información base de funcionamiento, más no datos realizados en ambiente de pruebas, todos los usuarios genéricos referentes a base de datos, sistemas u otros deben ser retirados y mantener privilegios sobre los usuarios de administración.

Art 3.2 El sistema en producción contara con el estándar de base de datos, capa media, versión y calidad de los ambientes de prueba, con el hardening de cada uno de los

elementos, esto quiere decir que deben retirarse configuraciones por defecto y asegurarlas para su uso.

Art 3.3 Garantizar los recursos indispensables para la ejecución en ambiente productivo

Art 3.4 Deben estar aislado los sistemas de test de los de producción

Arr 3.5 La plataforma debe mantenerse en constante actualización y la memoria técnica documentada y disponible para futuras referencias.

3.4.9.4 Políticas ambiente de administración

Art 4.1 Las etapas de seguridad, para su acceso deben tener un responsable asignado y evidenciar por software su ingreso.

Art. 4.2 El administrador es el encargado de asignar las funciones al usuario en el sistema, donde se determinará el mejor perfile que se ajusta al usuario para desarrollar sus actividades asignadas.

Art. 4.3 El administrador del servicio, poseerá el acceso al módulo de su configuración de su aplicativo que se encuentra a cargo.

Art. 4.4 Es obligatorio que el administrador de los sistemas informáticos vigile el correcto uso de los proyectos implementados.

Art. 4.5 Todos los usuarios que tengan asignada el acceso al proyecto de sistemas, dispondrán credencial única, identificado por un usuario y contraseña.

Art. 4.6 Los usuarios tendrán accesos a la información, conforme a sus funciones asignadas dentro de IDE-IA GEOCA.

Art. 4.7 La contraseña de acceso para el usuario tendrá una longitud mínima de ocho caracteres, donde estará compuesto por caracteres alfabéticos, numéricos y especiales.

Art. 4.8 El usuario debe cambiar la contraseña como mínimo una vez cada 3 meses, evitando infiltraciones de personas no deseadas mediante el usuario.

Art. 4.9 Los datos del proyecto información deben ser respaldados de acuerdo a la periodicidad de la actualización de sus datos y guardando los respaldos históricos periódicamente.

Art. 4.10 Se deben establecer procedimientos periódicos de auditoria a la integridad de los datos y proyectos informáticos, para garantizar su integridad.

Art. 4.11 Se monitoreará continuamente la operatividad de los registros de Logs, para detectar actividad sospechosa, además de generar el reporte de la herramienta OpenVas para detectar nuevas amenazas sobre los sistemas y proyectos implementados.

Art. 4.12 Se generará y mantendrá actualizada una bitácora completa, donde se encuentren registradas las ediciones, versiones y actualización del software por cada sistema instalado.

Art. 4.13 Dentro de las instalaciones de IDE-IA-GEOCA, habrá un equipo dedicado única y exclusivamente para el acceso remoto a los sistemas que contiene los servidores, la cual se mantiene con privilegios mediante por políticas de seguridades implementadas y asignadas a dicho equipo.

Art 4.14 Si se detecta amenazas y/o vulnerabilidades en un proyecto que pueda comprometer la integridad de la infraestructura, el administrador está en la potestad de aislar o dar de baja al proyecto mientras se mitiga la amenaza o se suprime la misma.

3.4.9.5 Políticas de seguridad perimetral

Art. 5.1 La seguridad perimetral será controlada a través de un firewall quien será el filtro de conexiones entrantes y salientes de la red, siendo capaz de discriminar puertos e IPs.

Art 5.2 Todas las conexiones no autorizadas deben estar restringidas, mediante es estándar normalmente cerrado.

Art 5.3 Definir la regla de Antispoofing, evitando accesos no autorizados falsificando IPs.

Art 5.4 Establecer los protocolos/puertos a ser publicado a nivel de internet.

Art 5.5 Definir la regla de administración, donde los hosts autorizados a realizar cambios sobre el equipo firewall sean los únicos con acceso a los mismos.

Art 5.6 Definir la regla saludable (stealth) que define el bloqueo todo tráfico desde cualquier interfaz o red directamente hacia el firewall

Art 5.7 Únicamente se concederá acceso a los protocolos, redes e IPs. necesarias para la operatividad de los proyectos implementados.

Art 5.8 Se definirá al final de toda la configuración la regla de bloqueo global, que boqueará todo el tráfico no explícitamente indicado.

3.4.9.6 Frecuencia de evaluación de las políticas

Se evaluará y revisará las políticas del presente documento, con frecuencia de un año, a cargo del comité.

3.4.9.7 Proceso de análisis de seguridad

El proceso de análisis de seguridad informática es un entorno complejo que se compone de varios disparadores dentro de ellos tenemos a:

- Amenazas posibles
- Consecuencias
- Ambiente
- Mecanismos
- Factor Humano

Todos ellos pueden generar riesgos para un sistema o red, es necesario contar con:

- Plan de Seguridad
- Plan de acción
- Políticas y procedimientos

Todos ellos obligatoriamente deben ser auditados, controlados y evidenciado mediante un informe y mitigación final.

Flujo del proceso de seguridad

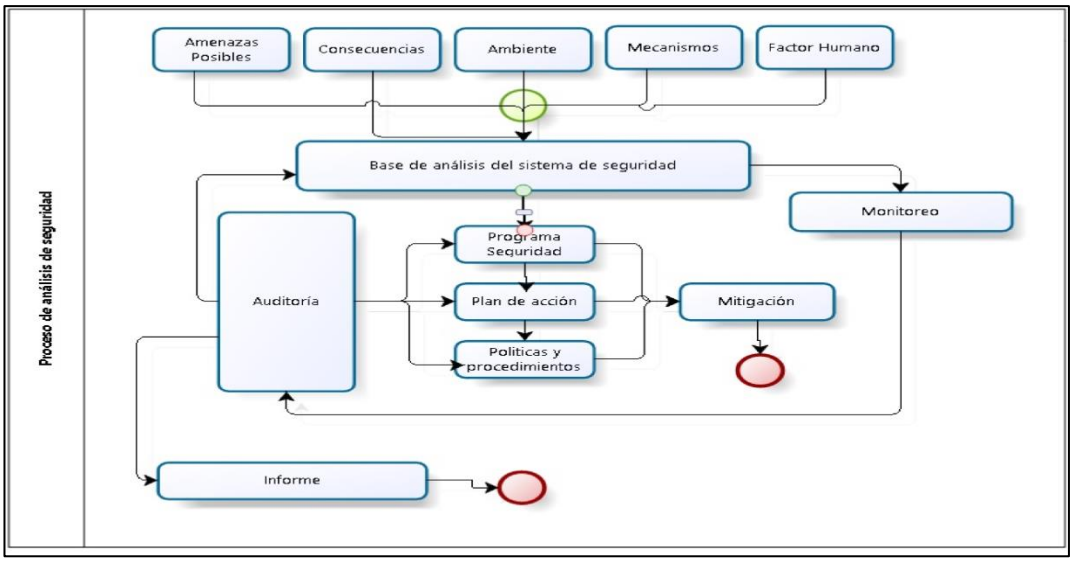


Figura. 21. Proceso de análisis de seguridad
Elaborado por: Darwin Jiménez y Marcelo Osorio

3.4.10 Manual de implementación de nuevos proyectos

El presente manual está enfocado en la seguridad y en los requerimientos necesarios para la implementación de nuevos proyectos sobre la infraestructura de grupo IDE-IA-GEOCA.

3.4.10.1 Solicitud de recursos

Luego de culminar el desarrollo es necesario solicitar formalmente la asignación de recursos y la coordinación de implementación en la infraestructura, esta solicitud será entregada al comité de IDE-IA-GEOCA contemplando la siguiente información:

- Tema del proyecto
- Sinopsis del proyecto desarrollado

- Características del hardware y software requerido
- Documento de tutor del proyecto, certificando que el proyecto es apto para el paso a producción

Como respuesta a esta solicitud se emite un certificado de aceptación para la implementación del proyecto, representada en el Anexo 1.

3.4.10.2 Formato de información de detalles técnicos:

Una vez aprobado por el comité la entrega de recursos, el interesado deberá llenar el formulario de información técnica, donde incluirá el detalle de configuración requerida para la puesta en marcha se su aplicación, Una vez revisado y aprobado por el comité del Grupo IDE-IA-GEOCA, este emitirá una fecha de implementación de proyecto, asignado un responsable para suministrar los recursos necesarios y generar la evaluación de puesta en producción, representada en el Anexo 2

3.4.10.3 Implementación

El tesista en conjunto con el administrador designado, procederá a cargar el proyecto en los recursos de infraestructura, bajo las normas establecidas en el capítulo "Procedimientos" del presente documento, cumpliendo todo lo mencionado en el formato de solicitud y el formato de detalles técnicos, con el objetivo de asegurar la calidad y cumplimiento de todo lo expresado. De esta forma se requiere que el tesistas entregue toda la información relacionada al proyecto bien documentada, para que sirva como referencia futura a continuación se listara todos los anexos que se deberán entregar:

- Manual de instalación, Operación y mantenimiento (backup, vaciado de logs)
- Manual de Usuario
- Código fuente y ejecutables
- Estructura de la base de datos

3.4.10.4 Pruebas

Una vez terminada la implementación se procede a validar que la operación del software cargado en la infraestructura sea estable y cumpla con todas las normas establecidas, esto certifica el responsable designado por el grupo IDE-IA-GEOCA, se entregará los siguientes resultados dentro del informe de pruebas:

1. Estudio de carga (Concurrencia de usuarios, ancho de banda, capacidad de disco)

El estudio de carga se debe realizar con herramientas especializadas, online y locales algunas de ellas son:

- Loadstorm.com
- NeoLoad
- Webserver Stress Tool

Se deberá seleccionar una de ellas en función del proyecto implementado, el estudio de capacidad de disco debe realizarse en función de los datos que almacene la información.

2. Pruebas de seguridad perimetral y vulnerabilidad de la plataforma.

- OpenVas es la herramienta efectiva para tener visibilidad de las amenazas de la plataforma

CONCLUSIONES

Las conclusiones que a continuación se describen, están enfocadas a contribuir nuevas aportaciones en beneficio de Seguridades de la información del grupo IDE-IA-GEOCA.

El resultado del estudio realizado demuestra que, en la actualidad la estrategia de administración de la infraestructura tecnológica del grupo IDE-IA-GEOCA, no es suficiente para salvaguardar la información, por lo que se está comprometiendo la integridad de los proyectos, en los análisis realizados detecta que en promedio se tiene un riesgo con el estándar CVSS del 43% para las vulnerabilidades Altas en el segmento WAN y un 60% en el análisis en el segmento LAN.

El análisis de vulnerabilidades, para los servidores del grupo IDE-IA-GEOCA concluye que, los riesgos más altos que se han identificado son los ataques de fuerza bruta al protocolo SSH2, ejecución de exploits a la base de datos Mysql al puerto 3306 desde ips no autorizadas y SSL Poodle que permitiría capturar la información transmitida mediante el protocolo https

Mediante el análisis realizado en referencia a las tablas 5, 7, 8 en la sección Vulnerabilidades Altas, se determina que los servidores del grupo IDE-IA-GEOCA, son constantemente analizados desde internet, en busca de protocolos y aplicaciones vulnerables, tratando de obtener las credenciales de root, desde ips no autorizadas que en su gran mayoría provienen desde el continente asiático de países como Hong Kong, China y Japón.

En el proceso de análisis se detectaron amenazas como el SSL Poodle en los 3 servidores, adicional a la información recopilada por las herramienta OpenVas, la Red Cedia notificó (Anexo 3) a los administradores de la infraestructura, que debe ser corregido el problema de seguridad; para lo cual se procedió a parchar los sistemas, una vez parchado los mismos, se concluye que los protocolos obsoletos usados para las comunicaciones seguras pueden ser susceptibles a fallos como en este caso la comunicación de SSL v1 y SSL v2 dejando como única opción de comunicación segura SSL v3 con algoritmos de encriptación SHA-256.

La implementación de los scripts con las reglas de seguridad, las políticas y procedimientos, permitió fortalecer la seguridad de la información del grupo IDE-IA-GEOCA, ya que al bloquear el acceso al 90% de los puertos publicados en principio, se mitiga las amenazas potenciales, dando un margen del 10% de posibles vulnerabilidades sobre los protocolos de servicios publicados para la operatividad de las plataformas.

La membresía que tiene el grupo IDE-IA-GEOCA mediante la Universidad Politécnica Salesiana, con la organización RED CEDIA (Red Nacional de Investigación y Educación del Ecuador) es de suma utilidad para identificar ataques externos, a la infraestructura del grupo, dado que son un ente que permanentemente ejecuta análisis y emite alertas de seguridad. (Véase, en: 1.5.1 Red Cedia - CSIRT y el Anexo 3)

RECOMENDACIONES

Debido a los problemas encontrados dentro del análisis de vulnerabilidades, se recomienda la implantación de equipos de monitoreo y la ejecución periódica de una herramienta que analice vulnerabilidades, esto permitirá garantizar la seguridad informática en la infraestructura del grupo IDE-IA-GEOCA.

Concientizar a los usuarios y administradores de las diferentes amenazas y buenas prácticas relacionadas a la seguridad de la información. Generando una cultura de seguridad en el manejo y protección de sus proyectos implementados en infraestructura del grupo IDE-IA-GEOCA.

Se recomienda aislar la red del Grupo IDE-IA-GEOCA con un firewall dedicado donde se gestione las políticas de seguridad de manera independiente, esto generaría autonomía y visibilidad de las amenazas potenciales y mejores tiempos de respuesta ante incidentes de seguridad, además de la implementación de zonas de seguridad.

Realizar hardening periódico de los sistemas operativos y servicios implementados con el fin de cerrar vulnerabilidades potenciales que puedan afectar la seguridad de la infraestructura.

Establecer tiempos de vida de los proyectos implementados y en su defecto dar mantenimiento constante a los proyectos que se requieran mantener en producción.

Se sugiere que, en base a las políticas y procedimientos propuestos en este documento; el grupo genere las instancias necesarias y validaciones para la ejecución de las mismas.

Se recomienda la implementación de un SIEM (Security Information and Event Management) y un DAM (Database Activity Monitoring), que permita recolectar logs de todas las plataformas implementadas y a su vez genere la correlación de los eventos, a fin de generar proactividad en la administración y seguridad de los sistemas.

Enfocar las seguridades informáticas como una política del grupo de investigación, con mira a implementar un CSIRT (Computer Emergency Response Team), que ayude a la mitigación e investigación de las amenazas de seguridad de las redes de la Universidad, el país y el mundo.

REFERENCIAS

CEDIA. (s.f.). Obtenido de https://www.cedia.org.ec/

Checkpoint Software Tecnologies. (2009). *Checkpoint Security Administrator R70.* Tel Aviv, Israel: Checkpoint Press.

Cisco. (2005). *Network Security Fundamentals.* Indiana, US.

Herzog, P. (23 de 08 de 2003). *Isecom SecureNet.* Recuperado el 04 de 06 de 2015, de ISECOM: http://isecom.securenetltd.com/OSSTMM.es.2.1.pdf

IntelSecurity, M. (2014). *Informe sobre amenazas.* Madrid, España: Mcaffe Lab Intel Security.

Jimeno Garcia, M. T., Miguel Peréz, C., Matas García, A. M., & Perez Agudin, J. (2008). *Destripa la Red Hacking Practico.* España: ANAYA.

Lawrence C. Miller, C. (2014). *Cybersecurity for Dummies For Palo Alto Networks edition.* Hoboken, NJ: John Wiley & Son.

Mike Schiffman, G. E. (2004). *CVSS: A Common Vulnerability Scoring System.* National Infrastructure Advisory Council.

Mitnik, K. (10 de 2011). Campus Party. (Varios, Entrevistador)

RFC2196. (1997). Site Security Handbook.

US-CERT Vulnerability Note Field Descriptions. (s.f.). Obtenido de http://www.kb.cert.org/vuls/html/fieldhelp

Wilding, E. (2006). *Information Risk and Security: Preventing and Investigating Workplace Computer Crime.* Gower Publishing, Ltd.

ANEXOS

Anexo 1. Formato de detalles técnicos

UNIVERSIDAD POLITÉCNICA SALESIANA	FORMATO REGISTRO DE ACTIVIDADES	IDE-IA-GEOCA http://ide.ups.edu.ec

FECHA	día	mes	año

DATOS DEL PROYECTO

TEMA DEL PROYECTO:	
DIRECTOR DE PROYECTO:	
DESCRIPCION DEL PROYECTO / RESUMEN:	

DATOS DEL TESISTA 1

NOMBRE TESISTA:		CI:	
CORREO:		TELÉFONO:	
SKYPE:		TWITTER/FACEBOOK:	

DATOS DEL TESISTA 2

NOMBRE TESISTA:		CI:	
CORREO:		TELÉFONO:	
SKYPE:		TWITTER/FACEBOOK:	

ACTIVIDAD

☐ *Desarrollo de aplicación* | *Actualización de aplicación* | *Configuración de Arquitectura*

SERVICIOS UTILIZADOS

NOMBRE	VERSION	PUERTO	OBSERVACIONES

ARCHIVOS INSTALADOS

ARCHIVO	DESCRIPCION

ARCHIVOS MODIFICADOS

ARCHIVO	DESCRIPCION

ACCESO AL SISTEMA

URL	LAN / PUBLICO

OBSERVACIONES ADICIONALES

FIRMA TESISTAS	FIRMA TUTOR	FIRMA ADMINISTRADOR

Anexo 2. Formato solicitud de recursos

UNIVERSIDAD POLITÉCNICA SALESIANA	FORMATO DE SOLICITUD DE RECURSOS TECNOLÓGICOS	IDE-IA-GEOCA http://ide.ups.edu.ec

FECHA DE SOLICITUD	día	mes	año

DATOS DEL PROYECTO

TEMA DEL PROYECTO:	
DIRECTOR DE PROYECTO:	
DESCRIPCION DEL PROYECTO / RESUMEN:	

DATOS DEL TESISTA 1

NOMBRE TESISTA:		CI:
CORREO:		TELÉFONO:
SKYPE:		TWITTER/FACEBOOK:

DATOS DEL TESISTA 2

NOMBRE TESISTA:		CI:
CORREO:		TELÉFONO:
SKYPE:		TWITTER/FACEBOOK:

ACTIVIDAD

☐ *Desarrollo de aplicación* *Actulización de aplicación* *Configuración de arquitectura*

REQUERIMIENTOS

SISTEMA OPERATIVO:		VERSIÓN / KERNEL:

OBSERVACIONES / REQUERIMIENTOS ESPECIFICOS / SERVICIOS / SOFTWARE / ACCESO INTERNET O RED:

VIGENCIA DE SOLICITUD

INICIO DE ACTIVIDADES				FIN DE ACTIVIDADES		
día	mes	año		día	mes	año

_____ _____

FIRMAS TESISTAS

USO INTERNO DEL ADMINISTRADOR

☐ *APROBADO* *RECHAZADO* *APROBACION PARCIAL*

DATOS DE ACCESO

IP(S):		PASSWORD:
HOSTNAME(S)		SSH: TELNET: SCP: FTP: WEB:
USUARIO(S):		OTROS PUERTOS:

OBSERVACIONES / REQUERIMIENTOS ESPECIFICOS / SERVICIOS / SOFTWARE / ACCESO INTERNET O RED:

VIGENCIA DE ACCESO Y HORARIO DE INTERVENCIONES

INICIO DE ACTIVIDADES				FIN DE ACTIVIDADES		
día	mes	año		día	mes	año

DIAS Y HORAS DE ACCESO: _____

_____

FIRMA ADMINISTRADOR

Anexo 3. Notificación CSIRT (Computer Emergency Response Team) – CEDIA

Fwd: RV: [CSIRT-CEDIA] Reporte de ShadowServer: ssl_poodle en IP 190.15.136.4

De: csirt@cedia.org.ec <csirt@cedia.org.ec>
Enviado: martes, 18 de agosto de 2015 23:30
Para: Juan Carlos Dominguez Ayala; ramirew@gmail.com; Washington Arsenio Ramirez Montalvan
Cc: csirt@cedia.org.ec
Asunto: [CSIRT-CEDIA] Reporte de ShadowServer: ssl_poodle en IP 190.15.136.4

wramirez@ups.edu.ec,ramirew@gmail.com,jdominguez@ups.edu.ec
ssl_poodle - 190.15.136.4

La IP 190.15.136.4 ha sido reportada por ShadowServer con problemas relacionados con ssl_poodle.

Es imperioso que se revise la configuración de firewall y servicios en 190.15.136.4 y corrijan el problema reportado pues este puede ser utilizado para consumir ancho de banda, realizar ataques a terceros y/o cometer delitos.

Adjuntamos un escaneo de la IP y un resumen de la actividad detectada en 190.15.136.4, para obtener información del formato adjuntado, acceda al sitio de ShadowServer: http://www.shadowserver.org/wiki/pmwiki.php?n=Services/Reports y escoja el enlace relacionado con ssl_poodle.

Atentamente

Ing. Ernesto Pérez Estévez, MSc.
CSIRT - CEDIA
http://csirt.cedia.org.ec
+(593) 9 9924 6504