UNIVERSIDAD PÚBLICA DE EL ALTO
CARRERA INGENIERIA DE SISTEMAS

TESIS DE GRADO

MODELO DE SEGURIDAD PARA INFRAESTRUCTURAS DE INFORMACIÓN

CASO:" IKRIT.SRL"

PARA OPTAR AL TÍTULO DE LICENCIATURA EN INGENEIRIA DE SISTEMAS
MENCIÓN: INFORMÁTICA Y COMUNICACIONES

POSTULANTE **:** ALVARO CHAMIZO GUTIERREZ

TUTOR METODOLÓGICO **:** M.Sc. ING. ENRIQUE FLORES BALTAZAR

TUTOR ESPECIALISTA **:** LIC. FREDY ALANOCA COARETI

TUTOR REVISOR : LIC. KATYA MARICELA PEREZ MARTINEZ

EL ALTO - BOLIVIA

2020

DEDICATORIA

A Dios

Por haberme guiado en todo este camino que recorrí y cuidar a las personas que me rodean.

A mi Padre

Eusebio Chamizo Mamani, por cuidarme, guiarme, y por todas sus enseñanzas que me transmitió a través de este tiempo, y pues que estoy orgulloso de mi padre.

A mi Madre

Vicenta Gutiérrez Villca, por haberme dado todo el cariño, por todo su amor, comprensión, estar a mi lado en las buenas y malas no me alcanzaría la vida para agradecerte todo lo que haz echo por mí.

A mis Hermanos

Wilmer y Rosario, por apoyarme en todo a su alcance.

A mis Tíos

Wily Gutiérrez, Regina. Por haber estado a mi lado incondicionalmente, aconsejarme en muchas situaciones y haber sido como unos padres para mí.

Plantida Gutiérrez. Por guiarme en todo momento, aconsejarme y apoyarme incondicionalmente.

A mis Amigos y Compañeros

Por todos los momentos buenos malos pero juntos, por su ayuda y orientación en momentos de incertidumbre y duda. Por los días y las noches y sobre todo las amanecidas de estudio que pasamos juntos.

AGRADECIMIENTO

A mi Tutor Metodológico

M.Sc. Ing. Enrique Flores Baltazar, por haberme ayudado y orientado al principio, por su guía para ayudarme a elegir el área del presente trabajo y gracias por todas las apreciaciones posteriores para mejorar este. En este camino hacia el final, su tiempo para revisar este. Por cada corrección y observación que me dio para lograr terminar mi tesis de grado.

A mi Tutor Especialista

Lic. Freddy Alanoca Coareti. muchas gracias por brindarme su apoyo incondicional en el transcurso de esta presente tesis y solo me queda agradecerle por todas las enseñanzas en el transcurso de esta tesis y los conocimientos brindados.

A mi Tutor Revisor

Lic. Katya Maricela Pérez Martínez muchas gracias por haberme ayudado en la redacción de esta tesis de grado, por cada observación que se me dio, por todo su tiempo con su paciencia, atención y guía en cuanto al desarrollo del presente trabajo de investigación.

A mi enamorada

Por brindarme su apoyo incondicional.

A mis compañeros

Por ayudarme con en la elección del tema y su orientación sobre las diferentes utilidades de la tecnología escogida.

A mis Docentes

Gracias por todo el conocimiento transmitido a mi persona y la paciencia para haberme enseñado todo lo que se.

Resumen

El avance de la tecnología es demasiado rápido ya que es poco habitual seguir el ritmo de la tecnología porque avanza a pasos agigantados y es un gran beneficio para toda la humanidad con este beneficio viene consecuencias negativas para nuestros datos personales y/o empresariales ya que podemos estar expuestos a robo de información personal como también robo de información de las instituciones, como también sufrir variedad de ataques, suplantación de servicios, entre otros por este motivo es fundamental tener una aplicación que busque las vulnerabilidades que existiera en su servidor así tratar de evitar futuros ataques que pueden pasar. Para esto utilizaremos distintas herramientas para la búsqueda de las vulnerabilidades que pudiera existir en un servidor.

Palabras clave: Vulnerabilidad, Búsqueda, UWE, Linux.

Summary

The advancement of technology is too fast since it is unusual to keep up with technology because it advances by leaps and bounds and it is a great benefit for all of humanity. With this benefit comes negative consequences for our personal data and / or entrepreneurs, since we can Being affected by theft of personal information as well as theft of information from institutions, as well as suffering a variety of attacks, impersonation of services, among others, for this reason it is essential to have an application that searches for vulnerabilities that exist on your server, so try to avoid future attacks that may happen. For this we will use different tools to search for vulnerabilities that could exist on a server.

Key words: Vulnerability, Search, UWE, Linux.

ÍNDICE

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

CAPITULO I

MARCO PRELIMINAR

1.1 INTRODUCCIÓN

Según (Ramos, 2011) indica que “En los últimos años, debido al incremento del uso de las computadoras y el espectacular crecimiento del internet y de los servicios que este ofrece, la detección de intrusos se ha convertido en una prioridad importante, ya que no resulta técnicamente factible construir un sistema invulnerable, pues a pesar de la existencia de numerosas medidas de seguridad para proteger los recursos informáticos de cualquier organización económica y aun cuando se respeten escrupulosamente todas las políticas de seguridad y las recomendaciones de los expertos no se puede suponer la ausencia de posibles ataques con éxito.”

Según (Ramos, 2011) indica que “En multitud de ocasiones los intrusos de red han superado los mecanismos de autentificación diseñados para proteger los sistemas pues con el aumento en el entendimiento sobre cómo funcionan los sistemas, los intrusos se han vuelto expertos en determinar las debilidades, empleando diversos niveles de engaño antes de imprimir en un sistema determinado, intentando cubrir sus huellas para que su actividad en el sistema no se descubra fácilmente.”

Según (Ramos, 2011) indica que “La seguridad de los sistemas informáticos es uno de los principios problemas con los que podemos encontrarnos hoy en día. Resulta de vital importancia la conservación, almacenamiento e integridad de la información en formato electrónico, ya que esta ha pasado de ser un elemento abstracto de baja importancia, a ser considerada incluso como un activo dentro del capital de las empresas.”

Se pretende realizar el modelo de seguridad para la infraestructura de información de la institución “IKRIT.SRL” que una vez implementado tendrá el objetivo de realizar el control de acceso control de puertos y explorar las vulnerabilidades para prevenir intrusos en la

infraestructura de información y brindar un informe así para maximizar la seguridad se utilizará las herramientas como ser Sistema Operativo Linux y lenguajes de programación JavaScript, PHP y herramientas como ser nmap, nvt, amap, entre otras.

1.2. ANTECEDENTES

La institución “IKRIT.SRL” es una entidad que se encarga del área de construcción y servicios.

Tabla: 1.1. *Datos de la institución.*

	DESCRIPCION
Razón Social	IKRIT CONSULTORES S.R.L.
Matricula de Comercio	00352765
Tipo societario	Sociedad de Responsabilidad Limitada.
Actividad	Servicios de consultoría e tecnologías informáticas de información, de comunicación, financieras, contables, administrativas y construcción.
Numero de NIT	00318954021
Actividad General	Información y Comunicaciones.
Actividad Primaria	Programación informática, consultoría de informática y actividades conexas.
Actividades Especificas	Actividades de consultoría de informática y de gestión de instalaciones informáticas.

Fuente: [Elaboración propia]

1.2.1 Internacional.

- Autor: NAVARRO A, Amílcar J.

  Gestión: febrero de 2007

  Universidad: Universidad Metropolitana

  Título: **“ METODOLOGIA PARA LA GESTION DE SEGURIDAD DE INFORMACION EN VENEZUELA”.**

  Las organizaciones hoy en día son amenazadas constantemente en sus activos, lo que puede representar miles o millones de dólares en pérdidas. La información es uno de los activos más valiosos que tienen las organizaciones y por ende debe ser administrada y protegida de acuerdo a su importancia. Un elemento crítico para el éxito y la supervivencia de las organizaciones, es la gestión efectiva de la información y de la Tecnología de Información (TI). En esta sociedad globalizada (donde la información viaja a través del “ciberespacio” sin las restricciones de tiempo, distancia y velocidad).

- Autor: Daniela V. Peña Q.

  Gestión: octubre de 2016

  Universidad: Universidad central de Venezuela.

  Título: **“DISEÑO E IMPLEMENTACION DE UNA RED PRIVADA VIRTUAL (VPN-SSL) UTILIZANDO EL METODO DE AUTENTICACION LDAP EN UNA EMPRESA PRIVADA”**.

  En la actualidad, las organizaciones han incrementado las implementaciones de la VPN-SSL, dicha implementación se encarga de conectar usuarios remotos a la LAN de la Organización. La conexión vía VPN-SSL, se establece mediante una infraestructura pública (Internet) de manera segura, ya que los datos se establecen a través de un canal

cifrado. La conexión a través de esta infraestructura pública, permite la reducción de costos en la implementación y se puede establecer la conexión segura desde cualquier ubicación geográfica.

1.2.2 Nacional

- Autor: Adalid Mamani Guarachi

  Gestión: 2015

  Universidad: Universidad Mayor de San Andrés.

  Título **"MODELO DE SEGURIDAD EN LAS APLICACIONES WEB"**.

  El trabajo de investigación es referente a las aplicaciones web que en la actualidad son de uso general en todos los ámbitos donde se utilizan la tecnología web. Tiene como énfasis de realizar un análisis de la seguridad en las aplicaciones web, en base a ello se plantea el Modelo de Seguridad en las Aplicaciones Web.

- Autor: Inés Margarita Ramos

  Gestión: 2011

  Universidad: Universidad Mayor de San Andrés.

  Título: **"MODELO PARA LA DETECCION DE INTRUSOS EN LA SEGURIDAD DE SISTEMAS INFORMATICOS APLICANDO LOGICA DIFUSA"**.

  El desarrollo de la tesis se apoya dentro del método científico que sirve de guía para la organización del proceso de investigación ya que cubrirá los requerimientos necesarios para llegar al cumplimiento de los objetivos planteados. En los últimos años, la seguridad informática se ha vuelto en una prioridad importante debido al incremento en el uso de las computadoras, el surgimiento del comercio electrónico y el rápido crecimiento de las

redes de computadoras, desde entonces las intrusiones toman ventaja de las vulnerabilidades del sistema.

1.3 PLANTEAMIENTO DEL PROBLEMA

Actualmente en la institución "IKRIT.SRL" no cuenta con un data center sino que cuenta con 1 rack de servidores de 7 bahías que cuenta con 3 servidores, 1 servidor de desarrollo, 1 servidor de publicidad y 1 servidor de Backup, tiene instalado sistema operativo Linux, tomcat como servidor, y entre otros servicios y cuenta con un conversor de fibra óptica a Red LAN, Para su seguridad solo tiene instalado firewall juniper networks, no cuenta con un encargado de seguridad para verificar los puertos y accesos.

1.3.1 Problema principal.

En la institución "IKRIT. SRL" no cuenta con un modelo de seguridad que permita describir las vulnerabilidades de la infraestructura de la información y servicios que tiene, ya que no cuenta con un responsable entendido en el tema.

1.3.2 Problemas secundarios.

- Falta de seguridad y carencia de control en los servidores (servicios, puertos, accesos).
- Ausencia de reportes sobre las vulnerabilidades existentes en la infraestructura de información de la institución "IKRIT.SRL".
- Insuficiencia de control al usuario en sus tareas y accesos.
- Falta de implementación de herramientas de monitoreo.

1.3.3. Formulación del problema.

¿De qué manera ayudaría un modelo de seguridad aplicando la infraestructura de información de "IKRIT.SRL"?

1.4 OBJETIVOS

1.4.1 Objetivo general.

Implementar un modelo de seguridad que permita el rastreo, evaluación, y el monitoreo de las acciones que hace el (usuario, sistema, servicio) para evitar usar las vulnerabilidades en contra de la institución “IKRIT.SRL”.

1.4.2 Objetivos específicos.

- Analizar los requerimientos de la institución.
- Ejecutar test y protocolos en servicios de “IKRIT.SRL”.
- Analizar las vulnerabilidades existentes en los servidores y servicios de “IKRIT.SRL”.
- Diseñar un modelo de búsqueda de vulnerabilidades de puertos y servicios.
- Poner en marcha reportes de vulnerabilidad de la institución “IKRIT.SRL” en sus servicios en base a las vulnerabilidades y diseñar un modelo de seguridad.
- Reportes de las vulnerabilidades encontradas, para apoyar la toma de decisiones.

1.5 HIPOTESIS

Con el apoyo de herramientas y metodologías se implementa un modelo para la búsqueda de vulnerabilidades en la infraestructura de la información (servidores y servicios) de “IKRIT.SRL”, con una eficiencia de 95%.

1.5.1 Identificación de variables.

a) Variable independiente

   Modelo de búsqueda de las vulnerabilidades.

b) Variable dependiente.

   Servidores y servicios.

1.5.2 Operaciónalizacion de variables.

Tabla: 1.2.

La siguiente tabla cuenta con la operacionalizacion de variables.

Variables	**Dimensiones**	**Indicadores**	**Actividades o Herramientas**
Variable Independiente Modelo de búsqueda de las vulnerabilidades	Encargado de la seguridad que se tiene en el modelo.	La cantidad de vulnerabilidades.	Verificar tanto como software y hardware si la seguridad es correcta utilizando nmap, ncrack, metasploit framework.
Variable Dependiente Servidores y servicios	Medición porcentual de seguridad en la infraestructura "IKRIT.SRL".	Control o el acceso indebido al sistema.	Uso cuestionario y de entrevistas a los usuarios.

Fuente: [Elaboración propia]

1.5.3 Conceptualización de variables.

Modelo de Seguridad. – Según (Álvarez, 2005, p. 4) indica que "Los trascendentales cambios operados en el mundo moderno caracterizados por un incesante desarrollo; la acelerada globalización de la economía, la acentuada dependencia que incorpora en el alto volumen de información y los sistemas que la proveen; el aumento de la vulnerabilidad y el amplio espectro de amenazas, tales como las amenazas cibernautitas; la escala y los costos de la inversiones actuales y futuras en información y en sistema de información y el potencial que poseen las

tecnologías para cambiar drásticamente las organizaciones y las prácticas de negocio, crear nuevas oportunidades y reducir costos, han impuesto nuevo retos a la práctica de la profesión de auditoria, en particular a la auditoria de sistemas."

Seguridad para infraestructura de la información. – Según (Bermudez-Bailon, 2015, p.1) indica que "En la actualidad toda empresa se basa en la información para tomar decisiones que permitan la continuidad del negocio, transformándose así en un activo importante para las organizaciones, siendo necesario protegerla ante cualquier evento que puede causar corrupción en los datos. Dada la importancia de la información, organizaciones internacionales de estandarización han elaborado normas de buenas prácticas para el resguardo y buen uso de la información y de los activos en general."

1.6 JUSTIFICACION

1.6.1 Justificación técnica.

El perfil de tesis se justifica técnicamente por la utilización de herramientas avanzadas y factibles para el diseño del modelo de seguridad: utilizare lenguajes de programación como JavaScript, PHP, nmap, ncat, ncrack, metasploit framework, maltego, yersinia y un gestor de base de datos PostgreSQL y servidor HTTP Apache, todo en base a software libre.

1.6.2 Justificación científica.

Se construirá un modelo de seguridad para la infraestructura de información, brindando un informe de vulnerabilidades si es que la tuviera con las herramientas de nmap, ncat, ncrack, metasploit framework, yersinia.

1.6.3 Justificación social.

El modelo de seguridad es necesario para la institución “IKRIT.SRL” para dar seguridad en los datos, reportes de vulnerabilidad si es que lo hubiera y para el usuario dar seguridad en su información.

La institución “IKRIT.SRL”, se beneficiará con el modelo de seguridad, así teniendo una infraestructura confiable y segura.

1.6.4 Justificación económica.

El modelo estará desarrollado en Software libre, por lo que no será un obstáculo el costo de inversión por licencias de funcionamiento.

1.7 METODOLOGIAS

1.7.1 Método científico.

- **Elección del tema. –** Según (Ruiz, 2007, p.35) indica que “En la elección del tema se concretará, tanto como sea posible el objeto de conocimiento; además habrá de estructurarse el título tentativo del proyecto de investigación, tentativo porque podría hacérsele algunas pequeñas precisiones durante el proceso de la investigación.”

  Planteamiento de la investigación. – Según (Ruiz, 2007, p.36) indica que “El problema es la fijación de las contradicciones que se dan en la propia realidad, contradicciones que se fijan en la teoría y que concluyen una vez “esclarecidas” con el planteamiento de un nuevo problema, cuya solución podría ser resuelta por otros investigadores. Para un adecuado planteamiento del problema se requiere de, eliminar del problema cualquier adición engañosa, o sea, identificar aquellas dificultades que chocan con la teoría.”

- **Justificación de problema de investigación. –** Según (Ruiz, 2007, p.45) indica que "En este apartado se explica las razones o los motivos por los cuales se pretende realizar la investigación por lo general es breve y concisa."
- **Objetivo de la investigación. –** Según (Ruiz, 2007, p.46) indica que "Los objetivos es parte fundamental en el proceso de la investigación científica o de cualquier estudio que se realizar, nos permite, predecir, explicar y describir los fenómenos y adquirir conocimientos de esos fenómenos estudiados."
- **Estructuración del esquema. –** Según (Ruiz, 2007, p.48) indica que "El esquema es la representación gráfica sistematizada, que tiene como función principal estructurar un conjunto de ideas y los datos necesarios e imprescindibles de manera sintetizada con el menor número de palabras, en un orden lógico, que permita captar en un solo golpe de vista la temática desglosada."
- **Marco teórico. -** Según (Ruiz, 2007, p50) indica que "El marco teórico es el conjunto de principios teóricos que guían la investigación estableciendo unidades relevantes para cada problema a investigar."
- **Elaboración de hipótesis. -** Según (Ruiz, 2007, p53) indica que "En toda investigación se debe establecer la hipótesis de investigación. La hipótesis debe concordar con la definición del problema, así como con los demás elementos del diseño."
- **Metodología. -** Según (Ruiz, 2007, p61) indica que "La metodología es un procedimiento general para obtener de una manera más precisa el objetivo de la investigación, dependiendo de la problemática que se vaya a estudiar se determina el tipo de investigación, es decir:"

a) Bibliográfica.

b) De Campo.

c) Experimental.

- **Cronograma. -** Según (Ruiz, 2007, p62) indica que "Es el apartado del diseño de la investigación elaborado por quien habrá de realizar la investigación, y en el que se señala las diferentes etapas de realización del proyecto en relación con los tiempos estimados."
- **Anexos**
- **Glosario**
- **Bibliografía**

1.7.2 Método de desarrollo.

1.7.2.1 Metodología UWE.

Según (Nieves-Guerrero, Ucán-Pech, & Menéndez-Domínguez, 2014, p.137) indica que "UWE es una metodología que permite especificar de mejor manera una aplicación Web en su proceso de creación mantiene una notación estándar basada en el uso de UML (Unified Modeling Language) para sus modelos y sus métodos, lo que facilita la transición. La metodología define claramente la construcción de cada uno de los elementos del modelo. En su implementación se deben contemplar las siguientes etapas y modelos."

- Análisis de requisitos
- Modelo de contenido
- Modelo de navegación
- Modelo de presentación
- Modelo de proceso

1.7.3. Metodología Ethical Hacking.

1.7.3.1 Metodología OSSTMM.

Según (Valencia Blanco, 2013, p.27) indica que "Metodología que propone un proceso de evaluación de una serie de áreas que refleja de manera fiel los niveles de seguridad presentes en la infraestructura que va a ser auditada, a estos niveles de seguridad se le denominan comúnmente "Dimensiones de Seguridad" y normalmente consiste en analizar los siguientes factores."

- ✓ Visibilidad.
- ✓ Acceso.
- ✓ Confianza.
- ✓ Autenticación.
- ✓ Confidencialidad.
- ✓ Privacidad.
- ✓ Autorización.
- ✓ Integridad.
- ✓ Seguridad.
- ✓ Alarma.

Como parte de un trabajo secuencial la metodología OSSTMM consta de 6 ítems los cuales comprenden todo sistema actual, estos son:

- ✓ Seguridad de la Información.
- ✓ Seguridad de los Procesos.
- ✓ Seguridad en las tecnologías de Internet.
- ✓ Seguridad en las comunicaciones.

- ✓ Seguridad inalámbrica.
- ✓ Seguridad Física.

1.8. MÉTRICA DE CALIDAD

Según (PowerData, 2016) indica que “La mala calidad de la información y de software impacta negativamente en el negocio a diferentes niveles:”

- Disminuye ingresos y aumenta el gasto.
- Incrementa el riesgo.
- Provoca una reducción de la confianza, tanto dentro como fuera de la organización.

Un enfoque proactivo tanto del gobierno de la información como del data quality permite la identificación temprana de errores o defectos que pueden ser corregidos a tiempo, eliminando de raíz problemas mayores. Los efectos positivos empiezan a notarse y sus beneficios aumentan en un ciclo de mejora continúa propiciado por el control de las métricas de calidad de software.

Esta monitorización facilita el evaluar:

- La calidad del producto.
- El rendimiento del equipo de desarrollo.
- La justificación del uso de nuevas herramientas o soluciones.
- Los resultados obtenidos a partir de la incorporación del software a los procesos y operaciones.

Para conseguir llegar al nivel de evaluación, es preciso contar con datos relevantes, precisos y actualizados sobre diferentes áreas, que faciliten una perspectiva global de la solución. Así, las métricas de calidad de software pueden aplicarse a diferentes contextos, como:

- El proyecto: son las que facilitan la gestión del riesgo permitiendo tomar el pulso a la iniciativa de desarrollo desde su inicio.
- El producto: están enfocadas a medir las características del software y todos los entregables que lo acompañan, fruto del proyecto de desarrollo, como modelos, componentes adicionales y documentación.
- El proceso: tienen por objeto identificar mejores prácticas para su exportación a futuros proyectos y, para conseguirlo, recopilan datos de distintas iniciativas a lo largo de un periodo de tiempo determinado.

1.8.1. ISO/IEC 25000

Según (ISO25000, 2019) indica que "ISO/IEC 25000, conocida como Suaré (System and Software Quality Requirements and Evaluation), es una familia de normas que tiene por objetivo la creación de un marco de trabajo común para evaluar la calidad del producto software.

Es el resultado de la evolución de otras normas anteriores, especialmente de las normas ISO/IEC 9126, que describe las particularidades de un modelo de calidad del producto software, e ISO/IEC 14598, que abordaba el proceso de evaluación de productos software. Esta familia de normas ISO/IEC 25000 se encuentra compuesta por cinco divisiones."

- ISO/IEC 2500n: División para gestión de la calidad
- ISO/IEC 2501n: División para el modelo de calidad.
- ISO/IEC 2502n: División para la medición de calidad.
- ISO/IEC 2503n: División para los requisitos de calidad.
- ISO/IEC 2504n: División para la evaluación de calidad

1.8.1.1. Métodos y técnicas.

- Testing
- Inspección
- Consulta.
- Modelado Analítico.
- Simulación

Los Métodos y Técnicas a Aplicar pueden ser: Los Métodos y Técnicas a Aplicar pueden ser:

- Cuantitativos versus Cualitativos.
- Automáticos, Semiautomáticos o Manuales.
- Desde Fácil a Difícil de Usar y Aprender.

1.8.1.2. Test.

Algunos puntos interesantes para medir y controlar son:

- Efectividad de la prueba/desarrollo
- Esfuerzo
- Sobre esfuerzo
- Cobertura de requisitos
- Cobertura de riesgos
- Cobertura de código
- Calidad del desarrollo
- Testing

1.9. HERRAMIENTAS

- ✓ **JavaScript. -** Según (Wikipedia, Wikipedia, 2020) indicia que " (abreviado comúnmente JS) es un lenguaje de programación interpretado, dialecto del estándar ECMAScript. Se define como orientado a objetos, basado en prototipos, imperativo, débilmente tipado y dinámico. Se utiliza principalmente en su forma del lado del cliente (client-side), implementado como parte de un navegador web permitiendo mejoras en la interfaz de usuario y páginas web dinámicas aunque existe una forma de JavaScript del lado del servidor (Server-side JavaScript o SSJS)."

- ✓ **PHP. -** Según (Wikipedia. (2019)). indicia que "Acrónimo recursivo en inglés de PHP: Hypertext Preprocessor (preprocesador de hipertexto), es un lenguaje de programación de propósito general de código del lado del servidor originalmente diseñado para el pre-procesado de texto plano en UTF-8. Posteriormente se aplicó al desarrollo web de contenido dinámico, dando un paso evolutivo en el concepto de aplicación en línea, por su carácter de servicio. Su implementación en los documentos HTML era aparentemente muy sencilla. Hay que decir, que, PHP no genera HTML, sino que ofrece una salida de texto con codificación UTF-8 compatible con los documentos HTML."

- ✓ **BOOTSTRAP. -** Según (Anónimo. (2019)). indicia que "Bootstrap es un kit de herramientas de código abierto para desarrollar con HTML, CSS y JS. Realice rápidamente prototipos de sus ideas o cree toda su aplicación con nuestras variables y mixins Sass, sistema de cuadrícula sensible, componentes pre compilados extensos y complementos potentes creados en jQuery."

- ✓ **NMAP. -** Según (Insecure. Com LLC. (2011)). indicia que "Es un programa de código abierto que sirve para efectuar rastreo de puertos y cuyo desarrollo se encuentra hoy a cargo de una comunidad. Fue creado originalmente para Linux, aunque actualmente es multiplataforma. Se usa para evaluar la seguridad de sistemas informáticos, así como para descubrir servicios o servidores en una red informática, para ello Nmap envía unos paquetes definidos a otros equipos y analiza sus respuestas."

- ✓ **NCAT. -** Según (Insecure. Com LLC. (2011)). indicia que "Es una utilidad de red repleta de funciones que lee y escribe datos a través de redes desde la línea de comandos. Ncat fue escrito para el Proyecto Nmap como una re implementación muy mejorada del venerable Netcat . Utiliza tanto TCP como UDP para la comunicación y está diseñado para ser una herramienta de fondo confiable para proporcionar instantáneamente conectividad de red a otras aplicaciones y usuarios. Ncat no solo funcionará con IPv4 e IPv6, sino que también proporciona al usuario un número prácticamente ilimitado de usos potenciales."

- ✓ **NCRACK. -** Según (Ithilgore. (20016)). indicia que "Esta herramienta de craqueo de autenticación en red de alta velocidad, fue construido para ayudar a las compañías a proteger sus redes probando todos sus hosts y dispositivos de red contra las contraseñas débiles. Los profesionales de la seguridad también confían en Ncrack al auditar a sus clientes. Ncrack fue diseñado utilizando un enfoque modular, una sintaxis de línea de comandos similar a Nmap y un motor dinámico que puede adaptar su comportamiento basado en la retroalimentación de la red. También permite una auditoría a gran escala rápida y confiable de múltiples hosts.

- ✓ **METASPLOIT FRAMEWORK. -** Según (Metasploit. (2019)). indicia que "Metasploit Framework es una plataforma de prueba de penetración modular basada en Ruby que le permite escribir, probar y ejecutar código de explotación. Metasploit Framework contiene un conjunto de herramientas que puede usar para probar vulnerabilidades de seguridad, enumerar redes, ejecutar ataques y evadir la detección. En esencia, Metasploit Framework es una colección de herramientas de uso común que proporcionan un entorno completo para pruebas de penetración y desarrollo de exploits."

- ✓ **MALTEGO. –** Según (Maltego technologies. (2020)). indicia que "Maltego es una herramienta interactiva de datos que presenta gráficos dirigidos para el análisis de enlaces. La herramienta se utiliza en investigaciones en línea para encontrar relaciones entre piezas de información de varias fuentes ubicadas en internet.

- ✓ **YERSINIA. -** Según (Offec Services Limited. (2020)). indicia que "Es un marco para realizar ataques de capa 2. Está diseñado para aprovechar algunas debilidades en diferentes protocolos de red. Pretende ser un marco sólido para analizar y probar las redes y sistemas desplegados."

- ✓ **DSNIFF. -** Según (McGraw-Hill. (2001)). indicia que "Es una colección de herramientas para auditorías de red y pruebas de penetración. dsniff, filesnarf, mailsnarf, msgsnarf, urlsnarf y webspy monitorean pasivamente una red en busca de datos interesantes (contraseñas, correo electrónico, archivos, etc.). arpspoof, dnsspoof y macof facilitan la intercepción del tráfico de red que normalmente no está disponible para un atacante (por ejemplo, debido a la conmutación de capa 2). sshmitm y webmitm

implementan ataques activos de mono en el medio contra sesiones SSH y HTTPS redirigidas mediante la explotación de enlaces débiles en PKI ad-hoc."

- ✓ **ETTERCAP. -** Según (Ornaghi-Escobar. (2009)). indicia que "Ettercap es una suite completa para ataques de hombre en el medio. Presenta olfateo de conexiones en vivo, filtrado de contenido sobre la marcha y muchos otros trucos interesantes. Admite la disección activa y pasiva de muchos protocolos e incluye muchas características para el análisis de red y host.
- ✓ **IKE-SCAN. -** Según (Anónimo. (2013)). indicia que "Es una herramienta de línea de comandos para el descubrimiento, identificación y prueba de sistemas IPsec VPN. Construye y envía IKE Fase 1-paquetes a los hosts especificados, y muestra las respuestas que se reciben.
- ✓ **NESSUS. -** Según (Wikipedia. (2013)). indicia que "Los escaneos de Nessus cubren una amplia gama de tecnologías que incluyen sistemas operativos, dispositivos de red, hipervisores, bases de datos, servidores web e infraestructura crítica.
- ✓ **SOCIAL ENGINEERING TOOLKIT. -** Según (TrustedSec. (2020)). indicia que "El kit de herramientas de ingeniería social (SET) fue creado y escrito por Dave Kennedy, el fundador de TrustedSec. Es una herramienta de código abierto basada en Python destinada a las pruebas de penetración en torno a la Ingeniería Social."

1.9.1. Base de datos.

- ✓ **PostgreSQL. -** Según (Wikipedia. (2020)). indicia que "Es un sistema de gestión de bases de datos relacional orientado a objetos y de código abierto, publicado bajo la licencia PostgreSQL, similar a la BSD o la MIT. Como muchos otros proyectos de código abierto, el desarrollo de PostgreSQL no es manejado por una empresa o persona,

sino que es dirigido por una comunidad de desarrolladores que trabajan de forma desinteresada, altruista, libre o apoyados por organizaciones comerciales.

1.9.2. Servidor WEB.

- ✓ **Apache. -** Según (Wikipedia. (2019)). indicia que "El servidor HTTP Apache es un servidor web HTTP de código abierto, para plataformas Unix (BSD, GNU/Linux, etc.), Microsoft Windows, Macintosh y otras, que implementa el protocolo HTTP/1.1 y la noción de sitio virtual según la normativa RFC 2616. Cuando comenzó su desarrollo en 1995 se basó inicialmente en código del popular NCSA HTTPd, pero más tarde fue reescrito por completo. Su nombre se debe a que alguien quería que tuviese la connotación de algo que es firme y enérgico, pero no agresivo, y la tribu Apache fue la última en rendirse al que pronto se convertiría en gobierno de Estados Unidos, y en esos momentos la preocupación de su grupo era que llegasen las empresas y "civilizasen" el paisaje que habían creado los primeros ingenieros de internet. Además, Apache consistía solamente en un conjunto de parches a aplicar al servidor de NCSA. En inglés, a patchy server (un servidor "parcheado") suena igual que Apache Server.

1.10. LIMITES Y ALCANCES

1.10.1. Limites.

El siguiente modelo de seguridad se aplicará en la infraestructura de "IKRIT.SRL" y no así en otra institución.

El prototipo dependerá de la información que provea la entidad.

1.10.2. Alcances.

Se tendrá los siguientes módulos:

- ✓ Modelo Test.
- ✓ Módulo de test de vulnerabilidad.
- ✓ Módulo de reportes de vulnerabilidad.
- ✓ Modelo de análisis de vulnerabilidad (servidor, servicios)

1.11. APORTES

Se brindará un informe de los sistemas, se podrá hacer una contingencia a todos los puntos vulnerables que tenga, se tendrá una mejora para no tener robo de la información y extracto de la información fuera de la institución, basado en la implementación de modelo de seguridad.

CAPITULO II

MARCO TEORICO

2.1. INTRODUCCIÓN

En este capítulo muestra una recopilación sobre conceptos que intervienen en el presente trabajo, herramientas que constituyen una base para el desarrollo del Tema.

2.2. MODELO

Según (Pressman, 2010). indicia que “Se crean modelos para entender mejor la entidad real que se va a construir. Cuando ésta es física (por ejemplo, un edificio, un avión, una máquina, etc.), se construye un modelo de forma idéntica, pero a escala. Sin embargo, cuando la entidad que se va a construir es software, el modelo debe adoptar una forma distinta. Debe ser capaz de representar la información que el software transforma, la arquitectura y las funciones que permiten que esto ocurra, las características que desean los usuarios y el comportamiento del sistema mientras la transformación tiene lugar. Los modelos deben cumplir estos objetivos en diferentes niveles de abstracción, en primer lugar, con la ilustración del software desde el punto de vista del cliente y después con su representación en un nivel más técnico.”

Según (Perez L. S., 2012). indicia que “Un modelo es una representación de un objeto, sistema o idea, de forma diferente al de la entidad misma. El propósito de los modelos es ayudarnos a explicar, entender o mejorar un sistema. Un modelo de un objeto puede ser una réplica exacta de éste o una abstracción de las propiedades dominantes del objeto.

Un modelo se utiliza como ayuda para el pensamiento al organizar y clasificar conceptos confusos e inconsistentes. Al realizar un análisis de sistemas, se crea un modelo del sistema que muestre las entidades, las interrelaciones, etc. La adecuada construcción de un modelo ayuda a organizar, evaluar y examinar la validez de pensamientos.”

2.2.1. Tipos de modelo.

2.2.1.1. Modelo de muestreo.

La prueba de software ejecuta m casos de prueba aleatorios y se certifica si no ocurren fallos o un número específico de ellos. El valor de m se deriva matemáticamente para asegurar que se logra la confiabilidad requerida.

2.2.1.2. Modelo de Componentes.

Se certifica un sistema compuesto de n componentes. El modelo de componentes permite al analista determinar la probabilidad de que el componente fallará antes de su conclusión.

2.2.1.3. Modelo de Certificación.

Según (Pressman, 2010). indicia que "La confiabilidad global del sistema se proyecta y se certifica. Al completar las pruebas de uso estadístico, el equipo de certificación tiene la información requerida para entregar el software que tenga un TMHF certificado, usando cada uno de estos modelos."

2.2.2. Características de un Modelo.

Según (Berenicemh10, 2013). indicia que "A veces, el modelo tiene por objeto reemplazar el sistema real para simplificar su estudio. Por ejemplo, podemos considerar que la Tierra y la Luna son partículas puntuales que poseen la masa de los astros considerados. Un modelo es a veces una imagen mental de la estructura o propiedades de un sistema. Así, la luz ha sido modelada como un flujo de partículas discretas (fotones) o como una onda continua y finalmente se introdujo el concepto de onda asociada a una partícula que fue ratificada experimentalmente. Ambos modelos confluían en uno solo y la luz se comportaba como una dualidad onda-partícula. Los criterios principales que un modelo debe satisfacer son los siguientes:"

- El modelo debe de ser lo más simple.
- El modelo no debe ser incompatible con las teorías establecidas en campos de estudio relacionado.
- El modelo debe ser capaz de predecir fenómenos que puedan ser comprobados experimentalmente.

2.3. PATRON DE DISEÑO

Según (RUBENFA, 2014). indicia que "Los patrones de diseño son soluciones para problemas típicos y recurrentes que nos podemos encontrar a la hora de desarrollar una aplicación.

Aunque nuestra aplicación sea única, tendrá partes comunes con otras aplicaciones: acceso a datos, creación de objetos, operaciones entre sistemas etc. En lugar de reinventar la rueda, podemos solucionar problemas utilizando algún patrón, ya que son soluciones probadas y documentadas por multitud de programadores."

2.3.1. ¿Qué es un Patrón de Diseño?

Es una solución general reusable que puede ser aplicada a problemas que ocurren comúnmente en el desarrollo de software, es la descripción o plantilla de cómo resolver un problema que puede ser usada en diferentes situaciones.

2.3.1.1. Elementos de Patrón de Diseño.

- Nombre del patrón- el nombre debe ser suficientemente descriptivo para saber de qué estamos hablando.
- Problema- describe el problema general o la situación a resolver.

- Solución- describe la solución general a implementar (debe ser adaptada de acuerdo a el contexto especifico).
- Consecuencias- describe lo bueno y lo malo que pasaría si se implementa.

2.3.1.2. Clasificación De Patrones de Diseño.

- Patrones Creacionales — Creational Design Patterns

  Proveen las técnicas para crear objetos. Algunos ejemplos son:

  Singleton (Instancia Unica)

  Abstract Factory (fabrica abstracta)

  Builder Pattern (Constructor virtual)

- Patrones Estructurales — Structural Design Patterns

  Describen la composición de los objetos y su organización. Ejemplos:

  Adapter Pattern (Adaptador)

  Decorator Pattern (Decorador)

- Patrones de Comportamiento — Behavioral Design Patterns

  Se enfocan en mejorar la comunicación entre los objetos en un sistema.

  Iterator Pattern (Iterador)

  Observer Pattern (Observador)

  Strategy Pattern (Estrategia)

2.3.2 ¿Qué es un Anti patrón?

Según (Amaya, 2016). indicia que “Es la respuesta común a un problema recurrente que es usualmente inefectiva y típicamente tiene mayor número de consecuencias negativas que buenas.

Como, por ejemplo: Clases Dios: éstas son clases que controlan muchas otras clases y tienen muchas dependencias y responsabilidades. Las clases Dios tienden a crecer hasta el punto en que su mantenimiento se convierte en una pesadilla.”

2.4. DISEÑO

Un diseño es la expresión de una idea que soluciona de forma innovadora un problema concreto y sirve de guía para llevarlo a la práctica, es decir, para construirlo y evaluarlo.

- Definir el problema que siempre nace de una necesidad.
- La forma o esquema para resolver la necesidad y elegir uno para analizarlo, estudio de factibilidad.
- Diseñar de forma preliminar la máquina, estructura, sistema o proceso seleccionado; permitiendo establecer las características globales y las específicas de cada componente.
- Realizar el análisis de todas y cada uno de los componentes y preparar los dibujos necesarios con sus respectivas especificaciones.

2.4.1. Desventajas

Según (Escobar, 2009). indicia que “Las desventajas de trabajar sin diseño son muchas: falta de una orientación adecuada para el equipo, ya que cada miembro puede tener ideas diferentes sobre lo que se quiere construir; se puede adelantar mucho en la construcción y tener que desecharlo todo por falta de consistencia o porque simplemente se asumió algo que después

resulta incorrecto; se le dedica demasiado tiempo a aspectos del problema y se descuida otros de igual o mayor importancia; no hay forma de evaluar si lo que se ha avanzado corresponde en tiempo y esfuerzo a lo que se habría esperado; y un largo etcétera.”

2.5. MAQUETADO

Es el diseño de la aplicación en lo relacionada la interfaz de usuario los componentes, las vistas, sin llegar a funcionalidad lógica, si en relación a el diseño de la interfaz.

2.5.1. Elementos de la Maquetación.

- Según (Resendiz, 2018). indicia que “Diseño de la Interfaz Gráfica de Usuario: que incluye la usabilidad, y elementos estéticos a la vista de aplicación, como la distribución de componentes, colores, gráficos, tipos de letra, elementos de interacción con el usuario.”
- Según (Resendiz, 2018). indicia que “Diseño de la Navegación: se diseña como el usuario navegara por la aplicación, donde se coloca la información, la distribución de la misma.”
- Según (Resendiz, 2018). indicia que “Diseño de Interfaz Técnica: que incluye los patrones de la interfaz, elementos comunes ubicación de funcionalidades estándar de la aplicación, como puede ser mover, agrandar cerrar una ventana.”

2.6. PROTOTIPO

Según (anonimo, 2019). indicia que “Un Prototipo es el primer dispositivo que se fabrica y del que se toman las ideas más relevantes para la construcción de otros diseños y representa todas las ideas en cuanto a diseño, soporte y tecnología que se les puedan ocurrir a sus creadores. Por lo general un prototipo no sale a la venta a menos que sea menos que sea un terminal

orientado para que otros desarrolladores de tecnología trabajen con él para insertar nuevas funciones o especificaciones a este para que funcione de una manera más eficiente.

Como analista de sistemas que va a presentar un prototipo del sistema de información, a usted le interesan mucho las reacciones que tendrán los usuarios y la administración con respecto al prototipo. Debe anticipar con precisión cómo reaccionarán al trabajar con el prototipo y qué tan bien se adaptarán a sus necesidades las características del sistema previstas. Las reacciones se recopilan a través de la observación, entrevistas y hojas de retroalimentación (posiblemente cuestionarios) diseñadas para obtener la opinión de cada persona sobre el prototipo a medida que interactúa con él."

La información que se recopila en la fase de prototipos permite al analista establecer prioridades y redirigir los planes sin sufrir repercusiones graves, con un mínimo de interrupción. Debido a esta característica, la creación de prototipos y la planeación van de la mano.

2.6.1 Prototipo de características selectas.

- Prototipo de Características Selectas: La cuarta concepción de los prototipos es la creación de un modelo operacional que incluya sólo algunas características del sistema final. Una analogía sería un nuevo centro comercial que abra antes de terminar de construir todas las tiendas.

  Al crear prototipos de sistemas de información de esta forma, es posible incluir sólo algunas características esenciales. Por ejemplo, el prototipo de un sistema mostraría a los usuarios un menú de pantalla con seis características, agregar un registro, actualizar un registro, eliminar un registro, buscar una palabra clave en un registro, listar un registro o escanear un registro, aunque sólo tres de las seis características estarían habilitadas para usarse, de manera que el usuario pueda agregar un registro (característica 1),

eliminar un registro (característica 3) y listar un registro (característica 5). La retroalimentación de los usuarios puede ayudar a los analistas a comprender lo que funciona y lo que no. También puede ayudar con las sugerencias sobre cuáles pueden ser las siguientes características a agregar.

2.6.2. Prototipos como Alternativa para el SDLC.

Algunos analistas argumentan que es necesario considerar a los prototipos como una alternativa al SDLC. El SDLC es una metodología lógica y sistemática para desarrollar sistemas de información. Las quejas sobre tener que pasar por el proceso del SDLC se concentran en dos aspectos interrelacionados. El primero es el largo tiempo requerido para pasar por el ciclo de vida de desarrollo. A medida que aumenta la inversión de tiempo del analista, el costo del sistema entregado se eleva en forma proporcional.

2.6.3. Desarrollo de un Prototipo.

Según (KENDALL, 2011). indicia que “Los prototipos son un medio excelente para obtener retroalimentación sobre el sistema propuesto y el grado en que cumple con las necesidades de información de sus usuarios, El primer paso de la creación de un prototipo es estimar los costos involucrados en la construcción de un módulo del sistema. Si los costos del tiempo de los programadores y del analista, así como los costos del equipo están dentro del presupuesto, se puede continuar con la construcción del prototipo. Ésta es una excelente manera de facilitar la integración del sistema de información en la cultura y sistema, más extensos, de la organización.”

2.6.4. Lineamiento para desarrollar un Prototipo.

Una vez tomada la decisión de crear un prototipo, hay que cumplir con cuatro lineamientos para integrar el prototipo en la fase de determinación de requerimientos del SDLC:

- Trabajar en Módulos Administrables: Al crear prototipos de algunas de las características de un sistema y convertirlos en un modelo funcional, es imperativo que el analista trabaje en módulos administrables. Una de las ventajas únicas de los prototipos es que no es necesario ni conveniente construir todo un sistema funcional para usarlos.
- Crear el Prototipo con rapidez: La velocidad es esencial para la creación de un prototipo exitoso de un sistema de información. Recuerde que una de las quejas sobre el SDLC tradicional es que el intervalo entre la determinación de los requerimientos y la entrega de un sistema completo es demasiado largo como para poder lidiar en forma efectiva con las necesidades en evolución de los usuarios.
- Modificar el prototipo: Un tercer lineamiento para desarrollar el prototipo es que su construcción debe admitir modificaciones. Para lograr esto hay que crearlo en módulos que no tengan un alto grado de interdependencia. Si cumplimos con este lineamiento encontraremos menos resistencia cuando haya que modificar el prototipo.
- Hacer énfasis en la Interfaz de Usuario: La interfaz del usuario con el prototipo (y con el sistema, en última instancia) es muy importante. Como lo que realmente tratamos de lograr con el prototipo es hacer que los usuarios articulen con más detalle sus requerimientos de información, deben ser capaces de interactuar con facilidad con el prototipo del sistema. También deben ser capaces de ver cómo el prototipo les permitirá realizar sus tareas. Para muchos usuarios, la interfaz es el sistema. No debe ser un obstáculo.

2.7. SERVICIOS

Según (Conceptodefinicion.de, 2019). indicia que “Un Servicio representa un conjunto de acciones las cuales son realizadas para servir a alguien, algo o alguna causa. Los servicios son funciones ejercidas por las personas hacia otras personas con la finalidad de que estas cumplan con la satisfacción de recibirlos. Los servicios prestados es una comunidad cualquiera están determinados en clases, a su vez estas clases están establecidas de acuerdo a la figura, personal o institucional que lo ofrece o imparte.”

2.7.1. Tipos de servicios.

Existen servicios públicos y servicios especializados.

- Los servicios públicos son funciones ejercidas por las instituciones públicas adscritas o conformadas por el gobierno los cuales son realizados con el fin de generar una estabilidad y comodidad en la sociedad.
- Los servicios especializados ya son una materia más selecta en acciones, pues, a pesar que estos son ofrecidos para cualquiera que esté en la disponibilidad de cancelar un pago por estos, no todos lo necesitan.

2.7.2. Puertos de Servicios más Utilizados.

Según (OpenCloud, 2016). indicia que:

- ✓ HTTP: puerto 80;
- ✓ HTTPS: puerto 443;
- ✓ FTP: puerto 21;
- ✓ FTPS/SSH: puerto 22;
- ✓ POP3: puerto 110
- ✓ POP3 SSL: puerto 995
- ✓ IMAP: puerto 143
- ✓ IMAP SSL: puerto 993
- ✓ SMTP: puerto 25 (alternativas: puerto 26 / puerto 2525)

- ✓ SMTP SSL: puerto 587
- ✓ MySQL: puerto 3306
- ✓ CPanel: puerto 2082
- ✓ CPanel SSL: puerto 2083
- ✓ WHM (Webhost Manager): puerto 2086
- ✓ WHM (Webhost Manager) SSL: puerto 2087
- ✓ Webmail: puerto 2095
- ✓ Webmail SSL: puerto 2096
- ✓ WebDAV/WebDisk: puerto 2077
- ✓ WebDAV/WebDisk SSL: puerto 2078

2.8. SERVIDORES

Según (g42roram, 2006-2020). indicia que "Un servidor, como la misma palabra indica, es un ordenador o máquina informática que está al "servicio" de otras máquinas, ordenadores o personas llamadas clientes y que les suministran a estos, todo tipo de información. A modo de ejemplo, imaginemos que estamos en nuestra casa, y tenemos una despensa.

Por tanto, un servidor en informática será un ordenador u otro tipo de dispositivo que suministra una información requerida por unos clientes (que pueden ser personas, o también pueden ser otros dispositivos como ordenadores, móviles, impresoras, etc.)."

Los más conocidos serian:

- Servidor WEB
- Servidor de correo electrónico
- Servidor de base de datos
- Servidor de juegos
- Servidor de proxy
- Servidor de DNS

Según (Frutos, 2016). indicia que “Un servidor es un ordenador o una partición muy potente de éste que se encarga de almacenar archivos y distribuirlos en Internet para que sean accesibles a los usuarios.

Lo cierto es que el uso de este término es muy ambiguo, ya que en el mundo de la informática se le llama originalmente servidor al programa que ofrece una serie de servicios, a los que se suele acceder por medio de programas especiales que se denominan clientes. Aunque, por extensión, suele llamarse servidor al ordenador en el que funcionan estos programas.”

2.8.1. Servidor Web.

Según (Anonimo, 2018). indicia que “Un servidor web, sirve para almacenar los ficheros de un sitio web. Así como ejecutarlos cuando un usuario hace una petición de acceso a una página. Ahora bien, para entender un poco más las funciones de un servidor web, debemos definirlo. Un servidor web, en palabras sencillas, es el encargado de transmitir los datos.”

2.8.1.1. ¿De dónde surge?

Un servidor web, surge de la necesidad de igualar la comunicación. Entre los diferentes lenguajes de programación, o plataformas. Debe estar permanentemente conectado a una red de alta velocidad, lo que forma parte de Internet. Esto permite alojar varias páginas web. Así como, almacenar los archivos de un sitio, y transmitir datos por el sistema de redes llamado Internet.

2.8.1.2. ¿Cómo funciona un servidor WEB?

Según (Anonimo, 2018). indicia que “Un servidor web, funciona básicamente de la siguiente forma cuando estamos navegando en un sitio en Internet. En el momento que hacemos una petición, se envía desde la dirección IP de nuestro computador, hacia la dirección IP del

servidor. Y es el servidor web, quien responde enviando información a la dirección IP que la solicita. Finalmente, se nos muestra en pantalla, los datos que queremos visualizar."

Según (Frutos, 2016). indicia que "los famosos servidores web, que almacenan los archivos HTML de una página y los proporciona a los clientes que los solicitan haciendo la transferencia de los archivos a través de la red mediante los navegadores.

Los servidores web son uno de los aspectos más importantes de Internet, ya que se trata de los encargados de despachar las páginas a los usuarios. Sin ellos, Internet como lo conocemos hoy en día simplemente no sería posible. Hoy veremos a fondo varios de los detalles más interesantes de los servidores web y su funcionamiento.

Quienes tengan conocimientos sobre lo que es un servidor no deben confundirlo con un servidor web, porque son dos cosas distintas, aunque sí es cierto que uno forma parte del otro, ya que de hecho el servidor web es uno de los componentes de un servidor. El server (o servidor) es el equipo en el cual se alojan los sitios o aplicaciones web, mientras que el servidor web es un software que forma parte del servidor, es el software que se encarga de despachar el contenido de un sitio web al usuario."

2.8.1.3. Para que sirve un servidor WEB.

Como ya habíamos comentado, la principal tarea que tiene un servidor web es la de despachar el contenido de un sitio web al usuario. Esto se logra mediante un proceso que a nuestros ojos no toma más que un segundo, pero a nivel del server es una secuencia más sofisticada de lo que parece.

2.8.1.4. Servidores WEB más utilizados.

Según (Borges S. , 2002-2020). indicia que “Entre los servidores web más utilizados del mundo podemos encontrar algunos como Apache, Nginx, LiteSpeed & IIS. Los primeros tres son predominantes en sistemas Linux, mientras que IIS está orientado para entornos Windows.”

- Apache: fue, durante casi 2 décadas, el webserver más utilizado del mundo, aunque en los últimos años ha perdido bastante terreno frente a rivales como Nginx o IIS. Aun así, sigue siendo un servidor web sólido, seguro, eficaz y fácil de configurar, sin mencionar que sigue siendo la opción predefinida para los servidores que corren cPanel, el panel de control más popular del mercado.
- Nginx: es un webserver que ha tenido un crecimiento increíble en cuestión de unos pocos años, al punto de que actualmente está por delante de Apache. Considerado por muchos como el web server más rápido hoy en día, su alta capacidad para despachar contenido, su seguridad y solidez lo convierten en la opción número 1 de muchos administradores de sistemas.
- LiteSpeed: es otro de los grandes webservers que podemos encontrar en el mercado. Si bien se trata de un software de pago, este servidor web ha demostrado que tiene un gran potencial. Combinando las reglas y flexibilidad de Apache y la velocidad y seguridad de Nginx, LiteSpeed se está abriendo camino como una alternativa muy sólida, rápida y segura. Su compatibilidad con cPanel también hace que sea popular entre servidores que utilizan dicho panel y que necesitan un mejor rendimiento que el brindado por Apache.
- IIS: se ha convertido en poco tiempo en el webserver más utilizado del mundo. Desarrollado por Microsoft, IIS es el servidor web que viene integrado por defecto en

servidores que corren Windows Server. Si bien es muy diferente a sus rivales de Linux, no deja de ser un webserver seguro, rápido y fácil de manejar.

2.8.1.5. Aplicaciones populares que corren en servidores WEB.

Según (Borges S. , 2002-2020). indicia que "Previamente comentábamos que un servidor web puede interpretar el lenguaje de programación de un sitio para poder despachar el contenido al navegador que le envía la solicitud. En otras palabras, los servidores web se caracterizan por ser compatibles con múltiples lenguajes de programación, entre los que podemos encontrar por ejemplo a PHP, ASP, Perl, Python, Ruby.

- PHP: ha sido durante un largo tiempo (y por supuesto sigue siendo) el lenguaje de programación web más utilizado a nivel mundial, y no existe otro que tenga una cuota ni por asomo cercana. Su facilidad de aprendizaje y potencial lo han llevado al puesto número del ranking de los más utilizados, y parece que seguirá allí durante un largo tiempo más.
- ASP.NET: es una de las tecnologías más utilizadas en servidores Windows, y está orientado a la creación de contenido del tipo dinámico, web apps y XML. Suele ir de la mano con el servidor web de Microsoft, IIS, aunque actualmente está disponible también para entornos Linux, sin embargo, su uso allí no es elevado.
- Perl: es un lenguaje complejo, pero a su vez muy poderoso, y si sabemos usarlo es posible aplicarlo a tareas áreas muy diversas, como por ejemplo programación de redes, bioinformática y finanzas.
- Python: se trata de un lenguaje multiplataforma ampliamente usado, de código abierto y orientado principalmente al contenido dinámico. Es común utilizarlo cuando se requiere

de programación orientada a objetos y también tiene soporte para programación imperativa.

- Ruby: otro lenguaje de contenido dinámico, Ruby nace con fuertes inspiraciones de Perl y Python, resultando ser un lenguaje orientado a objetos y reflexivo. Cuando es utilizado en desarrollo web, se suele hacer junto al framework Ruby on Rails. Una característica particular es que, dependiendo de cómo lo utilicemos, puede que no sea necesario que vaya de la mano de un servidor HTTP, como sí es el caso de PHP.

Como hemos visto se puede escribir mucho sobre servidores web, en esta oportunidad nos hemos enfocado en varios puntos como lo es el concepto de servidor web y su utilidad, sus principales características, además vimos cuáles son los más utilizados, así como los lenguajes de programación más comunes con los que son compatibles."

2.8.2. Servidor de Correo Electrónico.

Según (Frutos, 2016). indicia que "los servidores de correo, mueven los e-mails a través de las redes corporativas (vía LANs y WANs) y a través de Internet. Para acceder a nuestros correos, necesitamos un cliente como por ejemplo Outlook. Aunque es verdad que muchos usan servicios webmail como Gmail que son clientes de correo electrónico y que proveen una interfaz para acceder al correo.

Un servidor de correo es el encargado de enviar y recibir mensajes de correo electrónico entre hosts, usuarios o servidores. Entre sus funciones se incluyen el procesado de los mensajes, filtrado, almacenamiento, envío, recepción y reenvío de correos."

Es una de las aplicaciones más populares en usar el protocolo TCP/IP, y que permite en cuestión de segundos comunicarnos con cualquier persona en otra parte del mundo, evitando así escribir cartas, hablar por teléfono o utilizar otros medios de comunicación no tan rápidos.

2.8.2.1. componentes de servidor de correos.

- Servidor SMTP: es el encargado de realizar el envío y transmisión de nuestros emails desde nuestro servidor de correo hacia el destino.
- Servidor POP: es quien recibe los mensajes en un equipo local mediante el protocolo POP, que almacena en el equipo los mensajes sin dejar copia en el servidor (por defecto).
- Servidor IMAP: actúa como anfitrión de un servidor de correo, el cual obtiene una copia del correo que hay actualmente en el servidor de correo.
- Cliente de Correo local: Mozilla Thunderbird, Microsoft Outlook, Opera Mail, Evolution y otros son el ejemplo de clientes de correo que corren en nuestros equipos locales, y que pueden recibir el correo tanto por POP como IMAP.
- Cliente de Correo web: estos son los llamados Webmail, es decir, software de cliente de correo que corre remotamente en el servidor, como ya mencionamos en ejemplos con Roundcube, Squirrelmail, y los clásicos Hotmail, Gmail, Yahoo mail, etc. Estos clientes utilizan el protocolo IMAP para mostrar los mensajes.

2.8.2.2. Tipos de servidores de correo electrónico.

Existen muchísimos tipos de servidores de correo electrónico en internet, y todos funcionan de forma diferente, pero tienen como misión lo mismo: facilitare él envió o recepción de mensajes.

2.8.2.3. Servidores de salida de correo.

Según (Borges E. , InfraNetworking, 2019). indicia que “SMTP: como ya vimos anteriormente, el protocolo SMTP se utiliza para enviar correo, por lo que suele considerarse como un servidor de salida de correo. Su configuración se realiza en clientes de correo locales y remotos. Sus puertos de salida de correo son el 25 por defecto, 26 como puerto SMTP alternativo, 587 como puerto alternativo adicional (sobre todo en servidores cPanel), y 465 para recibir correo por SMTPS, implementando un certificado SSL/TLS que cifra el correo entrante.”

2.8.2.4. Servidores de entrada de correo electrónico.

- IMAP: este es el protocolo de correo más utilizado en la actualidad, permite sincronizar dispositivos dejando una copia en el servidor. Lo único malo de esta forma de descargar correo es que aumenta el uso de espacio en disco en el servidor. El puerto estándar de IMAP es el 143 para recibir correo sin encriptación. Mientras que el correo encriptado IMAP bajo un SSL/TLS suele correr en puertos como el 993.
- POP: la versión 3 de POP es la más usada en la actualidad. Sirve como dijimos antes, para descargar el correo hacia el cliente y borrar la copia que se almacena en el servidor. Este modelo permite descargar el correo solo en un cliente, no permitiendo la movilidad entre dispositivos. Los puertos que utiliza POP generalmente son el 110, y el 995 cuando ciframos la conexión con un certificado SSL/TLS.
- Exchange: existe otro protocolo desarrollado por Microsoft que se suele utilizar en sus servicios de correo corporativo y aplicaciones (Microsoft Exchange Server y Office 365 por ejemplo). El modo de funcionar es similar a IMAP, a decir verdad, solo que además agrega herramientas colaborativas para los usuarios, suele usarse mucho en empresas.

Según (Borges E. , InfraNetworking, 2019). indicia que “Los servidores de correo electrónico son los grandes potenciadores de las comunicaciones electrónicas en Internet. Como pudimos ver hoy, existen muchos servidores de correo, pero todos ellos tienen el mismo fin, entregar y enviar correos electrónicos desde un host/servidor, hacia un destino a través de Internet.”

2.8.3. Servidor de Base de Datos.

Según (Frutos, 2016). indicia que “los servidores de bases de datos, que podríamos llamar la “élite de los servidores”. Estos surgen de la necesidad de las empresas de manejar grandes y complejos volúmenes de datos, al tiempo de requerir compartir la información con un conjunto de clientes.”

Hoy en día la utilización de bases de datos es algo fundamental en cualquier aplicación, y por lógica su uso se ha extendido en las empresas, tanto offline como online. Las aplicaciones web y de escritorio las usan para escribir, modificar y recuperar información de forma rápida.

Al comenzar a trabajar con bases de datos nos enfrentaremos a un concepto nuevo, el cual se conoce como servidor de base de datos.

2.8.3.1 ¿Qué es un servidor de base de datos?

Según (Borges E. , InfraNetworking, 2019). indicia que “También conocido como data base server o RDBMS (Relational DataBase Management Systems) en caso de bases de datos relacionales, es un tipo de software de servidor que permiten la organización de la información mediante el uso de tablas, índices y registros.”

Las bases de datos que existen dentro, sirven para gestionar y administrar inmensas cantidades de información, como sucede en casos de empresas, instituciones, universidades o

bancos, que almacenan datos de usuarios/clientes tales como direcciones, teléfonos, emails, ingresos, egresos, calificaciones, etc.

2.8.3.2. Funciones de un servidor de base de datos.

Mediante el uso de un cliente de base de datos, se puede acceder a la información que se guarda en las diferentes bases de datos. Una vez el cliente ha accedido mediante un usuario, contraseña y nombre de host, se le permiten realizar diferentes tareas, dependiendo del nivel de privilegios que posea.

Algunos usuarios tienen privilegios de administrador y pueden administrar por completo las bases de datos a las que se conectan, mientas que otros usuarios tienen privilegios parciales para solo leer datos (hacer consultas de lectura, también llamado SELECT).

Los motores de bases de datos modernos permiten simultaneidad de consultas, lo que significa que un usuario puede escribir en determinada tabla, mientras que otro hace lectura de datos, o también escribe al mismo tiempo, todos desde diferentes lugares geográficos incluso, Una vez que el cliente de base de datos termina la consulta, la conexión con el server finaliza.

2.8.3.3. Uso de Servidores de Base de Datos.

- Según (Borges E. , InfraNetworking, 2019). indicia que “Administración de registros de personas: el uso de software para registros médicos, así como fichas de perfiles de clientes en clínicas, centros de odontología y más, es algo muy común de ver.”
- Según (Borges E. , InfraNetworking, 2019). indicia que “Administración de documentos: sirve para organizar documentos de texto de diversa índole, algo muy usado en las diferentes empresas.”

- Según (Borges E. , InfraNetworking, 2019). indicia que “Administración contable e impositiva: el uso de base de datos en estudios contables mejora el manejo de facturas, pagos de impuestos, gastos, ingresos y egresos.”
- Según (Borges E. , InfraNetworking, 2019). indicia que “Indexación de sitios web: el caso más popular del mundo es Google con su inmensa base de datos para indexar, gestionar y modificar los aspectos de sitios webs en sus resultados.”
- Según (Borges E. , InfraNetworking, 2019). indicia que “Servir contenido dinámico: con el auge del servidor PHP y la programación web, se comenzaron a usar las bases de datos para servir datos de foros, CMS, administraciones de usuarios, gestores de contenidos (como WordPress) y más.”

2.8.3.4. Ejemplo de Servidor de Base de Datos.

- MySQL Server: Es un servidor de bases de datos de tipo relacional, es considerada por muchos como la base de datos más popular del mundo.
- PostgreSQL: Es un servidor de bases de datos de tipo relacional, es considerada por muchos como la base de datos más popular del mundo, Se caracteriza por ofrecer una gran estabilidad, robustez y velocidad a la hora de administrar los datos.
- Microsoft SQL Server: es el servidor de base de datos SQL relacional de Microsoft. Es muy popular entre usuarios de la plataforma Windows Server, debido a que ofrece una compatibilidad nativa con el lenguaje de programación ASP/ASP.NET, así como con toda la suite de desarrollo de aplicaciones de sistemas operativos Windows.
- MongoDB Server: Es software libre, y a diferencia de MySQL, PostgreSQL y los demás, no guarda datos en tablas, sino en estructuras BSON (muy parecidas a JSON) dinámicas,

algo que hace que su acceso sea rápido y fácil, Se caracteriza por ser multiplataforma, corriendo sin problemas en Windows, Linux, MacOS y Solaris.

Según (Borges E. , InfraNetworking, 2019). indicia que “En general, motores como MySQL o MariaDB son soluciones estandarizadas para el 90% de las bases de datos pequeñas o medianas.

MySQL ofrece un rendimiento bueno, es flexible y fácil de implementar. Usando buenas prácticas a nivel de rendimiento en tus consultas y formas de almacenar la información, puede llegar a tener un gran rendimiento.

Mientras que soluciones basadas en NoSQL como MongoDB cuando hay mucha escritura de datos, se requiere disponibilidad inmediata y cuando el crecimiento en disco es realmente rápido.”

2.8.4. Servidor de Proxy.

Según (FM, 2017). indicia que “Se trata de unos servicios que te pueden ayudar a mejorar tu privacidad cuando navegas por la red, y que a menudo suelen confundirse con unas redes VPN con las que se pueden conseguir resultados similares, pero que son mucho más completas al no centrarse únicamente en tu navegación.”

2.8.4.1 ¿Qué es un Servidor Proxy?

Según (Barbosa, 2020). indicia que “Los servidores proxy generalmente se usan como un puente entre el origen y el destino de una solicitud. En nuestra imagen, puedes ver que la computadora necesita pasar por el servidor proxy para acceder a Internet, y este es uno de los usos comunes de los servidores proxy.

Un proxy es un equipo informático que hace de intermediario entre las conexiones de un cliente y un servidor de destino, filtrando todos los paquetes entre ambos. Siendo tú el cliente, esto quiere decir que el proxy recibe tus peticiones de acceder a una u otra página, y se encarga de transmitírselas al servidor de la web para que esta no sepa que lo estás haciendo tú."

De esta manera, cuando vayas a visitar una página web, en vez de establecer una conexión directa entre tu navegador y ella puedes dar un rodeo y enviar y recibir los datos a través de proxy. La página que visites no sabrá tu IP sino la del proxy, y podrás hacerte pasar por un internauta de otro país distinto al tuyo.

2.8.4.2. La utilidad de Proxy.

Según (FM, 2017). indicia que "Los proxys son utilizados muy a menudo para acceder a servicios que tienen bloqueado su contenido en determinado país. Por ejemplo, si una web no ofrece determinado contenido en tu país, pero sí en otro, haciéndote pasar por un internauta de ese otro país puedes acceder a él."

Según (FM, 2017). indicia que "Como muchos de estos servicios de proxy bloquean también cookies, scripts y otros objetos que están alojados en las webs, también son útiles para poder navegar de una manera mucho más privada y anónima."

2.8.4.3. ¿Para qué sirve un Servidor Proxy?

Según (Barbosa, 2020). indicia que "En este caso, Proxy puede cumplir algunas de las siguientes funciones:"

- Control de acceso: es posible que los administradores del servidor proxy permitan que ciertos usuarios tengan o no acceso a Internet a través de restricciones en su propio inicio de sesión o direcciones IP, proporcionando al entorno una capa adicional de protección.

- Filtrado de contenido: al estar en el medio del camino, el servidor también permite, o no, el acceso a ciertos sitios. Entre las reglas que se pueden aplicar están aquellas para bloquear sitios web específicos, pudiendo llegar a bloquear categorías completas.
- Cache: otro uso muy común para Web Proxies es hacer que realicen la función de caché. Esto hace que el proxy, después de acceder a una página, almacene el contenido de la misma en su sistema. Después de eso, las otras solicitudes a esta misma página no tendrán que ir a Internet, porque el contenido ya está almacenado en la memoria del proxy.

2.8.4.4. Proxy Inverso.

Según (Barbosa, 2020). indicia que "Otro uso muy común son los servidores de proxy inverso, el origen de la conexión siempre estuvo dentro de la red, pasaba por el proxy hasta Internet. En el caso del proxy inverso, el origen de las solicitudes está en Internet y busca acceder a un servidor dentro del entorno."

Los proxys inversos se usan comúnmente para manejar solicitudes a servidores que alojan páginas web. Algunos de los beneficios de utilizarlos de esta manera son:

- Equilibrio de carga: debido a que la estructura del servidor proxy inverso le permite conectarse a varios servidores de destino, puede dirigir las solicitudes a cada uno de ellos sin sobrecargar ninguna. Como otra característica de seguridad, las solicitudes de Internet conocerán solo la dirección IP del proxy y no todos los servidores y páginas que tiene la compañía.
- Cache: los servidores proxy también se utilizan para optimizar las solicitudes entre origen y destino. El servidor proxy inverso almacena elementos de página almacenados en servidores internos, buscando actualizaciones de contenido de vez en cuando, para

que los servidores de página reciban incluso menos solicitudes de red, lo que les permite funcionar aún mejor.

2.8.5. Servidor DNS.

Según (Padilla). indicia que “Es un sistemas globalmente distribuido, escalable y jerárquico. Ofrece una base de datos dinámica asociado direcciones IP de computadoras, servicios o cualquier recurso conectado a internet o red privada con información de diverso tipo. Soporta tanto IPv4 como IPv6, y la información se almacena en forma de registros “Resource Records (RR)” de distintos tipos los cuales puede almacenar direcciones IP y otro tipo de información. Esta información se agrupa en zonas, que corresponden a un espacio de nombres o dominio y que son mantenidas por el servidor DNS autoritativo de la misma.”

Según (INTEF, 2012). indicia que “Un servidor DNS es un servidor que traduce nombres de dominio IPs y viceversa. En las redes TCP/IP, cada PC dispone de una dirección IP para poder comunicarse con el resto de PCs. Es equivalente a las redes de telefonía en las que cada teléfono dispone de un número de teléfono que le identifica y le permite comunicarse con el resto de teléfonos.”

Trabajar con direcciones IP es incómodo para las personas, ya que requeriría conocer en todo momento las direcciones IP de los equipos a los que queremos conectarnos. En su lugar utilizamos nombres de dominios que son más facies de recordar y utilizar como ejemplo www.googlle.es, etc.

Un servidor NS es un servidor que permite averiguar la IP de un PC a partir de su nombre. Para ello, el servidor DNS dispone de una base de datos en la cual se almacenan todas las direcciones IP y todos los nombres de los PCs pertenecientes a su dominio.

- Zona de búsqueda directa: las resoluciones de esta zona devuelven la dirección IP correspondiente al recurso solicitado realiza las resoluciones que esperan como respuesta la dirección IP de u determinado recurso.
- Zona de búsqueda inversa: las resoluciones de esta zona buscan un nombre de equipo en función de su dirección IP; una búsqueda inversa tiene forma de pregunta del estilo "¿Cuál es el nombre DNS del equipo que utiliza la dirección IP 192.168?0.20?"
- Reenviador DNS: Servidor DNS designado por otros servidores DNS internos para su uso en consulta para resolver nombres de dominio DNS externos o fuera del dominio local.

  Linux dispone de varios paquetes de software que permite poner en marcha un servidor DNS. En este capítulo hablaremos e dos de ellos: el paquete "dnsmasq" que es un sencillo servidor DNS ideal para redes pequeñas como las que podeos encontrar en los centros educativos y el paquete "bind" que es un completo servidor DNS utilizando por muchos servidores DNS en internet.

2.8.5.1. Integrantes de DNS.

- Según (INTEF, 2012). indicia que "Espacio de dominio de nombres: Consiste en una estructura jerárquica de árbol donde cada nodo contiene cero o más registros (Resource Records, o RR) con información del dominio. Del nodo raíz, situado en el nivel más alto, parten las ramas que conforman las mencionadas zonas. Estas, a su vez, pueden contener uno o más nodos o dominios que a su vez pueden dividirse en subdominios según se baja en la jerarquía."
- Según (INTEF, 2012). indicia que "Servidores de Nombres: Son servidores encargados de mantener y proporcionar información del espacio de nombres o dominios. Por una

parte, existen servidores que almacenan información completa para uno o varios conjuntos del espacio de nombres (dominios) y de las cuales es responsable. Se dice que son servidores autoritativos de esas zonas/dominios en cuestión. Por otro lado, hay otro tipo de servidor que almacena conjuntos de registros de distintas zonas/dominios que obtiene consultando a los correspondientes servidores autoritativos de las mismas (búsquedas recursivas). Esta información la almacenan localmente de forma temporal (caché) y la renuevan periódicamente. Son los llamados servidores caché. Con los servidores de nombres y su intercomunicación se consigue la distribución y redundancia del espacio de dominios. Con esta organización de servidores de nombres, y su intercomunicación, se consigue la distribución y redundancia del espacio de dominios."

- Según (INTEF, 2012). indicia que "Resolvers: Son servidores caché o programas cliente los cuales se encargan de generar las consultas necesarias y obtener la información solicitada para ofrecerla al usuario que la solicita."

2.8.5.2. Amenazas y vulnerabilidades en DNS.

Según (Padilla). indicia que "En un entorno DNS se identifican varios puntos donde posibles ataques pueden desarrollarse. Estos puntos o "vectores de ataque" se sitúan tanto localmente en el propio servidor DNS y red local, como en las comunicaciones entre servidores y clientes."

- Amenazas locales: En la prevención de las amenazas locales, la solución más sencilla es la implementación de medidas y políticas de seguridad en la red interna. Mecanismos anti-spoofing, IDS/IPS7, así como la protección de los canales de acceso a los servidores y sus archivos sentarán la línea base de protección en esta área.
- Amenazas Servidor-Servidor: Actualizaciones dinámicas. Presentes cuando el tamaño de la organización o el número de servidores a administrar obliga a centralizar la

administración de los datos a través de DDNS (Dynamic DNS). Una opción válida para asegurar la comunicación sería dedicar un canal de comunicación restringido y/o implementar TSIG.

- Amenazas Servidor Master – Servidor Esclavo: Transferencias de zona. Cuando una organización cuenta con servidores esclavos, tiene la necesidad de ejecutar transferencias de zona maestro/esclavo. En estos casos la solución a considerar es la implementación de TSIG (Transaction SIGnature), de modo que las operaciones de transferencia de zona se firmen con una clave conocida por ambas partes. Adicionalmente la seguridad en las comunicaciones puede reforzarse usando SSL/TLS. Otras opciones pasarían por un canal de red privado para la transacción, o en caso extremo deshabilitarla y realizarla manualmente, lo cual no es una alternativa funcional.
- Amenazas Servidor Master – Servidor Cliente Cache/Resolver: Como se verá en el apartado Aleatoriedad del ID de transacción y puerto origen, las mejoras implementadas en las versiones recientes de Bind con la introducción de aleatoriedad en los puertos origen de la consulta, así como en los identificadores de mensaje, dificultan la posibilidad de envenenamiento de caché en los servidores DNS, pero, aun así, el ataque sigue siendo posible. La única solución considerada efectiva es adoptar DNSSEC.
- Amenaza Servidor – Cliente: En el flujo de información entre un cliente/resolver y un servidor master o caché, cabe la posibilidad de ataques locales para interceptar datos y de spoofing con objeto de suplantar al servidor DNS. Nuevamente, DNSSEC es la contramedida eficaz contra esta amenaza.

2.8.5.3. Debilidad en la Identificación y validación de mensajes DNS.

Según (Padilla). indicia que “Paralelamente al problema del uso del protocolo UDP en el transporte de mensajes DNS se añaden debilidades de diseño en el aspecto de la identificación y validación de los paquetes que favorecen la falsificación de los mismos.”

- Validación de respuestas: No obstante, el campo ID no es el único elemento que se comprueba al validar una respuesta y según se infiere del RFC10348, los mínimos requisitos para aceptar una respuesta son:
    - El puerto destino en el datagrama de respuesta debe ser el mismo que el puerto origen de la pregunta.
    - El ID del mensaje de respuesta debe ser el mismo que el ID del mensaje de pregunta.
    - El campo ANSWER debe referir el mismo recurso que el campo QUESTION.
    - La sección AUTHORITATIVE contiene los servidores autoritativos de la sección ANSWER.
- Identificador de mensaje ID: Debido a la escasa longitud destinada al campo ID del mensaje (16 bits) y a debilidades en la generación de la secuencia de los mismos, computacionalmente es relativamente sencillo construir un número suficiente de ID’s en un tiempo limitado para conseguir “acertar” con el ID original. Sin embargo, se han mejorado muchos aspectos en la fortificación del ID y otros valores en el mensaje DNS.

2.8.5.4. Fortificación de un Servicio DNS.

Se describen las medidas recomendadas para el bastionado y protección de un servicio DNS de forma genérica y con aplicación específica al software DNS Bind, el más usado mundialmente y actualmente en versión 9. Para ello se agrupan en tres capas los elementos que

integran el conjunto del servicio para dotar de una mayor granularidad la identificación de vectores de ataques y las medidas aplicables. Esta agrupación es la siguiente:

- Entorno Base: Elementos base del servicio a nivel de sistemas y comunicaciones.
    - Sistema Operativo
    - Software de Bind
    - Topología de Red
- Datos: Medidas en relación a la seguridad de los datos.
    - Parametrizaciones
    - Información de registros de zona
- Transacciones: protección de los mensajes en operaciones DNS.
    - Quieres (Consultas/Respuestas)
    - Transferencia de zona
    - Notificaciones
    - Actualizaciones Dinámicas

2.8.5.5. Configuración de Software.

- Control de Seguimiento del Software: Establecer una política de revisión del software para estar correctamente actualizado y al corriente de posibles vulnerabilidades o parches de seguridad. Se puede consultar el estado de las últimas versiones del software de BIND en el sitio Web del fabricante.
- Ocultar la versión: Deshabilitar directivas que puedan mostrar información sobre versión del software en ejecución. Esta información puede solicitarse con una consulta tipo TXT y clase CHAOS.

- Ejecutar el software DNS con un usuario No Privilegiado: El servicio de DNS no debe ejecutarse nunca como root o usuario privilegiado del sistema. Esta medida, unida al "enjaulado" del servicio en un entorno chroot, evitará posicionar al atacante en una situación de control del sistema en caso de ser comprometido.
- Asignación de Permisos: Asimismo, verificar la correcta asignación de permisos sobre los sistemas de ficheros y su contenido, evitando accesos no autorizados a configuraciones o ficheros de datos.
- Configuración de ficheros de Log: Configurar la recolección de logs a través de las directivas de logging en el fichero de configuración named.conf. Además, activar el envío a servidores remotos en la configuración de logs del sistema (por ejemplo, rsyslog. conf.).
- Arranque del servicio en el entorno restringido: Una vez configurado el entorno de chroot para Bind en /chroot/named, el servicio se debe arrancar tomando esa ruta como raíz.

2.8.5.6. Topología de Red.

Según (Padilla). indicia que "Una buena implementación de DNS debe separar siempre los servidores según su rol. Servidores autoritativos y cache recursivos serán dos componentes funcionales claramente diferenciados que requieren ser tratados de forma independiente en el diseño de la arquitectura de red."

Según (Padilla). indicia que "El diseño de la arquitectura de red es siempre un punto crítico a la hora de implementar un servicio accesible públicamente. En el caso de DNS, al ser por otra parte un elemento común a la estructura interna y externa de una organización es si cabe, aún más importante."

2.9. ALGORITMOS DE SEGURIDAD

Según (Montufar). indicia que “Un algoritmo es un procedimiento matemático o lógico para resolver un problema, Es un método para encontrar la respuesta correcta a un problema difícil. Para ello, el problema se divide en un numero especifico de pasos sencillos. Tiene un principio y un fin, aunque no un tamaño predeterminado.”

Según (Raffino, 2019). indicia que “En informática, un algoritmo es una secuencia de instrucciones secuenciales, gracias al cual pueden llevarse a cabo ciertos procesos y darse respuesta a determinadas necesidades o decisiones. Se trata de conjuntos ordenados y finitos de pasos, que nos permiten resolver un problema o tomar una decisión.”

Los algoritmos no tienen que ver con los lenguajes de programación, dado que un mismo algoritmo o diagrama de flujo puede representarse en diversos lenguajes de programación.

2.9.1. Partes de un Algoritmo.

Todo algoritmo debe constar de las siguientes partes

- Entrada (input): el ingreso de los datos que el algoritmo necesita para operar.
- Proceso: se trata de la operación lógica formal que el algoritmo emprenderá con lo recibido del input.
- Salida (Output): los resultados obtenidos del proceso sobre el (input), una vez terminada la ejecución del algoritmo.

2.9.2. ¿Para qué sirven un Algoritmo?

Según (Raffino, 2019). indicia que “Un algoritmo sirve para resolver paso a paso un problema. Se trata de una serie de instrucciones ordenadas y secuenciadas para guiar un proceso determinado.”

2.9.3. Tipos de Algoritmos.

Existen cuatro tipos de algoritmos en informática.

- Algoritmo computaciones.
- Algoritmo no computacional.
- Algoritmo cualitativo.
- Algoritmo cuantitativo.

2.9.3.1. Algoritmos computacionales.

Según (Virguez, 2019). indicia que “Los algoritmos computacionales representan una secuencia de pasos diseñados para llevar a cabo una tarea específica. También puede decirse que representan un conjunto de instrucciones claras que son programadas en un ordenador para poder solucionar un problema.”

2.9.3.1.1. Características de los Algoritmos Computacionales.

- Una secuencia de pasos limitada, que están definidos con claridad y cada uno es independiente del otro.
- Un agente (humano o inhumano) es el que aplica cada una de las etapas del proceso en un momento determinado.
- El agente tiene la capacidad de interpretar las instrucciones operacionales y al mismo tiempo guardar la información dada.
- Cuando se lleva a cabo una metodología específica, el resultado siempre va a ser el mismo en cada paso y en función de los datos iniciales.
- Como en todo proceso, culmina con un resultado.

Según (Virguez, 2019). indicia que “Tanto en informática como en otras disciplinas, se pueden identificar 3 tipos de algoritmos, los cuales son: secuenciales, condicionales y repetitivos. Además, existen aquellos que son cualitativos (utilizan palabras) y cuantitativos (usan cálculos numéricos).”

2.9.3.2. Algoritmos no computacionales.

Es un algoritmo que no requiere de una computadora para ser ejecutado.

2.9.3.3. Algoritmos cualitativos.

Según (Brito, 2008). indicia que “Un algoritmo es cualitativo cuando en sus pasos o instrucciones no están involucrados cálculos numéricos, las instrucciones para armar un aeromodelo, para desarrollar una actividad física o encontrar un tesoro.”

Los algoritmos cualitativos permiten dar solución a casos cotidianos en donde no es necesario utilizar operaciones matemáticas para llegar a dicha solución.

Ejemplo. Describir los pasos para ver una película en un cine

2.9.3.4. Algoritmos cuantitativos.

Según (Rojas, 2015). indicia que “Algoritmos cuantitativos a diferencia de los anteriores solucionan casos en donde es necesario el recubrir a las matemáticas para dar solución a dichos casos.

Ejemplo. Descubrir los pasos para sumas dos números.”

Según (robles, 2019). indicia que “Son lo contrario de los algoritmos cualitativos, porque se colocan elementos numéricos. Este tipo de algoritmos se utilizan en las matemáticas para realizar cálculos. Por ejemplo, para encontrar una raíz cuadrada o resolver una ecuación.”

2.10. PROTOCOLOS DE SEGURIDAD DE LA INFORMACION

Según (Cloud, 2015). indicia que “Cuando navegamos a través de internet nuestro navegador está intercambiando datos con las diferentes páginas web que visitamos. En ocasiones son datos que se comparten de forma automática, como nuestra dirección IP o nuestro historial de búsquedas, pero otras veces es información que damos de forma consciente como la tarjeta de crédito en una tienda online.”

2.10.1. Que es el protocolo de seguridad de la información.

Los protocolos de seguridad de red son un tipo de protocolo de red que garantiza la seguridad y la integridad de los datos en tránsito a través de una conexión de red como Internet. Están diseñados principalmente para evitar que usuarios, aplicaciones, servicios o dispositivos no autorizados accedan a los datos de la red. Esto se aplica a prácticamente todos los tipos de datos, independientemente del medio de red utilizado.

2.10.2. Tipo de Protocolos de Seguridad de la Información.

Estos son los protocolos más conocidos:

- Protocolo HTTP
- Protocolo FTP
- Protocolo SSH
- Protocolo DNS
- Protocolo de Base de Datos

2.10.3. Protocolo HTTP.

Según (Cloud, 2015). indicia que “El protocolo HTTP (Protocolo de transferencia de hipertexto) se basa en www (World Wide Web) que transmite mensajes por la red. Por ejemplo,

cuando un usuario ingresa al navegador e ingresa en la URL una búsqueda, la URL transmite los mensajes por HTTP al servidor web que el usuario solicitó. Luego, el servidor web responde y entrega los resultados de los criterios de búsqueda que había solicitado.”

Según (Bembibre, 2009). indicia que “El protocolo de este tipo opera con códigos de respuesta de tres dígitos, que comunican si conexión fue rechazada, si se realizó con éxito, si ha sido redirigida hacia otro URL, si existe un error por parte del cliente, o bien, por parte del servidor.”

Según (Bembibre, 2009). indicia que “Las aplicaciones y navegadores web tienden a complementar la acción del HTTP como ocurre, por ejemplo, con las denominadas "cookies", que permiten almacenar información de la sesión, función de la que no dispone este protocolo, ya que opera sin estado.”

2.10.4. Protocolo FTP.

Según (Cloud, 2015). indicia que “El protocolo FTP (protocolo de transferencia de archivos) se usa generalmente para transferir archivos a través de Internet. FTP usa un cliente-servidor para compartir archivos en una computadora remota. La forma en que funciona el FTP es como HTTP para enviar páginas web.”

Según (Arsys, 2015). indicia que “Para que pueda funcionar, FTP necesita establecer dos conexiones diferentes entre las partes, una de ellas para poder transferir los archivos y la otra para las respuestas y los comandos. Es el cliente el que realiza ambas conexiones, una que se abre y se cierra cada vez que se envían los archivos y otra sola y permanente utilizada para los comandos.”

2.10.5. Protocolo SSH.

Según (Cloud, 2015). indicia que “El protocolo SSH (Secure Socket Shell) proporciona una forma segura de acceder a internet a través de un ordenador remoto. SSH proporciona autenticación y encriptación entre dos computadoras que se conectan a Internet. SSH es bien utilizado por las administraciones de red para administrar sistemas por acceso remoto.”

Según (C., 2020). indicia que “Proporciona un mecanismo para autenticar un usuario remoto, transferir entradas desde el cliente al host y retransmitir la salida de vuelta al cliente. El servicio se creó como un reemplazo seguro para el Telnet sin cifrar y utiliza técnicas criptográficas para garantizar que todas las comunicaciones hacia y desde el servidor remoto sucedan de manera encriptada.”

2.10.5.1. Técnicas de Cifrado.

Según (C., 2020). indicia que “La ventaja significativa ofrecida por el protocolo SSH sobre sus predecesores es el uso del cifrado para asegurar la transferencia segura de información entre el host y el cliente. Host se refiere al servidor remoto al que estás intentando acceder, mientras que el cliente es el equipo que estás utilizando para acceder al host. Hay tres tecnologías de cifrado diferentes utilizadas por SSH:”

- Cifrado Simétrico
- Cifrado Asimétrico
- Hashing

2.10.5.1.1. Cifrado Simétrico.

Según (C., 2020). indicia que “El cifrado simétrico es una forma de cifrado en la que se utiliza una clave secreta tanto para el cifrado como para el descifrado de un mensaje, tanto por

el cliente como por el host. Efectivamente, cualquiera que tenga la clave puede descifrar el mensaje que se transfiere."

El cifrado simétrico a menudo se llama clave compartida (shared key) o cifrado secreto compartido. Normalmente sólo hay una clave que se utiliza, o a veces un par de claves donde una clave se puede calcular fácilmente con la otra clave.

2.10.5.1.2. Cifrado Asimétrico.

Según (C., 2020). indicia que "A diferencia del cifrado simétrico, el cifrado asimétrico utiliza dos claves separadas para el cifrado y el descifrado. Estas dos claves se conocen como la clave pública (public key) y la clave privada (private key). Juntas, estas claves forman el par de claves pública-privada (public-private key pair)."

2.10.5.1.3. Hashing.

Según (C., 2020). indicia que "El hashing unidireccional es otra forma de criptografía utilizada en Secure Shell Connections. Las funciones de hash unidireccionales difieren de las dos formas anteriores de encriptación en el sentido de que nunca están destinadas a ser descifradas. Generan un valor único de una longitud fija para cada entrada que no muestra una tendencia clara que pueda explotarse. Esto los hace prácticamente imposibles de revertir."

2.10.6. Protocolo DNS.

Según (Cloud, 2015). indicia que "El protocolo DNS (Sistema de nombres de dominio) mantiene un directorio de nombres de dominio traducidos a direcciones IP. El DNS rastrea al usuario para ubicar la dirección web en la dirección IP correspondiente. Por ejemplo, si un usuario ingresa la URL google.com, el servidor web no está leyendo el nombre google.com está leyendo la dirección IP NUMÉRICA que corresponde a google.com (208.65.155.84.)."

Según (Upgrade, 2019). indicia que “El protocolo DNS es el método que se utiliza en la actualidad como forma sencilla de recordar los nombres de dominio en lugar de la IP a la que apuntan haciendo que los usuarios accedan más fácilmente a las webs.”

Según (Upgrade, 2019). indicia que “Para los usuarios es más fácil escribir www.nombrededominio.com que una IP como 123.45.678.90. Resulta mucho más sencillo acceder a las páginas webs escribiendo el dominio, siempre más fácil de memorizar y recordar que una secuencia numérica; todo eso es posible gracias al sistema DNS.”

2.10.7. Protocolo Base de Datos.

Un protocolo es una serie de reglas que utilizan dos ordenadores para comunicarse entre sí. Con los programas que hay actualmente el problema a la conexión de base de datos es más practico ya que buenas bases de datos proporcionan una gestión sectorial que evitan las repeticiones, permiten la ordenación protocolaria.

2.10.7.1. Cadena de Conexión.

Según (Perez L. , 2016). indicia que “Las cadenas de conexión son la representación en texto de las propiedades de conexión para un proveedor de datos. La cadena de conexión puede ser de dos formas distintas.”

- En la primera no hay que indicar ni usuario ni password.
- En la segunda sí que hay que indicar esos dos datos.

2.11. PUERTOS

Según (Alexalvarez0310, 2009). indicia que “Los puertos se indican por números, y cuando los servicios se refieren a la Web, van incluidos en la sintaxis de la mayoría de las ULRs. Para que sea posible utilizar un servicio de un servidor es necesario que el puerto

correspondiente del servidor sea el correcto y que esté habilitado. Se podría decir que el servidor debe estar “escuchando” por dicho puerto. “

2.11.1. Puertos bien conocidos 1-1023.

Según (Sanz, 2013). indicia que “Son puertos reservados para el sistema operativo y usados por “protocolos bien conocidos” como por ejemplo HTTP (servidor WEB), POP3/SMTP (Servidor de E-Mail) y TELNET. Si queremos usar uno de estos puertos tendemos que arrancar el servicio que los use teniendo permisos de administrador.”

- ✓ 21 TCP FTP
- ✓ 21 UDP FTP
- ✓ 22 TCP SSH
- ✓ 22 UDP SSH
- ✓ 23 TCP Telnet
- ✓ 23 UDP Telnet
- ✓ 25 TCP SMTP
- ✓ 25 UDP SMTP
- ✓ 66 TCP Oracle SQLNet
- ✓ 66 UDP Oracle SQLNet
- ✓ 79 TCP Finger
- ✓ 79 UDP Finger
- ✓ 80 TCP HTTP – Web Aliens vs. Predator
- ✓ 80 UDP HTTP – Web
- ✓ 107 TCP Remote Telnet Service
- ✓ 107 UDP Remote Telnet Service
- ✓ 110 TCP POP3
- ✓ 110 UDP POP3
- ✓ 118 TCP SQL Services
- ✓ 118 UDP SQL Services
- ✓ 119 TCP NNTP – Grupos de Noticias
- ✓ 119 UDP NNTP – Grupos de Noticias
- ✓ 137 TCP NetBios Name Service
- ✓ 137 UDP NetBios Name Service
- ✓ 138 TCP NetBios Datagram Service
- ✓ 138 UDP NetBios Datagram Service
- ✓ 139 TCP NetBios Session Service
- ✓ 139 UDP NetBios Session Service
- ✓ 150 TCP SQL-Net

- ✓ 150 UDP SQL-Net
- ✓ 161 TCP Snmp
- ✓ 194 TCP Internet Relay Chat
- ✓ 194 UDP Internet Relay Chat
- ✓ 209 TCP Quick Mail Protocol
- ✓ 209 UDP Quick Mail Protocol
- ✓ 217 TCP dBASE Unix
- ✓ 217 UDP dBASE Unix
- ✓ 389 TCP NetMeeting
- ✓ 407 TCP Timbuktu pro
- ✓ 407 UDP Timbuktu pro
- ✓ 443 TCP HttpS
- ✓ 445 TCP Microsoft-Ds (compartir archivos en win 2000)
- ✓ 515 TCP printer
- ✓ 522 TCP NetMeeting
- ✓ 531 TCP Conference
- ✓ 531 UDP Conference
- ✓ 568 TCP Microsoft Shuttle
- ✓ 568 UDP Microsoft Shuttle
- ✓ 569 TCP Microsoft Rome
- ✓ 569 UDP Microsoft Rome
- ✓ 666 TCP doom ID Software
- ✓ 666 UDP doom ID Software
- ✓ 700 UDP Buddy Phone
- ✓ 701 UDP Buddy Phone
- ✓ 992 TCP Telnet SSL
- ✓ 992 UDP Telnet SSL
- ✓ 993 TCP IMAP4 SSL
- ✓ 993 UDP IMAP4 SSL
- ✓ 995 TCP POP3 SSL
- ✓ 995 UDP POP3 SSL

2.11.2. Puertos registrados 1024-49151

Según (Sanz, 2013). indicia que “Son denominados Registrados y pueden ser usados por cualquier aplicación. Existe una lista publica en la web del IANA donde se puede ver que protocolo que usa cada uno de ellos”

- ✓ 1024–5000 TCP Dwyco Video Conferencing
- ✓ 1414 UDP CuSeeMe
- ✓ 1417 TCP Timbuktu pro
- ✓ 1417 UDP Timbuktu pro
- ✓ 1418 TCP Timbuktu pro

- ✓ 1418 UDP Timbuktu pro
- ✓ 1419 TCP Timbuktu pro
- ✓ 1419 UDP Timbuktu pro
- ✓ 1420 TCP Timbuktu pro
- ✓ 1420 UDP Timbuktu pro
- ✓ 1424 UDP CuSeeMe
- ✓ 1547 TCP LapLink
- ✓ 1720 TCP NetMeeting CuSeeMe
- ✓ 1731 TCP NetMeeting
- ✓ 1812 UDP CuSeeMe
- ✓ 1813 UDP CuSeeMe
- ✓ 2300 TCP Everquest
- ✓ 2300 UDP Everquest Age off Empires
- ✓ 2300 – 2400 TCP Battlecom
- ✓ 2300 – 2400 UDP Battlecom Aliens vs. Predator
- ✓ 2301 TCP Age off Empires
- ✓ 2301 UDP Age off Empires
- ✓ 2302 TCP Age off Empires
- ✓ 2302 UDP Age off Empires
- ✓ 2303 TCP Age off Empires
- ✓ 2303 UDP Age off Empires
- ✓ 2304 TCP Age off Empires
- ✓ 2304 UDP Age off Empires
- ✓ 2305 TCP Age off Empires
- ✓ 2305 UDP Age off Empires
- ✓ 2306 TCP Age off Empires
- ✓ 2306 UDP Age off Empires
- ✓ 2307 TCP Age off Empires
- ✓ 2307 UDP Age off Empires
- ✓ 2308 TCP Age off Empires
- ✓ 2308 UDP Age off Empires
- ✓ 2309 TCP Age off Empires
- ✓ 2309 UDP Age off Empires
- ✓ 2310 TCP Age off Empires
- ✓ 2310 UDP Age off Empires
- ✓ 2311 TCP Age off Empires
- ✓ 2311 UDP Age off Empires
- ✓ 2400 TCP Everquest Age off Empires
- ✓ 2611 TCP Black and White
- ✓ 2612 TCP Black and White
- ✓ 3000 TCP Active Worlds
- ✓ 3000 UDP Calista IP phone (saliente)
- ✓ 3100-3999 TCP Delta Force
- ✓ 3100-3999 UDP Delta Force

- ✓ 3128 TCP Squid Proxy
- ✓ 2301 TCP Age off Empires
- ✓ 3389 TCP Windows 2000 Terminal Server
- ✓ 3389 UDP Windows 2000 Terminal Server
- ✓ 3568 UDP Delta Force 2
- ✓ 3569 UDP Delta Force 2
- ✓ 4000 TCP Diablo II ICQ
- ✓ 4099 TCP AIM Talk
- ✓ 4661 TCP Edonkey 2000
- ✓ 4662 TCP Edonkey 2000 Overnet
- ✓ 4662 UDP Overnet
- ✓ 4665 UDP Edonkey 2000

2.11.3. Puertos dinámicos 49152-65535.

Son denominados dinámicos o privilegiados normalmente se asignan en forma dinámica a las aplicaciones de clientes al iniciarse la conexión. Se utiliza en conexiones peer to peer.

2.12. SEGURIDAD

Según (Jimenez, 2017). indicia que "Existen diferentes definiciones del término seguridad informática. De ellas nos quedamos con la definición ofrecida por el estándar para la seguridad de la información ISO/IEC 27001, que fue aprobado y publicado en octubre de 2005 por la International Organizations for Standardization (ISO) y por la comisión International Electrotechnical Commission (IEC)."

Según (Significados.com., 2017). indicia que "Seguridad también se entiende como una medida de asistencia, subsidio o indemnización. En este contexto, existen algunas palabras con significado similar como estabilidad, garantía, protección, asilo, auxilio, amparo, defensa y fianza. Del mismo modo, palabras opuestas serían desprotección y desamparo."

- Seguridad Social
- Seguridad en el trabajo

- Seguridad industrial
- Seguridad privada

Según (micarrerauniversitaria.com, 2019). indicia que “Los inconvenientes de seguridad en los equipos de informática que se hacen presente dentro de las instituciones, tienen que ver con las intromisiones, hurto de información, dificultades con los virus, etc.; sumado a la falta de legislación informática donde se caractericen las infracciones informáticas.”

- Estudia riesgos del sistema informático, definir su vulnerabilidad e instalar los dispositivos de salvaguarda que garanticen la confidencialidad, integridad y disponibilidad de la información.
- Organiza la seguridad y clasificación de los recursos.
- Oriente la Seguridad física y del entorno.
- Establece la protección e inspección de acceso al sistema.
- Seguridad en la operación y producción.
- Seguridad en el software: sistemas operativos, bases de datos y aplicaciones.
- Seguridad en los operadores.
- Aplica las especificaciones de seguridad a los fines de que los sistemas informáticos respeten las normas estándar de seguridad.
- Diseña la seguridad del sistema informático siguiendo las normas.
- Lidera proyectos de Seguridad basados en las normas estándar, que posibiliten obtener acreditaciones de seguridad exigidas por la ley.
- Vigila la observancia legal de los sistemas informáticos empleados en la organización: datos personales, propiedad intelectual, software legal, etc.

2.12.1. Seguridad en centros de Cómputo.

- Según (Jimenez, 2017). indicia que “Seguridad lógica: Consiste la seguridad lógica en la aplicación de barreras y procedimientos que resguarden el acceso a los datos y sólo se permita acceder a ellos a las personas autorizadas expresamente para hacerlo. Existe un viejo dicho en la seguridad informática: Todo lo que no está permitido debe estar prohibido; y esto es lo que debe asegurar la seguridad lógica.

  Hablar de seguridad lógica, pues, es hablar de seguridad de la información, y el valor subjetivo que esta tiene, resultando que el bien a proteger son los datos que tienen, manejan y disponen una determinada empresa. Las nuevas tecnologías, sin duda alguna, han modificado este aspecto en los últimos años a una velocidad sorprendente.”
- Según (Jimenez, 2017). indicia que “Seguridad física: Cuando hablamos de seguridad física entramos en un sector que engloba una lista de amenazas muy amplia. Dentro de esta categoría encontramos sistemas informáticos, vehículos, mobiliario, desastres naturales, sabotajes o acciones hostiles por parte de otras personas.”

  Creemos que la mejor acción de seguridad es la prevención, servicios de seguridad física que recomendamos:

  - Biométrico, control de huella digital.
  - Control de presencia para la gestión del personal.
  - Instalación y mantenimiento de control de acceso.
  - Barreras de acceso y puertas automáticas mecánicas.
- Según (Valenzuela, 2011). indicia que “Seguridad en la utilización de equipos: Es el conjunto de métodos, documentos, programas y dispositivos físicos destinados a lograr

que los recursos de computó disponibles en un ambiente dado, sean accedidos y exclusivamente por quienes tienen la autorización para hacerlo."

- Privacidad: la información debe ser vista y manipulación principalmente por quienes tienen el derecho o la autoridad de hacerlo.
- Integridad: la información debe ser consistente.

- Según (Wikipedia, Wikipedia, 2020). indicia que "Seguridad al restaurar equipos: En Restaurar sistema, el usuario puede crear un punto de restauración manualmente, elegir un punto existente para restaurar el sistema o cambiar la configuración. Por otra parte, la restauración en sí puede deshacerse posteriormente. Los puntos de restauración viejos se eliminan para evitar que el disco duro se llene. Restaurar sistema respalda archivos de sistema con ciertas extensiones (.dll, .exe, etc.), y los guarda para posterior restauración y uso. También respalda el Registro y la mayoría de controladores."

2.12.2. Tipos de Seguridad.

Existen diversos tipos de seguridad informática que una empresa debe vigilar para evitar pérdida de datos y/o prestigio.

2.12.2.1. Seguridad de Hardware.

Según (U.I.V., 2018). indicia que "La seguridad de hardware se puede relacionar con un dispositivo que se utiliza para escanear un sistema o controlar el tráfico de red, Los ejemplos más comunes incluyen cortafuegos o firewalls de hardware y servidores proxy."

De entre los diferentes tipos de seguridad informática, son los sistemas de hardware los que pueden proporcionar una seguridad más robusta, además de que también pueden servir como capa adicional de seguridad para los sistemas importantes.

2.12.2.2. Seguridad de Software.

Según (U.I.V., 2018). indicia que “La seguridad de software se utiliza para proteger el software contra ataques maliciosos de hackers y otros riesgos, de forma que nuestro software siga funcionando correctamente con este tipo de riesgos potenciales. Esta seguridad de software es necesaria para proporcionar integridad, autenticación y disponibilidad. Entre los tipos de seguridad informática, este campo de la seguridad de software es relativamente nuevo.”

Los defectos de software tienen diversas ramificaciones de seguridad, tales como errores de implementación, desbordamientos de buffer, defectos de diseño, mal manejo de errores, etc. Con demasiada frecuencia, intrusos maliciosos pueden introducirse en nuestros sistemas mediante la explotación de algunos de estos defectos de software. Las aplicaciones que tienen salida a Internet presentan además un riesgo de seguridad más alto.

2.12.2.3. Seguridad de Red.

Según (U.I.V., 2018). indicia que “La seguridad de red se refiere a cualesquiera actividades diseñadas para proteger la red. En concreto, estas actividades protegen la facilidad de uso, fiabilidad, integridad y seguridad de su red y datos. La seguridad de red efectiva se dirige a una variedad de amenazas y la forma de impedir que entren o se difundan en una red de dispositivos. Muchas amenazas a la seguridad de la red hoy en día se propagan a través de Internet.” Los más comunes incluyen:

- Virus, gusanos y caballos de Troya
- Software espía y publicitario
- Ataques de día cero, también llamados ataques de hora cero
- Ataques de hackers
- Ataques de denegación de servicio

- Intercepción o robo de datos
- Robo de identidad

2.13. INFRAESRUCTURA

Según (Saavedra, 2018). indicia que “El servicio que ofrece el conjunto de dispositivos y aplicaciones necesarios para una empresa, es conocido como infraestructura IT. Este sistema se gestiona a través de la monitorización mediante el despliegue de los equipos suficientes, máquinas y software para el cliente.”

Según (XERALNET, 2018). indicia que “Se podría definir como el conjunto de elementos para el almacenamiento de los datos de una empresa. En ella se incluye el hardware, el software y los diferentes servicios necesarios para optimizar la gestión interna y seguridad de información.”

2.13.1. Elementos de la Infraestructura.

Según (Saavedra, 2018). indicia que “Son cuatro los elementos que forman la infraestructura tecnológica IT:”

- Servidores: existen distintos tipos de servidores en función de las necesidades de las empresas y el tamaño de estas.
- Almacenamiento: son diferentes soluciones de almacenamiento las que pueden aplicarse, entre otras, las hiperconvergentes, cabinas de almacenaje y los dispositivos NAS como posibles copias de seguridad.
- Networking: esto permite distintas funcionalidades al sistema sin correr riesgos de seguridad. La agilidad y la flexibilidad hacen aumentar la visibilidad en las redes.

- Seguridad: este elemento proporciona seguridad informática a la empresa y facilita el acceso a los datos en caso de pérdida o un ataque al sistema.

2.13.2. Infraestructura Hardware.

Es toda la parte física necesaria para el desarrollo de una actividad: ordenadores, monitores, videocámaras, routers, Wi-Fi, teléfonos, sensores, escáneres, impresores, cableado.

2.13.3. Infraestructura Software.

Según (XERALNET, 2018). indicia que "Son los sistemas y programas que facilitan el funcionamiento de otras aplicaciones. Existen dos tipos fundamentales: los sistemas operativos y los programas informáticos como bases de datos, procesadores de texto, herramientas de ofimática."

Es importante disponer de un equipo de servidores de calidad para garantizar que las aplicaciones corporativas funcionen correctamente, como por ejemplo el correo electrónico o la gestión de dominios. Asimismo, interviene en toda la gestión eficaz del entorno informático.

2.14. INFORMACION

Según (Significados, 2017). indicia que "Como información denominamos al conjunto de datos, ya procesados y ordenados para su comprensión, que aportan nuevos conocimientos a un individuo o sistema sobre un asunto, materia, fenómeno o ente determinado."

Según (Significados, 2017). indicia que "La consecuencia más importante de la información es cambiar el estado de conocimiento que un individuo o sistema maneja con respecto a determinado fenómeno o cuestión, todo lo cual influirá en las acciones, actitudes o decisiones que se tomen a partir de la nueva información."

- La información debe tener cierto grado de utilidad.

- La información deberá poseer vigencia o actualidad.
- la información deberá ser confiable.

Tipos de información:

- Información ad perpetuam: En Derecho, se conoce la información que se hace para perpetua memoria, es decir, para que conste en lo sucesivo en las acciones judiciales que tengan lugar.
- Información Financiera: Como información financiera se denomina el conjunto de datos relativos a la situación económica de una persona, una entidad, un mercado o un país, y que se emplea con la finalidad de analizar su solidez y liquidez, y establecer parámetros que permitan tomar decisiones relativas a operaciones comerciales o inversiones.
- Información en Informática: En la Informática, como información se denomina el conjunto de datos organizados y procesados que funcionan como mensajes, instrucciones y operaciones o cualquier otro tipo de actividad que tenga lugar en una computadora.
- Información privilegiada: Se denomina información privilegiada aquella que es exclusiva de un grupo de personas o empresas, y que proporciona ciertas ventajas competitivas a quienes la posean.

2.14.1. Dato.

Según (Significados.com, 2017). indicia que “Los datos representan un fragmento de una cantidad, medida, descripción o palabra, los cuales son agrupados o clasificados de una determinada manera para generar de información.”

Según (Significados.com, 2017). indicia que “En informática, los datos alimentan todo el sistema. La identificación de los datos es generada por el sistema de estructura de datos del programa informático. La representación de estos datos son los que inciden en la creación de algoritmos o instrucciones.”

Algunas de las formas para la recopilación de datos son hechas por:

- Encuestas
- Datos estadísticos

En informática, los datos se diferencian de la información por el grado de relevancia y utilidad vigente. Los datos, por ejemplo, pueden ser números, palabras o variables, en cambio, la información son estos datos procesados para que haga sentido en un contexto específico.

En programación, los tipos de datos es la forma en que se clasifican para ser usados para la generación de un proceso, programa o instrucción.

Los tipos de datos se clasifican en:

- Datos numéricos: comporta todos los tipos de números sean ellos enteros, decimales, reales o exponenciales.
- Datos alfanuméricos: son caracteres alfabéticos, numéricos o especiales que no son usados para operaciones matemáticas. También se incluye lo que se llaman cadenas que son datos más extensos como, por ejemplo, la dirección de alguien.
- Datos lógicos: responden a la pregunta con un verdadero (true) o falso (false).

2.15. VULNERAVILIDAD

Según (INCIBE, 2017). indicia que “Una vulnerabilidad (en términos de informática) es una debilidad o fallo en un sistema de información que pone en riesgo la seguridad de la información pudiendo permitir que un atacante pueda comprometer la integridad, disponibilidad o confidencialidad de la misma, por lo que es necesario encontrarlas y eliminarlas lo antes posible. Estos «agujeros» pueden tener distintos orígenes, por ejemplo: fallos de diseño, errores de configuración o carencias de procedimientos.”

Por tanto, las vulnerabilidades son las condiciones y características propias de los sistemas de una organización que la hacen susceptible a las amenazas.

2.15.1. Tipo de Vulnerabilidades.

Según (Dongee, 2018). indicia que “cualquier investigador experimentado o simplemente un hacker con gran recorrido en la materia pueden hacer uso de sus conocimientos para encontrar los errores de una web y vulnerarlo con técnicas empleadas.”

- CLICKJACKING: Según (Dongee, 2018). indicia que “Este tipo de ataques se aplica más que todo en páginas como Facebook y Twitter, lo que permite realizar acciones de redirección en la web de la víctima. Al utilizar el clickjacking el hacker utiliza diferentes capas transparentes o en marca de agua para poder engañar al usuario para que cliquee en un determinado botón o enlace en otro sitio cuando pretendía hacer clic en la página de nivel superior.”
- CROSS SITE SCRIPTING (XSS): Según (Dongee, 2018). indicia que “También conocido como Cross Site Scripting (CSS), es una vulnerabilidad bastante empleada y que se encuentra en la mayoría de las aplicaciones web. Esto le permite al hacker insertar

un código malicioso dentro de las páginas que visitan los internautas para así evitar el acceso al site o poner en práctica el phishing.”

- FALSIFICACIÓN DE SOLICITUDES ENTRE SITIOS/CSRF: Según (Dongee, 2018). indicia que “Este tipo de ataque también se conoce como sesión montada o ataque con un solo clic y se abrevia con las siglas CSRF o XSRF. Esta vulnerabilidad se transmite a través de comandos no autorizados.”
- EJECUCIÓN REMOTA DE CÓDIGO: Según (Dongee, 2018). indicia que “Esta vulnerabilidad es una de las más conocidas y utilizadas por los hackers. A través de la ejecución de códigos, el pirata cibernético podrá conocer los errores que puede tener el sitio e implantar un malware, que a su vez explotará la vulnerabilidad de la página web y le facilitará al delincuente la ejecución de código de manera remota, trayendo como consecuencia que el hacker tenga el control absoluto sobre el sistema informático de la web.”
- INCLUSIÓN DE ARCHIVOS LOCALES (LFI) E INCLUSIÓN DE ARCHIVOS REMOTOS (RFI): Según (Dongee, 2018). indicia que “La vulnerabilidad de inclusión de archivos es un problema que se puede conseguir generalmente afectando las aplicaciones que dependen de un tiempo de ejecución de secuencias de comandos. Esta vulnerabilidad es producida cuando una app web crea una ruta al código ejecutable utilizando una variable controlada por el atacante de una manera que le permite controlar qué archivo se ejecuta en el tiempo de ejecución.”
- ATAQUE DE INYECCIÓN SQL: Según (Dongee, 2018). indicia que “Este tipo de ataque es una técnica que emplea la inyección de códigos para explotar la vulnerabilidad de un determinado sitio web. Se utiliza comúnmente para atacar aplicaciones que son

controladas únicamente por datos, donde se colocan sentencias de SQL en un campo de entrada para su ejecución."

- VULNERABILIDAD DE REDIRECCIÓN DE URL: Según (Dongee, 2018). indicia que "Esta vulnerabilidad funciona como una aplicación que toma un parámetro específico y re-direcciona a los usuarios a sitios sin ninguna validación. Es utilizada ampliamente en los ataques conocidos como phishing, donde los usuarios son engañados y caen dentro de un sitio web malicioso."

2.15.2. Errores más frecuentes.

Según (Rosell, 2017). indicia que "En los últimos años se ha avanzado mucho en el ámbito de la ciberseguridad, pero todavía las pequeñas y medianas empresas y, sobre todo, las que se acaban de crear, siguen descuidando ciertos aspectos que podrían poner en serio peligro la continuidad de sus negocios. Falta perspectiva real de los peligros que les pueden amenazar y de las consecuencias que podrían conllevar."

- Instalar un antivirus o un cortafuego.
- Creer que la información de su negocio no interesa a nadie.
- Considerar que los informáticos son los únicos responsables de la ciberseguridad.
- Considerar que la ciberseguridad no requiere un mantenimiento.
- No firmar acuerdos de confidencialidad.
- Incumplimiento de la LOPD (Ley Orgánica de Protección de Datos).
- Falta de seguridad en los contratos.
- Falta de seguridad de la red y los sistemas.
- Pensar que una amenaza a la empresa siempre vendría de un "tercero".
- Ofrecer servicios a través de Internet y olvidar la ciberseguridad.

2.16. LINUX

Según (Wikipedia, Wikipedia, 2020). indicia que “Una distribución GNU/Linux (coloquialmente llamada distro) es una distribución de software basada en el núcleo Linux que incluye determinados paquetes de software para satisfacer las necesidades de un grupo específico de usuarios, dando así origen a ediciones domésticas, empresariales y para servidores. Por lo general están compuestas, total o mayoritariamente, de software libre, aunque a menudo incorporan aplicaciones o controladores propietarios.”

2.16.1. Por qué usar Linux.

Linux se ha convertido en uno de los sistemas más confiables del planeta. Combina esa confiabilidad con un costo de entrada cero y tendrás la solución perfecta para una plataforma de escritorio.

Cero costos de entrada debido a que es completamente gratuito. Puedes instalar Linux en tantas computadoras como desees sin tener que pagar licencias de software. Tampoco tiene costo el software y aplicaciones complementarias.

2.16.2. Linux y su inmunidad a los virus.

Según (Cansino, 2019). indicia que “Un virus informático es cualquier tipo de código o software malintencionado que puede infectar una computadora. Otro aspecto importante a favor de Linux es el reducido impacto de los virus de computadora.”

Lograr que un virus infecte a una máquina Linux es un gran desafío, eso no significa que deba estar sin protección. Aunque un aspecto positivo es su casi inmunidad a estos virus.

Ya sea en el escritorio o en un servidor también debes saber que este sistema funciona sin problemas. No es extraño que un servidor Linux funcione por años sin ser reiniciado. Eso es verdadera estabilidad y confiabilidad.

2.16.3. Linux Sistema Operativo de Código Abierto.

Según (Cansino, 2019). indicia que "Linux se distribuye bajo una licencia de código abierto. Esto significa que es mejorado continuamente por una comunidad de desarrolladores. Está diseñado para seguir siendo gratuito."

El código abierto sigue la filosofía de libertad de uso y distribución. Puedes ejecutar libremente el programa, independientemente si tu propósito es personal o comercial.

2.16.4. Tipos de Distribuciones Linux.

Según (Cansino, 2019). indicia que "Linux tiene varias versiones diferentes que le permiten adaptarse a casi cualquier tipo de usuario. Desde usuarios nuevos hasta usuarios experimentados, encontrarán un tipo de Linux que puede satisfacer sus necesidades."

Las distribuciones de Linux más populares son:

- Ubuntu Linux
- Kali Linux
- Linux Mint
- Arco de linux
- Fedora
- Debian
- openSUSE.

2.17. MODULO

Según (Wikipedia, Wikipedia, 2020). indicia que “En programación, un módulo es una porción de un programa de ordenador. De las varias tareas que debe realizar un programa para cumplir con su función u objetivos, un módulo realizará, comúnmente, una de dichas tareas (o varias, en algún caso).”

Según (Wikipedia, Wikipedia, 2020). indicia que “Un módulo recibe como entrada la salida que haya proporcionado otro módulo o los datos de entrada al sistema si se trata del módulo principal de éste; y proporcionará una salida que, a su vez, podrá ser utilizada como entrada de otro módulo o bien contribuirá directamente a la salida final del sistema, si se retorna al módulo principal.”

2.18. ETHICAL HACKING

Según (Solorzano, 2015). indicia que “Hoy en día existen muchos sistemas que contienen información valiosa para las compañías. Las empresas guardan información de sus finanzas o datos sensibles de los clientes en computadoras que están generalmente conectadas a la red.”

Según (Solorzano, 2015). indicia que “Los expertos en seguridad informática aplican varios métodos y técnicas para proteger a dichos sistemas de cualquier ataque de hackers o crackers malintencionados para evitar que estos roben o borren información. Uno de esos métodos es el Ethical Hacking.”

El objetivo fundamental del Ethical Hacking es explotar las vulnerabilidades existentes en los sistemas, haciendo pruebas de intrusión, que sirven para verificar y evaluar la seguridad

física y lógica de los sistemas de información, redes de computadoras, aplicaciones web, bases de datos, servidores, etc.

Los beneficios que ofrece el Ethical Hacking son:

- Otorgar un panorama acerca de las vulnerabilidades encontradas para tomar medidas.
- Evidencia configuraciones no adecuadas en las aplicaciones instaladas.
- Identifica a qué sistemas les hacen falta actualizaciones.
- Disminuir el tiempo y esfuerzo requeridos para afrontar situaciones de riesgo.

Según (Iniseg, 2018). indicia que "Hacking ético es una forma de referirse al acto de una persona, o mejor conocido como hacker, que utiliza sus conocimientos de informática y seguridad para encontrar vulnerabilidades o fallas de seguridad en el sistema, con el objetivo de reportarlas en la organización para que se tomen todas las medidas necesarias que posibilite prevenir una catástrofe cibernética, como el robo de información."

Según (Iniseg, 2018). indicia que "Los profesionales que se dedican al Hacking ético, practican una serie de pruebas o test denominados "Test de penetración" cuyo objetivo es poder burlar las diferentes vallas de seguridad que tiene la red para diferentes organizaciones, con la única intención de probar su efectividad, o, por el contrario, demostrar la vulnerabilidad de aquel sistema."

2.18.1. Tipos de Ethical Hacking.

Las pruebas de penetración se enfocan principalmente en las siguientes perspectivas:

- Pruebas de penetración con objetivo: se buscan las vulnerabilidades en partes específicas de los sistemas informáticos críticos de la organización.

- Pruebas de penetración sin objetivo: consisten en examinar la totalidad de los componentes de los sistemas informáticos pertenecientes a la organización. Este tipo de pruebas suelen ser las más laboriosas.
- Pruebas de penetración a ciegas: en estas pruebas sólo se emplea la información pública disponible sobre la organización.
- Pruebas de penetración informadas: aquí se utiliza la información privada, otorgada por la organización acerca de sus sistemas informáticos. En este tipo de pruebas se trata de simular ataques realizados por individuos internos de la organización que tienen determinado acceso a información privilegiada.
- Pruebas de penetración externas: son realizas desde lugares externos a las instalaciones de la organización. Su objetivo es evaluar los mecanismos perimetrales de seguridad informática de la organización.
- Pruebas de penetración internas: son realizadas dentro de las instalaciones de la organización con el objetivo de evaluar las políticas y mecanismos internos de seguridad de la organización.

2.18.2. Modalidades de Hacking.

Según (capa8, 2015). indicia que “Dependiendo de la modalidad que el cliente provea al consultor, el servicio de hacking ético se puede ejecutar en una de las 3 modalidades: Black-box Hacking, Grey-box Hacking, White-box Hacking. la modalidad escogida afectará el costo y la duración de las pruebas de intrusión, puesto que a menor información recibida mayor será el tiempo invertido en investigar por parte del auditor.”

- Black-box Hacking: Esta modalidad se aplica a pruebas de intrusión externas. se llama de este modo, por que el cliente solamente le proporciona el nombre de la empresa a

auditar al consultor, por lo que este, obra a ciegas, la infraestructura de la organización es una caja negra para él.

- Grey-box Hacking: suele utilizarse como sinónimo para referirse a las pruebas de intrusión internas. pero algunos auditores les llaman también Hacking de Caja Gris a una prueba externa a la cual el cliente proporciona información limitada sobre los equipos públicos a ser auditados. Ejemplo: un listado con datos como las direcciones IP y el Tipo/Función del equipo (Router, Firewall, Web-Server, etc…).
- White-box Hacking: Algunas veces denominado Hacking Transparente. Esta modalidad se aplica a pruebas de intrusión solamente y se llama de esta forma por que la empresa cliente le da al auditor información completa de las redes y los sistemas a auditar.

2.19. INGENIERIA DE SOFTWARE

Según (Pressman, 2010). indicia que “El software de computadora es el producto que construyen los programadores profesionales y al que después le dan mantenimiento durante un largo tiempo. Incluye programas que se ejecutan en una computadora de cualquier tamaño y arquitectura, contenido que se presenta a medida que se ejecutan los programas de cómputo e información descriptiva tanto en una copia dura como en formatos virtuales que engloban virtualmente a cualesquiera medios electrónicos. La ingeniería de software está formada por un proceso, un conjunto de métodos (prácticas) y un arreglo de herramientas que permite a los profesionales elaborar software de cómputo de alta calidad.”

2.19.1. ¿Por qué es importante?

Según (Pressman, 2010). indicia que “El software es importante porque afecta a casi todos los aspectos de nuestras vidas y ha invadido nuestro comercio, cultura y actividades

cotidianas. La ingeniería de software es importante porque nos permite construir sistemas complejos en un tiempo razonable y con alta calidad.”

2.19.2. ¿Cuáles son los pasos?

Según (Pressman, 2010). indicia que “El software de computadora se construye del mismo modo que cualquier producto exitoso, con la aplicación de un proceso ágil y adaptable para obtener un resultado de mucha calidad, que satisfaga las necesidades de las personas que usarán el producto. En estos pasos se aplica el enfoque de la ingeniería de software”

2.19.3. Etapas.

1. Según (Xavi, 20113). indicia que “Análisis de requerimientos: Se extraen los requisitos del producto de software. En esta etapa la habilidad y experiencia en la ingeniería del software es crítica para reconocer requisitos incompletos, ambiguos o contradictorios. Usualmente el cliente/usuario tiene una visión incompleta/inexacta de lo que necesita y es necesario ayudarle para obtener la visión completa de los requerimientos. El contenido de comunicación en esta etapa es muy intenso ya que el objetivo es eliminar la ambigüedad en la medida de lo posible.”
2. Según (Xavi, 20113). indicia que “Especificación: Es la tarea de describir detalladamente el software a ser escrito, de una forma rigurosa. Se describe el comportamiento esperado del software y su interacción con los usuarios y/o otros sistemas.”
3. Según (Xavi, 20113). indicia que “Diseño y arquitectura: Determinar cómo funcionará de forma general sin entrar en detalles incorporando consideraciones de la implementación tecnológica, como el hardware, la red, etc. Consiste en el diseño de los componentes del sistema que dan respuesta a las funcionalidades descritas en la segunda

etapa también conocidas como las entidades de negocio. Generalmente se realiza en base a diagramas que permitan describir las interacciones entre las entidades y su secuenciado."

4. Según (Xavi, 20113). indicia que "Programación: Se traduce el diseño a código. Es la parte más obvia del trabajo de ingeniería de software y la primera en que se obtienen resultados. No necesariamente es la etapa más larga ni la más compleja, aunque una especificación o diseño incompletos/ambiguos pueden exigir que, tareas propias de las etapas anteriores se tengan que realizarse en esta."
5. Según (Xavi, 20113). indicia que "Prueba: Consiste en comprobar que el software responda/realice correctamente las tareas indicadas en la especificación. Es una buena praxis realizar pruebas a distintos niveles (por ejemplo, primero a nivel unitario y después de forma integrada de cada componente) y por equipos diferenciados del de desarrollo (pruebas cruzadas entre los programadores o realizadas por un área de test independiente)."
6. Según (Xavi, 20113). indicia que "Documentación: Realización del manual de usuario, y posiblemente un manual técnico con el propósito de mantenimiento futuro y ampliaciones al sistema. Las tareas de esta etapa se inician ya en la primera fase, pero sólo finalizan una vez terminadas las pruebas."
7. Según (Xavi, 20113). indicia que "Mantenimiento: En esta etapa se realizan un mantenimiento correctivo (resolver errores) y un mantenimiento evolutivo (mejorar las funcionalidades y/o dar respuesta a nuevos requisitos)."

2.19.4. Métodos de Evaluación.

- Según (Marquez, 2020). indicia que “Caja Negra: Es el método en el cual el elemento es estudiado desde el punto de vista de las entradas que recibe y las salidas o respuestas que produce, sin tener en cuenta su funcionamiento interno. Estas pruebas son realizadas desde la interfaz gráfica. Ejemplo: caja negra testing sería el cual una persona haría antes de comprar un coche, encender las luces, encender el motor entre otras pruebas (Sin necesidad de saber cómo funciona el coche por dentro).”
- Según (Marquez, 2020). indicia que “Caja blanca: El método de pruebas es el cual mira el código y la estructura del producto que se va a probar y usa ese conocimiento para la realización de las pruebas. Ejemplos: realizar pruebas de tipo caja blanca sería la técnica que usa un mecánico cuando llevas tu coche al mecánico y tiene que buscar una avería.”

2.19.5. Costos.

Según (Roque, 2014). indicia que “La estimación de costos en el desarrollo de software es un factor realmente importante para el análisis de los proyectos, constituye un tema estratégico contar con métricas para medir el costo de un proyecto de software garantizando la eficiencia, competitividad, eficacia y excelencia. Un elemento indispensable en cualquier sistema económico constituye el asegurar el papel del costo en la planificación del país y fundamentalmente en la correcta dirección de la empresa mediante mecanismos ágiles que permitan un elevado grado de confiabilidad.”

- Fundamentar tendencias actuales, metodologías y conceptos más importantes relacionados con el costo de un producto de software.
- Identificar los principales modelos para calcular el costo del software.
- Estudiar las métricas utilizadas en la creación de un producto de software.

2.19.6. Arquitectura cliente servidor.

En el modelo cliente servidor, el cliente envía un mensaje solicitando un determinado servicio a un servidor (hace una petición), y este envía uno o varios mensajes con la respuesta (provee el servicio). En un sistema distribuido cada máquina puede cumplir el rol de servidor para algunas tareas y el rol de cliente para otras.

Diseño de software de arquitectura cliente - servidor es un modelo de sistema en el que dicho sistema se organiza como un conjunto de servicios y servidores asociados, más los clientes que acceden y usan los servicios.

- Principales componentes del modelo son:
- Un conjunto de servidores que ofrecen a otros subsistemas.
- Un conjunto de cliente que llaman a los servicios ofrecidos por los servidores. Puede tener varias instancias de un programa cliente ejecutándose concurrentemente.
- Una red que permite a los clientes acceder a estos servicios.

2.19.6.1. Cliente.

El Cliente normalmente maneja todas las funciones relacionadas con la manipulación y despliegue de datos, por lo que están desarrollados sobre plataformas que permiten construir interfaces gráficas de usuario (GUI), además cliente-servidor de acceder a los servicios distribuidos en cualquier parte de una red.

Las funciones que lleva a cabo el proceso cliente se resumen en los siguientes puntos:

- Administrar la interfaz de usuario.
- Interactuar con el usuario.
- Procesar la lógica de la aplicación y hacer validaciones locales.

- Generar requerimientos de bases de datos.
- Recibir resultados del servidor.
- Formatear resultados.

2.19.6.2. Servidor.

Según (ITTGWEB, 2016). indicia que “Es el proceso encargado de atender a múltiples clientes que hacen peticiones de algún recurso administrado por él. Al proceso servidor se le conoce con el término back-end.”

Según (ITTGWEB, 2016). indicia que “El servidor normalmente maneja todas las funciones relacionadas con la mayoría de las reglas del negocio y los recursos de datos.”

Las funciones que lleva a cabo el proceso servidor se resumen en los siguientes puntos:

- Aceptar los requerimientos de bases de datos que hacen los clientes.
- Procesar requerimientos de bases de datos.
- Formatear datos para trasmitirlos a los clientes
- Procesar la lógica de la aplicación y realizar validaciones a nivel de bases de datos.

2.19.7. Modelo vista controlador.

Según (Garcia M. , 2017). indicia que “El MVC es un patrón de diseño arquitectónico de software, que sirve para clasificar la información, la lógica del sistema y la interfaz que se le presenta al usuario. En este tipo de arquitectura existe un sistema central o controlador que gestiona las entradas y la salida del sistema, uno o varios modelos que se encargan de buscar los datos e información necesaria y una interfaz que muestra los resultados al usuario final.”

Según (arlethparedes, 2012). indicia que “El Modelo Vista Controlador (MVC) es un patrón de arquitectura de software que separa los datos de una aplicación, la interfaz de usuario, y la

lógica de control en tres componentes distintos (Modelo, Vista y Controlador). El Patrón MVC se ve frecuentemente en aplicaciones Web, donde la Vista es la página HTML y el código que provee de datos dinámicos a la página; el Modelo es el Sistema de Gestión de Base de Datos y la Lógica de negocio; el Controlador es el responsable de recibir los eventos de entrada desde la Vista."

- Según (Garcia M. , 2017). indicia que "Modelo: este componente se encarga de manipular, gestionar y actualizar los datos. Si se utiliza una base de datos aquí es donde se realizan las consultas, búsquedas, filtros y actualizaciones.

  El Modelo es el responsable de:

  Según (arlethparedes, 2012). indicia que

  - "Acceder a la capa de almacenamiento de datos. Lo ideal es que el modelo sea independiente del sistema de almacenamiento."
  - "Define las reglas de negocio (la funcionalidad del sistema). Un ejemplo de regla puede ser: "Si la mercancía pedida no está en el almacén, consultar el tiempo de entrega estándar del proveedor"."
  - "Lleva un registro de las vistas y controladores del sistema."
  - "Si estamos ante un modelo activo, notificará a las vistas los cambios que en los datos pueda producir un agente externo (por ejemplo, un fichero batch que actualiza los datos, un temporizador que desencadena una inserción, etc.). Un ejemplo de MVC con un modelo pasivo (aquel que no notifica cambios en los datos) es la navegación web, que responde a las entradas del usuario, pero no detecta los cambios en datos del servidor."

- Según (Garcia M. , 2017). indicia que “Vista: este componente se encarga de mostrarle al usuario final las pantallas, ventanas, páginas y formularios; el resultado de una solicitud. Desde la perspectiva del programador este componente es el que se encarga del frontend; la programación de la interfaz de usuario si se trata de una aplicación de escritorio, o bien, la visualización de las páginas web (CSS, HTML, HTML5 y Javascript).”

  Las vistas son responsables de:

  Según (arlethparedes, 2012). indicia que:

  - “Recibir datos del modelo y los muestra al usuario.”
  - “Tienen un registro de su controlador asociado (normalmente porque además lo instancia).”
  - “Pueden dar el servicio de “Actualización ()”, para que sea invocado por el controlador o por el modelo (cuando es un modelo activo que informa de los cambios en los datos producidos por otros agentes).”

- Según (Garcia M. , 2017). indicia que “Controlador: este componente se encarga de gestionar las instrucciones que se reciben, atenderlas y procesarlas. Por medio de él se comunican el modelo y la vista: solicitando los datos necesarios; manipulándolos para obtener los resultados; y entregándolos a la vista para que pueda mostrarlos.”

  El controlador es responsable de:

  Según (arlethparedes, 2012). indicia que:

  - “Recibe los eventos de entrada (un clic, un cambio en un campo de texto, etc.).”
  - “Contiene reglas de gestión de eventos, del tipo “SI Evento Z, entonces Acción W”. Estas acciones pueden suponer peticiones al modelo o a las vistas. Una de

estas peticiones a las vistas puede ser una llamada al método “Actualizar ()”. Una petición al modelo puede ser “Obtener_tiempo_de_entrega (nueva_orden_de_venta)”.”

2.20. Metodología UWE

Según (Ricardo, 2011). indicia que “UWE está especializada en la especificación de aplicaciones adaptativas, y por tanto hace especial hincapié en características de personalización, como es la definición de un modelo de usuario o una etapa de definición de características adaptativas de la navegación en función de las preferencias, conocimiento o tareas de usuario.”

Según (Ricardo, 2011). indicia que “Otras características relevantes del proceso y método de autoría de UWE son el uso del paradigma orientado a objetos, su orientación al usuario, la definición de un meta-modelo (modelo de referencia) que da soporte al método y el grado de formalismo que alcanza debido al soporte que proporciona para la definición de restricciones sobre los modelos.”

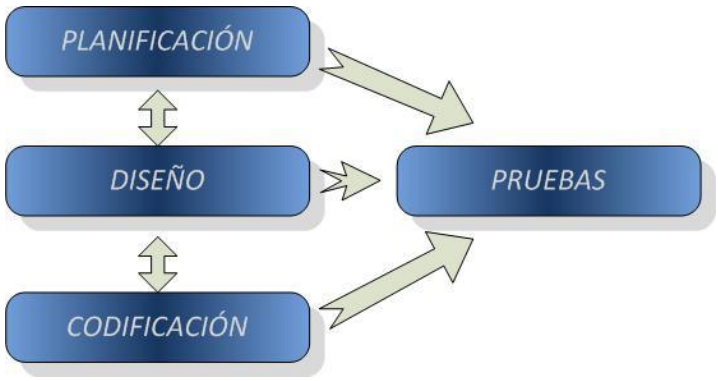


Figura: 2.1. Metodología UWE

Fuente: [Galiano 2012]

2.20.1. Modelos.

Según (Vega, 2012). indicia que “Se utiliza para obtener nuevas clases navegacionales y enlaces entre ellas, que se agregan al modelo que se obtiene a partir del modelo de clases. El modelo que propone UWE.” Está compuesto por 6 etapas o sub-modelos:

- Modelo de Casos de Uso: modelo para capturar los requisitos del sistema.
- Modelo de Contenido: es un modelo conceptual para el desarrollo del contenido.
- Modelo de Usuario: es modelo de navegación, en el cual se incluyen modelos estáticos y modelos dinámicos.
- Modelo de Estructura: en el cual se encuentra la presentación del sistema y el modelo de flujo.
- Modelo Abstracto: incluye el modelo a de interfaz de usuario y el modelo de ciclo de vida del objeto.
- Modelo de Adaptación.

2.20.2. Faces.

1. Según (Sanchez, 2017). indicia que “Captura, análisis y especificación de requisitos: Durante esta fase, se adquieren, reúnen y especifican las características funcionales y no funcionales que deberá cumplir la aplicación web.”
2. Según (Sanchez, 2017). indicia que “Diseño del sistema: Se basa en la especificación de requisitos producido por el análisis de los requerimientos, el diseño define cómo estos requisitos se cumplirán, la estructura que debe darse a la aplicación web.”
3. Según (Sanchez, 2017). indicia que “Codificación del software: Se realizan las tareas que comúnmente se conocen como programación; que consiste, esencialmente, en llevar

a código fuente, en el lenguaje de programación elegido, todo lo diseñado en la fase anterior.”

4. Según (Sanchez, 2017). indicia que “Pruebas: Las pruebas se utilizan para asegurar el correcto funcionamiento de secciones de código.”
5. Según (Sanchez, 2017). indicia que “La Instalación o Fase de Implementación: Proceso por el cual los programas desarrollados son transferidos apropiadamente al computador destino.”
6. Según (Sanchez, 2017). indicia que “El Mantenimiento: Es el proceso de control, mejora y optimización del software ya desarrollado e instalado”

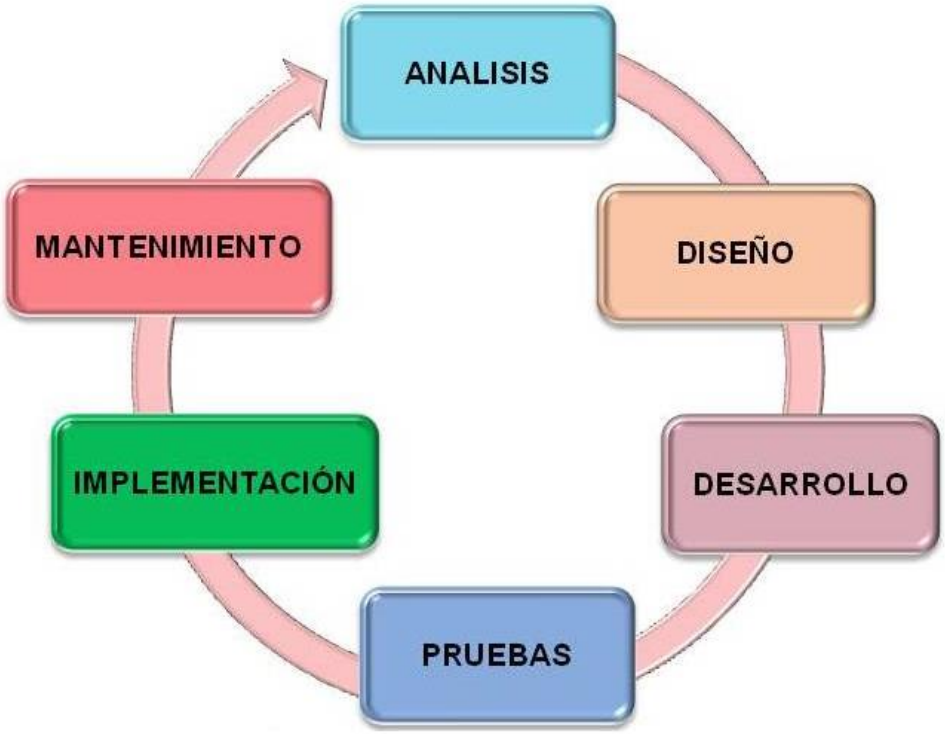


Figura: 2.2. Faces de UWE

Fuente: [Rocha,2015]

2.21. METRICAS DE CALIDAD

Según (PowerData, 2016). indicia que “La mala calidad de la información y de software impacta negativamente en el negocio a diferentes niveles:

- Disminuye ingresos y aumenta el gasto.
- Incrementa el riesgo.
- Provoca una reducción de la confianza, tanto dentro como fuera de la organización.”

Según (PowerData, 2016). indicia que “Un enfoque proactivo tanto del gobierno de la información como de la data quality permite la identificación temprana de errores o defectos que pueden ser corregidos a tiempo, eliminando de raíz problemas mayores. Los efectos positivos empiezan a notarse y sus beneficios aumentan en un ciclo de mejora continúa propiciado por el control de las métricas de calidad de software.”

Esta monitorización facilita el evaluar:

- La calidad del producto.
- El rendimiento del equipo de desarrollo.
- La justificación del uso de nuevas herramientas o soluciones.
- Los resultados obtenidos a partir de la incorporación del software a los procesos y operaciones.

Según (PowerData, 2016). indicia que “Para conseguir llegar al nivel de evaluación, es preciso contar con datos relevantes, precisos y actualizados sobre diferentes áreas, que faciliten una perspectiva global de la solución. Así, las métricas de calidad de software pueden aplicarse a diferentes contextos,” como:

- El proyecto: son las que facilitan la gestión del riesgo permitiendo tomar el pulso a la iniciativa de desarrollo desde su inicio.
- El producto: están enfocadas a medir las características del software y todos los entregables que lo acompañan, fruto del proyecto de desarrollo, como modelos, componentes adicionales y documentación.
- El proceso: tienen por objeto identificar mejores prácticas para su exportación a futuros proyectos y, para conseguirlo, recopilan datos de distintas iniciativas a lo largo de un periodo de tiempo determinado.

Sin embargo, a la hora de centrarse en la solución en sí, existen algunas métricas de calidad de software imprescindibles, como las que tienen que ver con los cinco siguientes criterios:

1. Métricas de exactitud: intentan aportar información sobre la validez y precisión del software y su estructura, incluyendo la etapa de despliegue, pero también la de pruebas y la función de mantenimiento.
2. Métricas de rendimiento: a través de ellas se consigue medir el desempeño del software, tanto de cada uno de sus módulos, como del sistema al completo.
3. Métricas de usabilidad: hay que descartar la complejidad y buscar una solución intuitiva y user-friendly. este tipo de métricas de calidad de software ayudan a determinar si la solución cumple con dichos requisitos.
4. Métricas de configuración: las limitaciones, el estilo de código y todos los datos relativos al desarrollo y cualidades del producto se verán evaluados en base a estas métricas.
5. Métricas de eficiencia: minimización de latencias, velocidad de respuesta, capacidad, es un enfoque similar al de la productividad, pero con un matiz un poco distinto, que, añadido a aquél, aporta una visión mucho más completa de la solución.

2.21.1. ISO/IEC 25000

Según (ISO25000, 2019). indicia que “Conocida como SQuaRE (System and Software Quality Requirements and Evaluation), es una familia de normas que tiene por objetivo la creación de un marco de trabajo común para evaluar la calidad del producto software.

Es el resultado de la evolución de otras normas anteriores, especialmente de las normas ISO/IEC 9126, que describe las particularidades de un modelo de calidad del producto software, e ISO/IEC 14598, que abordaba el proceso de evaluación de productos software. Esta familia de normas ISO/IEC 25000 se encuentra compuesta por cinco divisiones.”

2.21.1.1. Usabilidad

Según (ISO25000, 2019). indicia que “Capacidad del producto software para ser entendido, aprendido, usado y resultar atractivo para el usuario, cuando se usa bajo determinadas condiciones.” Esta característica se subdivide a su vez en las siguientes sub-características:

- Capacidad para reconocer su adecuación. Capacidad del producto que permite al usuario entender si el software es adecuado para sus necesidades.
- Capacidad de aprendizaje. Capacidad del producto que permite al usuario aprender su aplicación.
- Capacidad para ser usado. Capacidad del producto que permite al usuario operarlo y controlarlo con facilidad.
- Protección contra errores de usuario. Capacidad del sistema para proteger a los usuarios de hacer errores.
- Estética de la interfaz de usuario. Capacidad de la interfaz de usuario de agradar y satisfacer la interacción con el usuario.

- Accesibilidad. Capacidad del producto que permite que sea utilizado por usuarios con determinadas características y discapacidades.

2.21.2. Cócono II.

Según (Gomez , A. Lopez, M. Migani, S., 2017). indicia que “Permite realizar estimaciones en función del tamaño del software, y de un conjunto de factores de costo y de escala. Posee tres modelos: Composición de Aplicación, Diseño Temprano y Post-Arquitectura.”

2.21.2.1. Modelo post-arquitectura.

Según (Gomez , A. Lopez, M. Migani, S., 2017). indicia que “El esfuerzo nominal ajusta usando 17 factores multiplicadores de esfuerzo.”

Según (Gomez , A. Lopez, M. Migani, S., 2017). indicia que “El mayor número de multiplicadores permite analizar con más exactitud el conocimiento disponible en las últimas etapas de desarrollo, ajustando el modelo de tal forma que refleje fielmente el producto de software bajo desarrollo.”

2.21.2.2. Formulas.

La Fórmula propuesta en este modelo es la siguiente:

PM(estimado) = PM(nominal) * $\prod_{i=1}^{17} EMi$

Los factores de clasifican en cuatro áreas: Producto, Plataforma, Personal y Proyecto

2.21.3. Métricas de costos.

Según (SBuendia, 2012). indicia que “Sirve para establecer mediciones para el tamaño de desarrollo y el trabajo requerido para llevarlo a cabo. Su objetivo es el definir el tamaño de un sistema y establecer unidades de medición.”

Según (SBuendia, 2012). indicia que “El tamaño de software se mide por: puntos por función, por líneas de código, por clases y objetos, tablas en una base de datos, elementos GUI, CU y UCP (simple 5CU, mediano 10 CU, complejo 15 CU o +).”

Se define el esfuerzo, como la suma de tiempo dedicado por las personas para realizar una actividad, se mide en días, horas, semanas o meses.

El esfuerzo juega un papel importante para el calcular el costo de nuestro proyecto.

2.22. HERRAMIENTAS

2.22.1. Herramientas.

Las herramientas que utilizaremos son las siguientes:

- JavaScript: “Es un lenguaje que puede ser utilizado por profesionales y para quienes se inician en el desarrollo y diseño de sitios web. No requiere de compilación ya que el lenguaje funciona del lado del cliente, los navegadores son los encargados de interpretar estos códigos.” (Valdes, 2007)

  Según (Valdes, 2007). indicia que “Java por su parte tiene como principal característica ser un lenguaje independiente de la plataforma. Se puede crear todo tipo de programa que puede ser ejecutado en cualquier ordenador del mercado: Linux, Windows, Apple, etc. Debido a sus características también es muy utilizado para internet.”

Con el surgimiento de lenguajes como PHP del lado del servidor y Javascript del lado del cliente, surgió Ajax en acrónimo de (Asynchronous Javascript And XML). El mismo es una técnica para crear aplicaciones web interactivas. Este lenguaje combina varias tecnologías:

- HTML y Hojas de Estilos CSS para generar estilos.
- Implementaciones ECMAScript, uno de ellos es el lenguaje Javascript.
- XMLHttpRequest es una de las funciones más importantes que incluye, que permite intercambiar datos asincrónicamente con el servidor web, puede ser mediante PHP, ASP, entre otros.

- PHP: "Es un lenguaje de programación de propósito general que se ejecuta en el lado del servidor, Es un lenguaje interpretado, Tiene múltiples formas de utilizarse, ya que puede utilizarse con scripts, de forma estructurada o programación en objetos.

  Fue creado por Rasmus Lerdorf y apareció en el año 1994, Está creado con la licencia de software libre PHPv3_01, que es una licencia Open Source.

  PHP se utiliza principalmente para crear páginas web, para crear contenido dinámico y para trabajar con bases de datos y HTML.

  Soporta la mayoría de bases de datos, MySQL, PostgreSQL, SQL Server, MongoDB, para casi todas existen drivers, y si no es así podemos utilizar el driver ODBC, que se conecta a cualquier base de datos." (Solano A. , 2019).

  Otra opción para utilizar PHP sería con un script desde la línea de comandos.

  Es un lenguaje de programación de propósito general que se ejecuta en el lado del servidor.

  - Es un lenguaje interpretado.

- Tiene múltiples formas de utilizarse, ya que puede utilizarse con scripts, de forma estructurada o programación en objetos.
- Fue creado por Rasmus Lerdorf y apareció en el año 1994.
- Está creado con la licencia de software libre PHPv3_01, que es una licencia Open Source.

- BOOTSTRAP: "Es un framework originalmente creado por Twitter, que permite crear interfaces web con CSS y JavaScript, cuya particularidad es la de adaptar la interfaz del sitio web al tamaño del dispositivo en que se visualice. Es decir, el sitio web se adapta automáticamente al tamaño de una PC, una Tablet u otro dispositivo.

  Tiene un soporte relativamente incompleto para HTML5 y CSS 3, pero es compatible con la mayoría de los navegadores web. La información básica de compatibilidad de sitios web o aplicaciones está disponible para todos los dispositivos y navegadores. Existe un concepto de compatibilidad parcial que hace disponible la información básica de un sitio web para todos los dispositivos y navegadores." (ARWEB, 2014)

  Según (Axarnet, 2017). indicia que "Actualmente, Bootstrap es una de las alternativas más populares a la hora de desarrollar tanto sitios webs como aplicaciones. Una de las principales ventajas que ofrece es que permite la creación de sitios y apps 100% adaptables a cualquier tipo de dispositivo. Una cuestión de suma importancia teniendo en cuenta que a día de hoy son cada vez más los usuarios que acceden a Internet a través de sus teléfonos y tabletas."

  Gracias a un sistema GRID que permite realizar un diseño haciendo uso de 12 columnas para insertar el contenido, los usuarios pueden crear sitios web responsive de una manera mucho más sencilla e intuitiva.

- NMAP: “Es una aplicación multiplataforma usada para explorar redes y obtener información acerca de los servicios, sistemas operativos y vulnerabilidades derivadas de la conjunción de éstos.” (Informática, 2007)

  Según (Informática, 2007). indicia que “Es muy usado por todo aquél que se interesa por las tareas de seguridad y hacking en general, desde Administradores de Sistemas a interesados con fines menos respetables. Las técnicas de escaneo que usa Nmap han sido ya implementadas en sistemas de detección de intrusos y firewalls, ya que los desarrolladores de sistemas de seguridad también usan Nmap en su trabajo y toman medidas. No obstante, pese a estar ampliamente documentado su funcionamiento, hay formas de escaneo que lo hacen difícil de detectar cuando se trata de obtener información.”

  Existe una amplia gama de utilidades de monitorización de red gratuitas, así como escáneres de vulnerabilidades de código abierto gratuitos disponibles para administradores de red y auditores de seguridad. Lo que hace que Nmap destaque como la herramienta que los administradores de IT y de redes necesitan conocer es su flexibilidad y potencia. Aunque la base de la funcionalidad de Nmap es el análisis de puertos, permite una variedad de capacidades relacionadas, incluyendo:

  - Mapeo de red: Nmap puede identificar los dispositivos en una red (también llamado descubrimiento de host), incluyendo servidores, enrutadores y conmutadores, y cómo están conectados físicamente.
  - Detección de SO: Nmap puede detectar los sistemas operativos que se ejecutan en los dispositivos de red (también llamados OS fingerprinting), proporcionando el nombre del proveedor, el sistema operativo subyacente, la versión del software e incluso una estimación del tiempo de actividad de los dispositivos.

- Descubrimiento de servicios: Nmap no sólo puede identificar hosts en la red, sino también si actúan como servidores de correo, web o de nombres, y las aplicaciones y versiones particulares del software relacionado que están ejecutando.
- Auditoría de seguridad: Averiguar qué versiones de sistemas operativos y aplicaciones se están ejecutando en los hosts de red permite a los administradores de red determinar su vulnerabilidad a fallas específicas. Si un administrador de red recibe una alerta sobre una vulnerabilidad en una versión particular de una aplicación, por ejemplo, puede escanear su red para identificar si esa versión de software se está ejecutando en la red y tomar medidas para parchear o actualizar los hosts relevantes. Los scripts también pueden automatizar tareas como la detección de vulnerabilidades específicas.

  (marindelafuente, 2019)

Según (Informatica, 2007). indicia que "Es muy usado por todo aquél que se interesa por las tareas de seguridad y hacking en general, desde Administradores de Sistemas a interesados con fines menos respetables. Las técnicas de escaneo que usa Nmap han sido ya implementadas en sistemas de detección de intrusos y firewalls, ya que los desarrolladores de sistemas de seguridad también usan Nmap en su trabajo y toman medidas. No obstante, pese a estar ampliamente documentado su funcionamiento, hay formas de escaneo que lo hacen difícil de detectar cuando se trata de obtener información."

- NCAT: "Es una utilidad de red con una funcionalidad similar al comando cat, pero para la red. Es una herramienta CLI de propósito general para leer, escribir y redirigir datos a través de una red. Está diseñado para ser una herramienta de fondo confiable que se

puede usar con scripts u otros programas. También es una gran herramienta para la depuración de la red, ya que puede crear cualquier tipo de conexión que uno pueda necesitar.” (Kunar, 2020)

Según (Kunar, 2020). indicia que “puede ser una herramienta de escaneo de puertos, o una herramienta de seguridad, o la herramienta de monitoreo y también es un simple proxy de TCP. Como tiene tantas características, se conoce como una red navaja suiza. Es una de esas herramientas que todo administrador del sistema debe conocer y dominar, Los administradores del sistema pueden usarlo para auditar la seguridad de su sistema, pueden usarlo para encontrar los puertos que están abiertos y luego asegurarlos. Los administradores también pueden usarlo como cliente para auditar servidores web, servidores telnet, servidores de correo, etc. Con 'nc' podemos controlar cada carácter enviado y también podemos ver las respuestas a las consultas enviadas.”

Según (Garcia G. , 2008). indicia que “Es una utilería para Linux y Windows que fue escrita originalmente para sistemas Unix, Berkeley y System V. Ha sido llamada la Navaja Militar Suiza multiusos en virtud de la gran versatilidad y potencia contenida en tan mínimo espacio y con tan poco código”

Herramienta imprescindible en el mundo de la seguridad informática. Es análoga a la ganzúa del ratero. Entender esta utilería es amarla. NetCat ha sido la estrella principal en cientos de ataques. El verdadero secreto de su poder radica en el buen manejo que se le dé.

- NCRACK: “Es una de las herramientas favoritas para descifrar contraseñas. Se basa en las bibliotecas de nmap. Viene preinstalado con Kali Linux OS. Se puede combinar con nmap para obtener excelentes resultados. La única desventaja es que admite muy pocos

servicios, a saber, FTP, SSH, Telnet, FTP, POP3, SMB, RDP y VNC.” (EHACKING, 2019)

Según (creadpag, 2018). indicia que “Es una herramienta de craqueo de autenticación de red de alta velocidad. Fue construido para ayudar a las compañías a proteger sus redes probando proactivamente todos sus hosts y dispositivos de red para las contraseñas pobres. Los profesionales de la seguridad también confían en Ncrack al auditar a sus clientes. Ncrack fue diseñado utilizando un enfoque modular, una sintaxis de línea de comandos similar a Nmap y un motor dinámico que puede adaptar su comportamiento basado en la retroalimentación de la red. Permite una auditoría a gran escala rápida y confiable de múltiples hosts.”

- METASPLOIT FRAMEWORK: “Metasploit framework es una herramienta desarrollada en Perl y Ruby en su mayor parte, que está enfocada a auditores de seguridad y equipos Red Team y Blue Team, Es una herramienta muy completa que tiene muchísimos exploits, que son vulnerabilidades conocidas, en las cuales tienen también unos módulos, llamados payloads, que son los códigos que explotan estas vulnerabilidades.” (Rizaldos, 2018)

  Según (Rizaldos, 2018). indicia que “Además, ofrece la posibilidad de exportar nuestro malware a cualquier formato, ya sea en sistemas Unix o Windows.

  Destacar también que es multiplataforma y gratuita, aunque tiene una versión de pago, en la que se nos ofrecen exploits ya desarrollados, pero cuyo coste es bastante elevado. La versión gratuita es muy interesante porque contiene todas las vulnerabilidades públicas.”

  Según (Jazz, 2014). indicia que “Un metasploit es un programa de código fuente abierto, que se utiliza para la gestión de vulnerabilidades informáticas y en desarrollo de firmas

para poder detectar posibles intrusos. Actúa buscando vulnerabilidades de seguridad en una maquina remota. En el caso de Kali Linux cuanta con el Metasploit Framework que cuenta con una de las más grandes, si no la más grande de las bases de datos de exploits públicos y que ya han sido probados."

Elegir y configurar el Exploit (Código que permite aprovechar la vulnerabilidad de un sistema).

Opcionalmente confirmar si el objetivo es susceptible al exploit elegido.

Elegir y configurar el Payload (Código que se ejecutara una vez explotemos la vulnerabilidad).

Elegir la técnica de codificación para que un IPS ignore el Payload.

Ejecutar el Exploit.

- MALTEGO: “Es una de las herramientas más completas y mejor implementadas que existen actualmente en el mercado enfocada sobre todo en la recolección de información y minería de datos, su valor añadido con respecto a las herramientas existentes en el mercado actualmente: La representación de la información en una forma simbólica, es decir, la información es presentada en distintos formatos de forma visual y enseñan las distintas relaciones encontradas entre la información presentada, por otro lado Maltego permite enumerar información relacionada con elementos de red y dominios de una forma bastante comprensible, así como también permite enumerar información relacionada con personas, datos tales como direcciones de email, sitios web asociados, números de teléfono, grupos sociales, empresas asociadas, etc.” (Adastra, 2011)

  Maltego es multiplataforma ya que se encuentra escrito en Java, como resultará obvio uno de los requisitos para que funcione adecuadamente es necesario tener una máquina virtual de Java correctamente instalada y al ser una aplicación gráfica, en sistemas

operativos GNU/Linux es necesario tener instalado un administrador de ventanas X11. Por otro lado, Maltego cuenta con dos tipos de distribuciones, una distribución comercial y una comunitaria, la diferencia entre ambas esta principalmente en que la comunitaria tiene ciertas restricciones que limitan su uso de forma considerable en entornos empresariales, de hecho, la versión comunitaria no puede ser utilizada para uso comercial, además de que solamente se pueden retornar 12 resultados por transformación por este motivo y algunos otros, si se intenta utilizar esta herramienta para fines distintos a los meramente educativos, es necesario adquirir una licencia del producto.

- YERSINIA: “Es una herramienta de red diseñada para aprovechar algunas debilidades en diferentes protocolos de red. Pretende ser un marco sólido para analizar y probar las redes y sistemas desplegados. Se implementan ataques para los siguientes protocolos de red: Spanning Tree Protocol (STP), Cisco Discovery Protocol (CDP), Dynamic Trunking Protocol (DTP), Dynamic Host Configuration Protocol (DHCP), Hot Standby Router Protocol (HSRP), IEEE 802.1Q, IEEE 802.1X, Protocolo de enlace entre conmutadores (ISL), Protocolo de enlace de VLAN (VTP).” (SON, 2017)
    - Ataque de DOS que envía BPDU conf
    - Ataque de DOS enviando tcn BPDU
    - Ataque de NONDOS reclamando el papel de la raíz
    - Ataque ONDOS Reclamando un rol no root
    - Ataque de DOS que causa elecciones eternas de raíz
    - Ataque de DOS que causa la desaparición de la raíz

Según (SECURITYTRAILS, 2018). indicia que “Esta herramienta puede atacar conmutadores, enrutadores, servidores DHCP y muchos otros protocolos. Incluye una elegante interfaz gráfica de usuario GTK, modo basado en ncurses, puede leer desde un archivo de configuración personalizado, admite el modo de depuración y ofrece guardar los resultados en un archivo de registro.”

Protocolo de red compatibles:

- LAN inalámbricas 802.1q y 802.1x
- Protocolo de descubrimiento de Cisco (CDP)
- Protocolo de configuración dinámica de host (DHCP)
- Protocolo de enlace dinámico (DTP)
- Protocolo de enlace entre conmutadores (ISL)
- Protocolo de enrutador en espera activa (HSRP)
- Protocolo de árbol de expansión (STP)
- Protocolo de enlace de VLAN (VTP)

- DSNIFF: “Es una colección de herramientas de auditoría de red y pruebas de penetración. dsniff, filesnarf, mailsnarf, msgsnarf, urlsnarf y webspy monitorea pasivamente una red de datos interesantes (contraseñas, correos electrónicos, archivos, etc). arpspoof, dnsspoof y macof facilita la interceptación de tráfico de red que normalmente no está disponible para un atacante. sshmitm y webmitm implementan ataques activos-hombre-en-el-medio contra SSH redirigida y HTTPS sesiones por la explotación de enlaces débiles en ad-hoc PKI.” (Admin, 2014)

  Dsniff es un conjunto de herramientas creadas para auditar redes y realizar test de penetración, Tiene un conjunto de herramientas amplio.

Según (Song, 2020). indicia que “Poderosa herramienta de auditoría y pruebas de penetración de redes. Incluye varias herramientas: dsniff, filesnarf, mailsnarf, msgsnarf, urlsnarf, y webspy monitorean pasivamente una red en busca de datos interesantes (passwords, e-mail, archivos, etc.). arpspoof, dnsspoof, y macof facilitan la intercepción de tráfico en la red normalmente no disponible para un atacante.”

- ETTERCAP: En una suite completa para realizar ataques de hombre en el medio. Permite interceptar conexiones en vivo, filtrar contenido al vuelo y varios otros trucos interesantes. Soporta disección activa y pasiva de varios protocolos e incluye diversas características para el análisis de red y host.

  Según (ReYDeS, 2014). indicia que “Ettercap generará un ataque “ARP Spoofing” la cual es una técnica donde un atacante envía mensajes ARP (Address Resolution Protocol) “Spoofed” o falsos en una Red Local Interna. Generalmente, la intención es asociar la dirección MAC del atacante con la dirección IP de otro host (como el gateway o pasarela por defecto), causando que cualquier tráfico destinado para esta dirección IP sea en su lugar enviada hacia el atacante. Este ataque es utilizado como un comienzo para un ataque de Hombre En el Medio.”

  Según (Herrero, 2008). indicia que “Ettercap es un sniffer/interceptor/logger para redes LAN con switchs, que soporta la disección activa y pasiva de muchos protocolos (incluso cifrados) e incluye muchas características para el análisis de la red y del host (anfitrión).”

  Entre sus funciones, las más destacadas son las siguientes:

  - Inyección de caracteres en una conexión establecida emulando comandos o respuestas mientras la conexión está activa.

  - Compatibilidad con SSH1: Puede interceptar users y passwords incluso en conexiones “seguras” con SSH.
  - Compatibilidad con HTTPS: Intercepta conexiones mediante http SSL (supuestamente seguras) incluso si se establecen a través de un proxy.
  - Intercepta tráfico remoto mediante un túnel GRE: Si la conexión se establece mediante un túnel GRE con un router Cisco, puede interceptarla y crear un ataque “Man in the Middle”.
  - “Man in the Middle” contra túneles PPTP (Point-to-Point Tunneling Protocol).
  - Soporte para Plug-ins.

- NESSUS: “Es una potente aplicación de detección de vulnerabilidades muy usada tanto por los hackers, como por los expertos en seguridad informática cuando tienen que realizar auditorías, Nessus es un programa de escaneo de vulnerabilidades en diversos sistemas operativos. Consiste en un demonio o diablo, nessusd, que realiza el escaneo en el sistema objetivo, y nessus, el cliente (basado en consola o gráfico) que muestra el avance e informa sobre el estado de los escaneos. Desde consola nessus puede ser programado para hacer escaneos programados con cron.” (Linux, 2018)

  En operación normal, nessus comienza escaneando los puertos con nmap o con su propio escaneador de puertos para buscar puertos abiertos y después intentar varios exploits para atacarlo. Las pruebas de vulnerabilidad, disponibles como una larga lista de plugins, son escritos en NASL (Nessus Attack Scripting Language, Lenguaje de Scripting de Ataque Nessus por sus siglas en inglés), un lenguaje scripting optimizado para interacciones personalizadas en redes.

- SOCIAL ENGINEERING TOOLKIT: “Disponible para Linux y Mac OS X, Social Engineering Toolkit (conocido como SET) es un marco de prueba de penetración de código abierto basado en Python que lo ayudará a lanzar ataques de Ingeniería Social en muy poco tiempo.” (SECURITYTRAILS, 2018)

  Tipos de ataque que puede lanzar SET

  - Ataques basados en WiFi AP: este tipo de ataque redirigirá o interceptará paquetes de usuarios que usan nuestra red WiFi
  - SMS y ataques de correo electrónico: aquí, SET intentará engañar y generar un correo electrónico falso para obtener credenciales sociales
  - Ataques basados en la web: le permite clonar una página web para que pueda atraer a usuarios reales mediante ataques de suplantación de identidad o phishing.
  - Creación de cargas útiles (.exe): SET creará un archivo .exe malicioso que, después de ejecutarse, comprometerá el sistema del usuario que hace clic en él.
  - Pruebas de penetración rápida.
  - Integración con módulos de terceros.
  - Generador de ataques de phishing
  - Lanzar ataques QRCode
  - Soporte para vectores de ataque Powershell

  Según (Luz, 2016). indicia que “Cuando se audita la seguridad informática de una empresa, siempre se debe auditar también al eslabón más débil: las personas. La ingeniería social es la práctica de obtener información confidencial a través de la manipulación de usuarios legítimos del sistema, con el único objetivo de obtener información, acceso al sistema e incluso privilegios elevados en dicho sistema. SET, o

también conocido como Social-Engineer Toolkit te permitirá practicar estas técnicas fácilmente.”

Es un framework de código abierto para realizar pentesting de sistemas y redes, enfocado específicamente en ataques de ingeniería social para conseguir su objetivo. SET tiene una serie de herramientas para realizar ataques personalizados que nos permitirán realizar un ataque de manera rápida y efectiva. Esta herramienta ha sido desarrollada por la firma de seguridad TrustedSec y está disponible de manera libre para todos nosotros.

2.22.2. Base de Datos.

Según (Lockhart, 1996-9). indicia que “POSTGRESQL Los sistemas de mantenimiento de Bases de Datos relacionales tradicionales (DBMS, s) soportan un modelo de datos que consisten en una colección de relaciones con nombre, que contienen atributos de un tipo específico. En los sistemas comerciales actuales, los tipos posibles incluyen numéricos de punto flotante, enteros, cadenas de caracteres, cantidades monetarias y fechas. Está generalmente reconocido que este modelo será inadecuado para las aplicaciones futuras de procesado de datos. El modelo relacional sustituyó modelos previos en parte por su "simplicidad espartana". Sin embargo, como se ha mencionado, esta simplicidad también hace muy difícil la implementación de ciertas aplicaciones. Postgres ofrece una potencia adicional sustancial al incorporar los siguientes cuatro conceptos adicionales básicos en una vía en la que los usuarios pueden extender fácilmente el sistema.”

- clases
- herencia
- tipos
- funciones

Otras características aportan potencia y flexibilidad adicional:

- Restricciones (Constraints)
- Disparadores (triggers)
- Reglas (rules)
- Integridad transaccional

Según (Lockhart, 1996-9). indicia que “Estas características colocan a Postgres en la categoría de las Bases de Datos identificadas como objeto-relacionales. Nótese que éstas son diferentes de las referidas como orientadas a objetos, que en general no son bien aprovechables para soportar lenguajes de Bases de Datos relacionales tradicionales. Postgres tiene algunas características que son propias del mundo de las bases de datos orientadas a objetos. De hecho, algunas Bases de Datos comerciales han incorporado recientemente características en las que Postgres fue pionera.”

SQL se ha convertido en el lenguaje de consulta relacional más popular. El nombre “SQL” es una abreviatura de Structured Query Language (Lenguaje de consulta estructurado). En 1974 Donald Chamberlain y otros definieron el lenguaje SEQUEL (Structured English Query Language) en IBM Research. Este lenguaje fue implementado inicialmente en un prototipo de IBM llamado SEQUEL-XRM en 1974-75. En 1976-77 se definió una revisión de SEQUEL llamada SEQUEL/2 y el nombre se cambió a SQL.

2.22.3. servidor WEB.

Según (B., 2019). indicia que “APACHE HTTP Server es un software de servidor web gratuito y de código abierto para plataformas Unix con el cual se ejecutan el 46% de los sitios web de todo el mundo. Es mantenido y desarrollado por la Apache Software Foundation.

Les permite a los propietarios de sitios web servir contenido en la web, de ahí el nombre de servidor web. Es uno de los servidores web más antiguos y confiables, con la primera versión lanzada hace más de 20 años, en 1995."

Cuando alguien quiere visitar un sitio web, ingresa un nombre de dominio en la barra de direcciones de su navegador. Luego, el servidor web envía los archivos solicitados actuando como un repartidor virtual.

Según (B., 2019). indicia que "Aunque llamamos a Apache un servidor web, no es un servidor físico, sino un software que se ejecuta en un servidor. Su trabajo es establecer una conexión entre un servidor y los navegadores de los visitantes del sitio web (Firefox, Google Chrome, Safari, etc.) mientras envían archivos entre ellos (estructura cliente-servidor). Apache es un software multiplataforma, por lo cual funciona tanto en servidores Unix como en Windows."

CAPITULO III

MARCO APLICATIVO

3.1. INTRODUCCIÓN

En este capítulo se aplicará lo mencionado en capítulos anteriores, el desarrollo del prototipo, aplicado casos de uso, costo.

3.2. ESQUEMA DEL SISTEMA

El siguiente grafico muestra la estructura del prototipo.

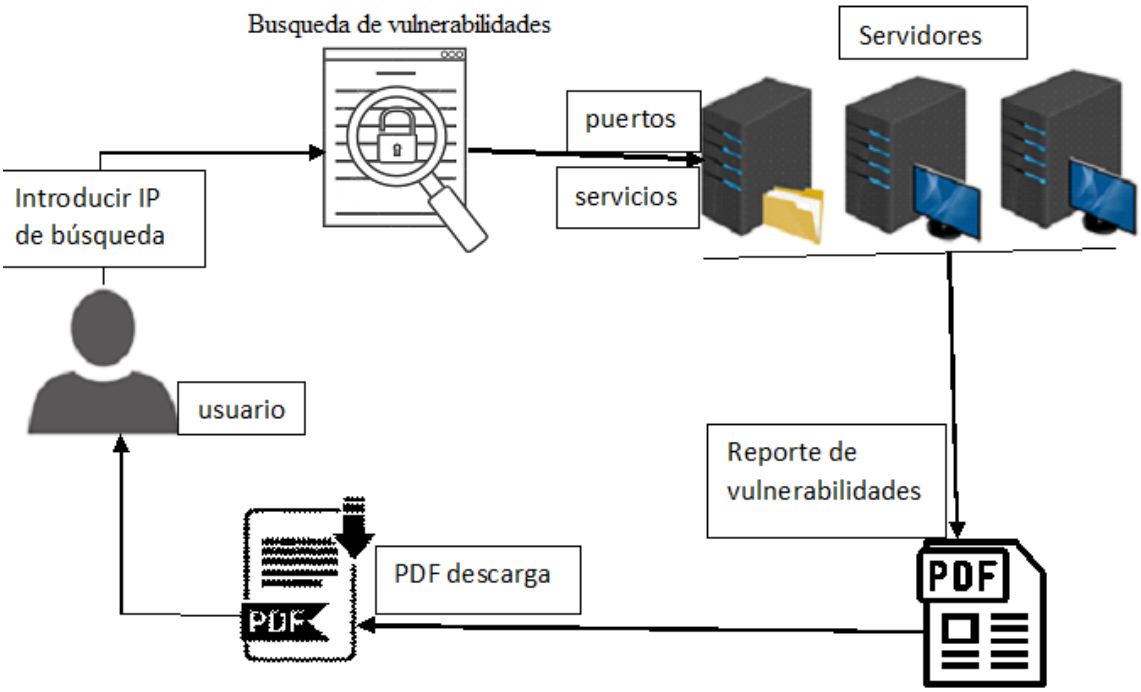


Figura: 3.1 Esquema de prototipo.

Fuente: [Elaboración propia]

3.3. APLICACIÓN DE LA METODOLOGÍA ESCOGIDA (UWE)

3.3.1 Requerimientos funcionales del prototipo.

Tabla: 3.1. *Tabla de requerimientos funcionales*

REFERENCIA	FUNCION	CATEGORIA
R. 1	Test y protocolos de seguridad.	Oculto

R. 2	Analizar las vulnerabilidades que existe en sus servidores.	Oculto
R. 3	Dar reportes de vulnerabilidades.	Evidente
R. 4	Control al usuario en accesos y tareas.	Oculto

Fuente: [Elaboración propia]

3.3.2. Requerimientos no funcionales del prototipo.

Para el prototipo de modelo de seguridad para infraestructura de la información debe contar con los siguientes requerimientos:

Instalar Kali Linux, Contar con acceso a internet, tener una IP publica, tener conocimientos básicos en el manejo de una computadora.

3.3.3. Diagrama de caso de uso de uso general

En la figura 3.1 Se da a conocer el diagrama de caso de uso general del modelo de seguridad para infraestructura de información.

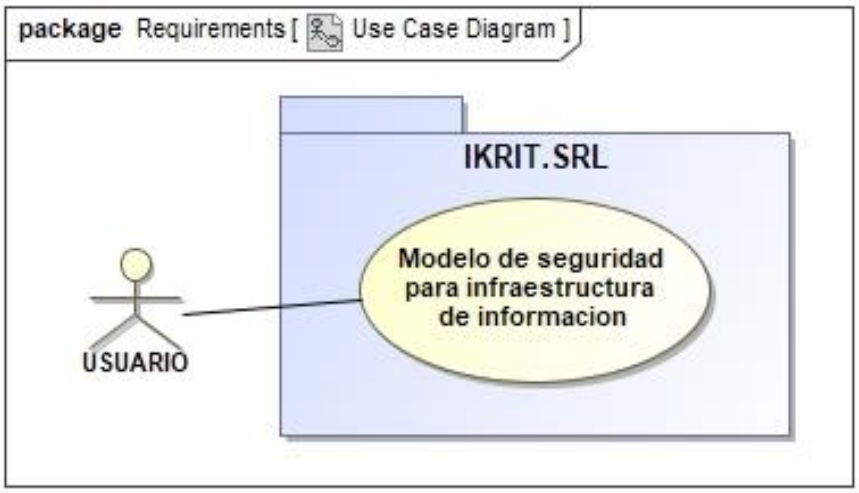


Figura: 3.2 Diagrama De Caso De Uso General Del modelo de seguridad.

Fuente: [Elaboración propia]

3.3.3.1. Documentos De Especificación De Caso De Uso De Alto Nivel

En la siguiente tabla 3.2. se detalla el documento de especificación de caso de uso de alto nivel.

Tabla: 3.2. *Tabla de Especificación De Caso De Uso De Alto Nivel*

Caso de uso:	**Modelo de seguridad para infraestructura de información**
Actores:	Usuario
Tipo:	Primario
Descripción:	El modelo de seguridad tiene por objetivo verificar IP's.

Fuente: [Elaboración propia]

3.3.4. Diagrama de caso de uso a nivel expandido.

En la figura 3.3 se da a conocer el diagrama de caso de uso Administrar Usuario de nivel expandido del modelo de seguridad para infraestructura de información.

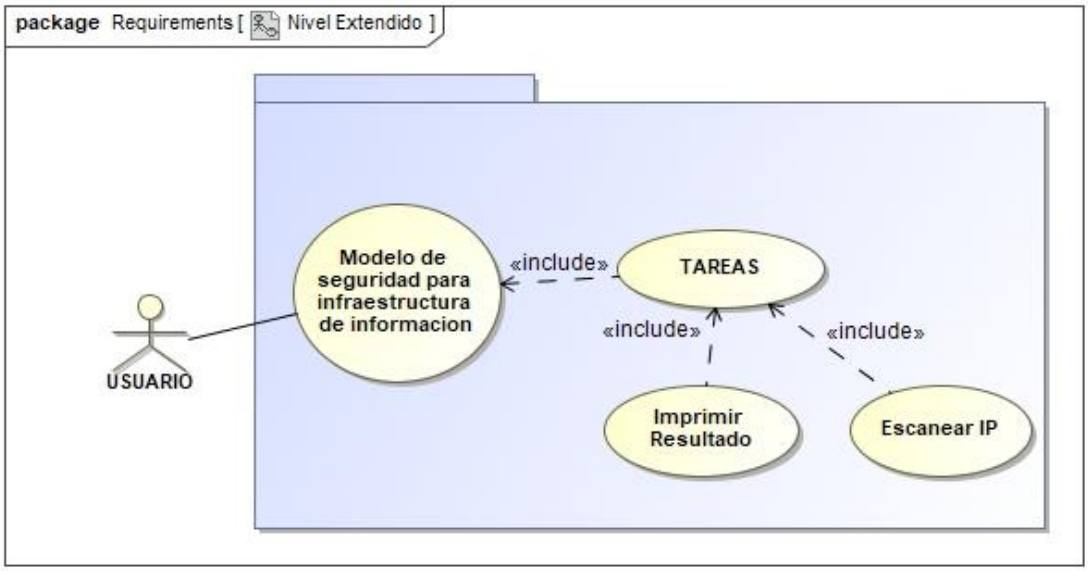


Figura: 3.3 Diagrama de caso de uso a nivel expandido.

Fuente: [Elaboración propia]

3.2.4.1. Documento de Especificación de Casos de Uso de Nivel Expandido

En la tabla 3.3 se encuentra el documento de especificación de caso de uso de nivel expandido.

Tabla: 3.3. *Tabla de Especificación de Casos de Uso de Nivel Expandido*

Caso de uso:	Modelo de seguridad para infraestructura de información
Actores:	Usuario
Tipo:	Primario
Descripción	El usuario ingresara al modelo de seguridad de infraestructura de información para realizar una búsqueda de vulnerabilidades que tiene su sistema.
Pre-condiciones:	Contar con internet

Actores:	**Prototipo:**
El usuario ingresara al prototipo.	El prototipo mostrara la vista al ingreso del sistema
El usuario ingresara el nombre de usuario y contraseña	El prototipo permitirá el ingreso del usuario si es correcto los datos.
El usuario ingresara a la vista inicial del prototipo.	El prototipo mostrara las siguientes opciones: • Inicio • Buscar Buscar vulnerabilidad Reportes

	Resultados
El usuario ingresara a la pestaña de Buscar y seleccionara la opción Buscar vulnerabilidades	En esta opción que dice escanear una vez haciéndole click nos mostrará una ventana en el cual se pondrá la dirección IP y búsqueda rápida, Y una vez echo eso comenzara a buscar las vulnerabilidades que hay en la IP que puso. Igualmente se podrá descargar el reporte en PDF de las vulnerabilidades que encontró. También tenemos botones que nos permitirá, parar (stop), iniciar (start), borrar(delete).
El usuario ingresara a la pestaña de buscar y seleccionara la opción reportes	En esta opción podremos visualizar en una tabla el reporte de la IP que se escaneo
El usuario ingresara a la pestaña de buscar y seleccionara la opción Resultados	En esta opción el usuario podrá visualizar los resultados que muestre el escaneo de la dirección IP.

Fuente: [Elaboración propia]

3.3.5. Diagrama de modelo conceptual

En esta figura se da a conocer el diagrama conceptual

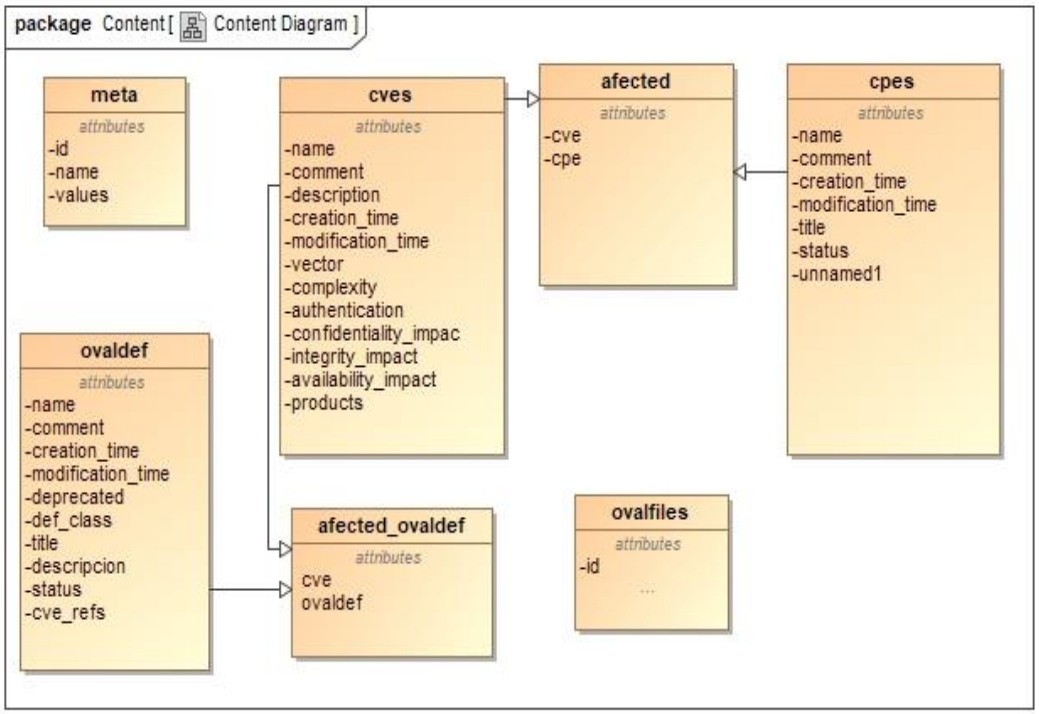


Figura: 3.4. figura de modelo de navegación.

Fuente: [Elaboración propia]

3.3.6. Diagrama de Modelos de Navegación.

En esta figura se muestra es el modelo de navegación del prototipo.

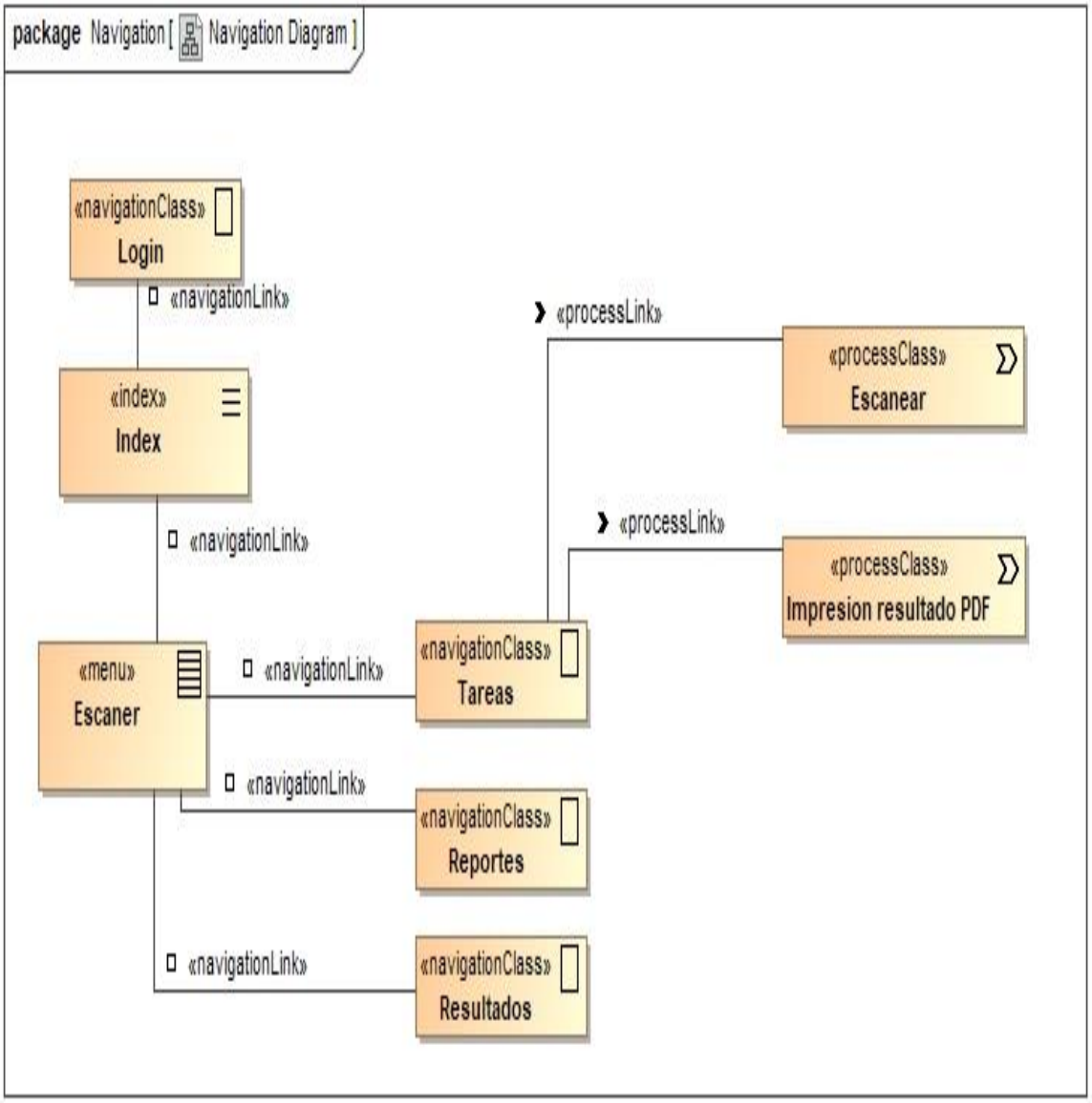


Figura: 3.5. figura de modelo de navegación.

Fuente: [Elaboración propia]

3.3.7. Diagrama de Modelo de Presentación.

En el diagrama 3.6. podremos apreciar la interfaz de Inicio de sección que tendrá el prototipo.

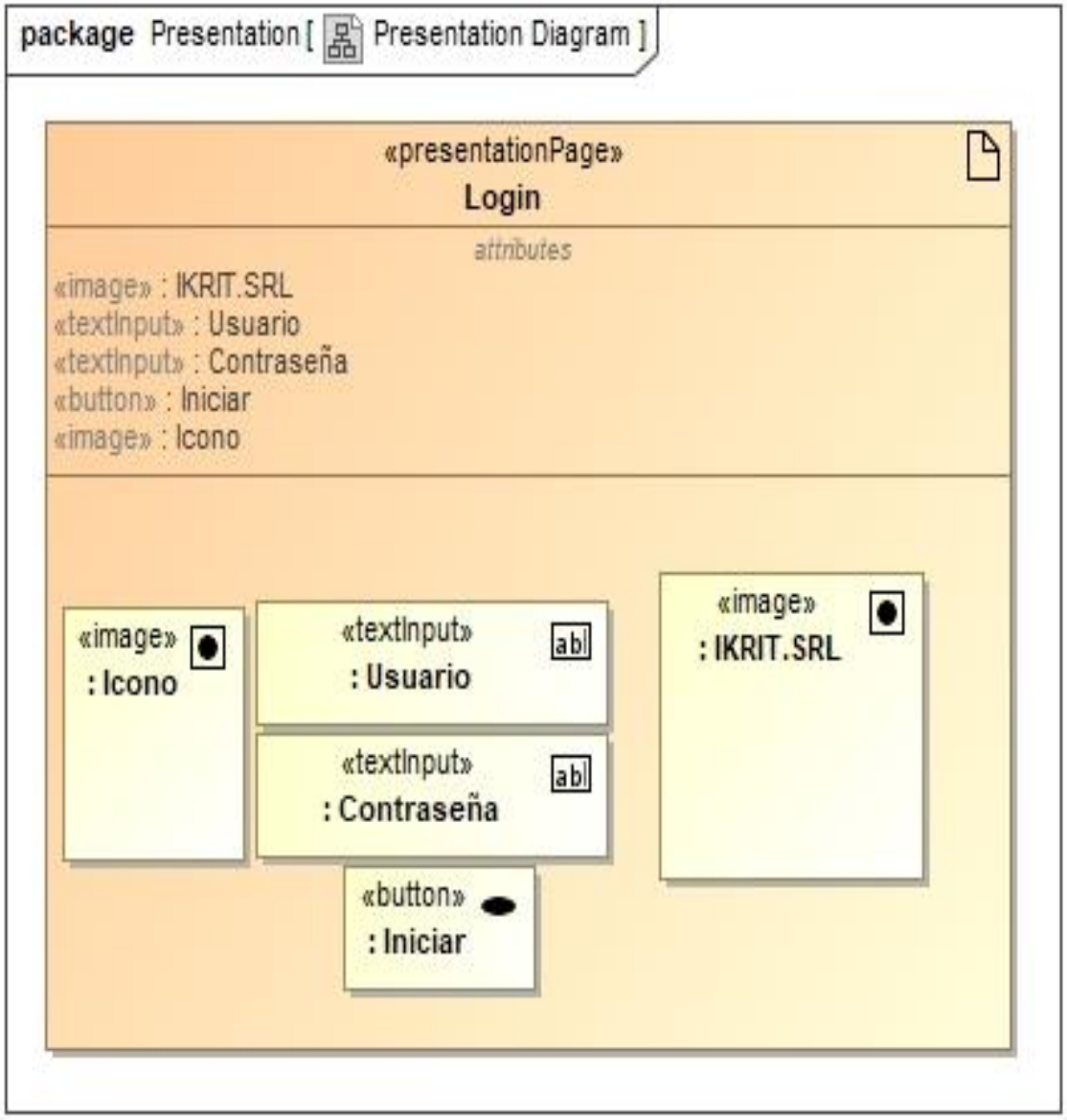


Figura: 3.6. diagrama de Inicio de sesión.

Fuente: [Elaboración propia]

En la figura 3.7. apreciara la interfaz de inicio.

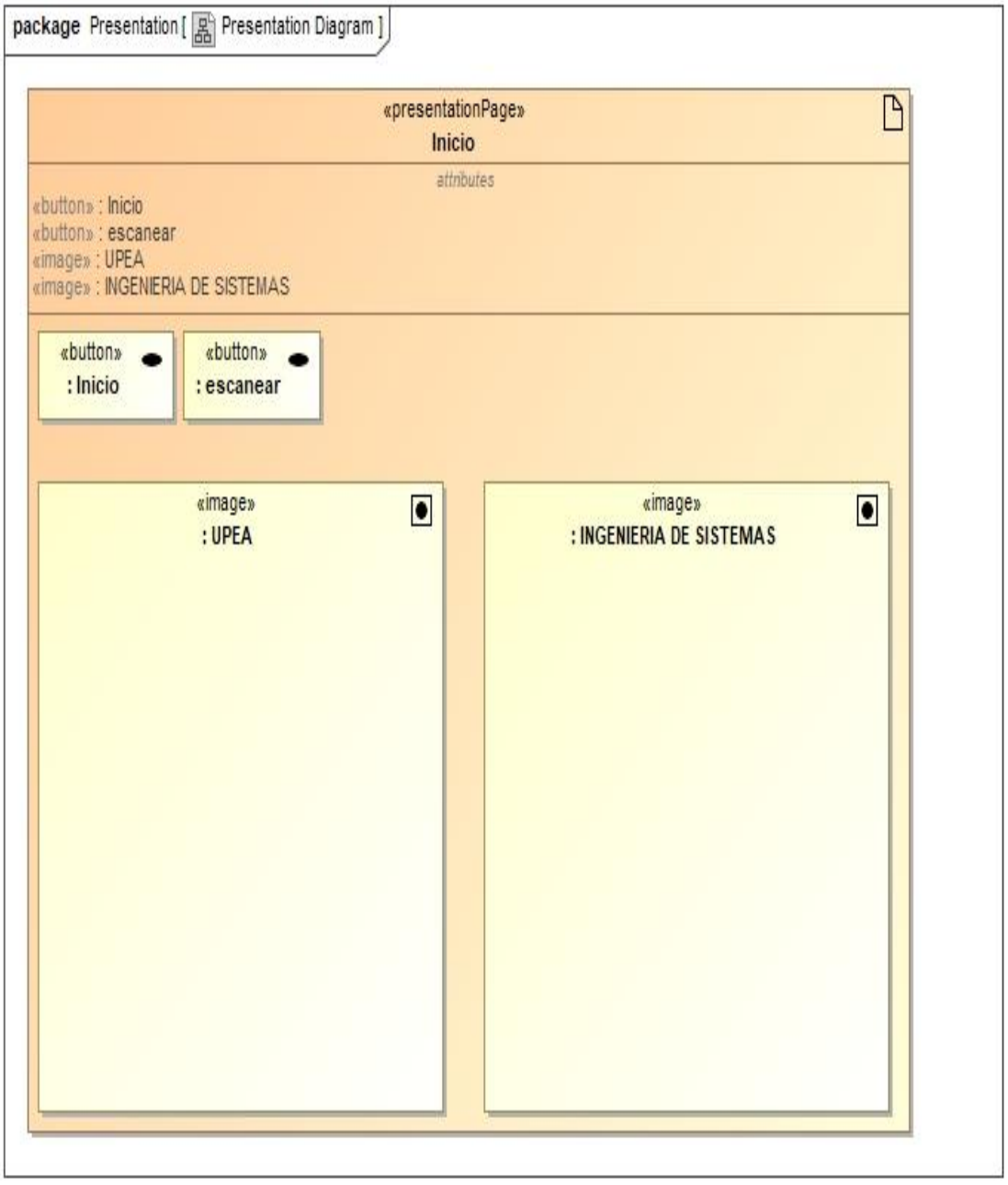


Figura: 3.7. diagrama de inicio.

Fuente: [Elaboración propia]

En la figura 3.8. apreciara la interfaz de tareas.

Figura: 3.8. diagrama de tareas.

Fuente: [Elaboración propia]

En la figura 3.9. apreciara la interfaz en el cual se pone la IP publica a la que se quiere escanear.

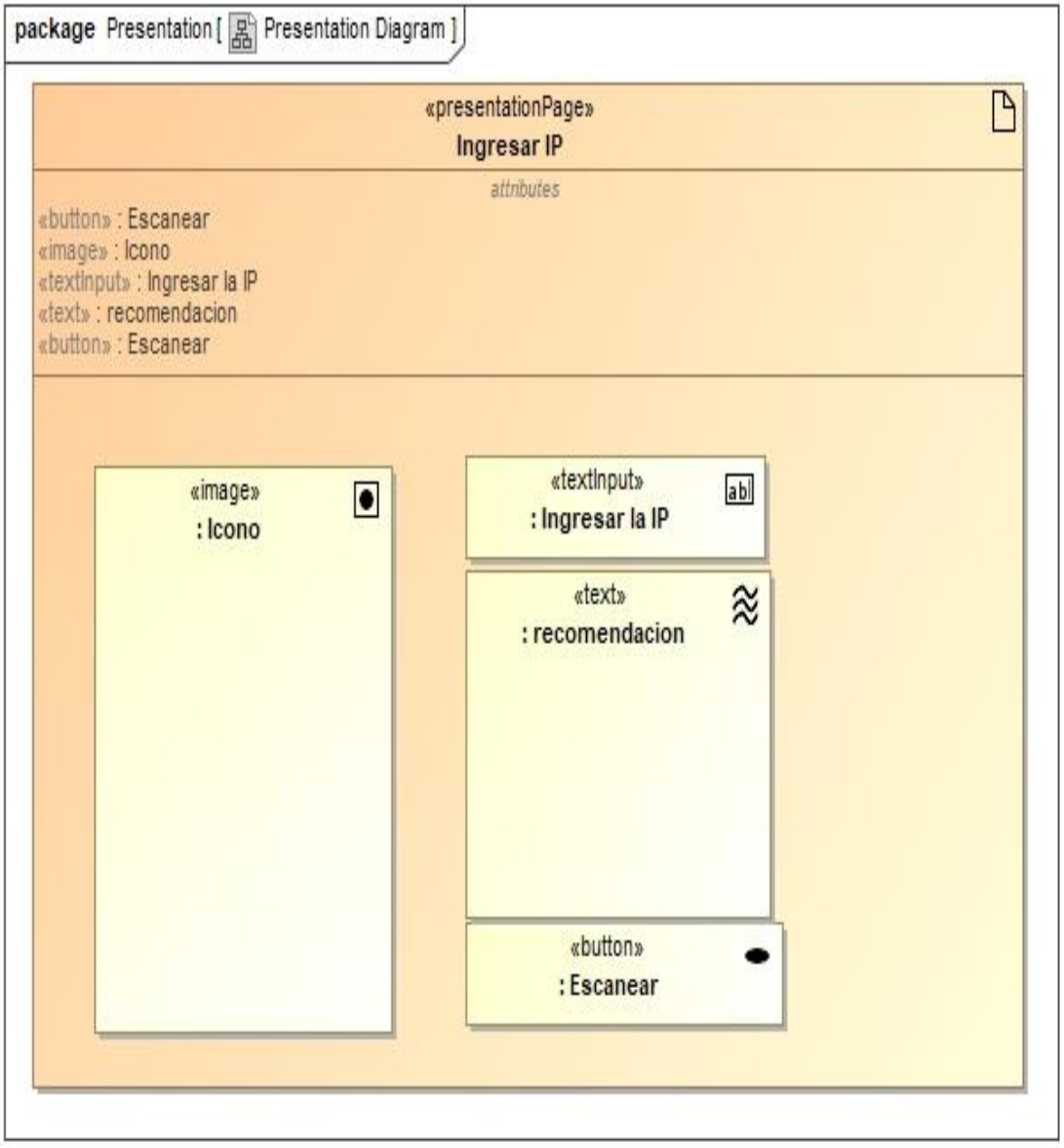


Figura: 3.9. diagrama en la que se introduce la IP.

Fuente: [Elaboración propia]

En la figura 3.10. podrá apreciar la interface de cómo sacar reporte en PDF.

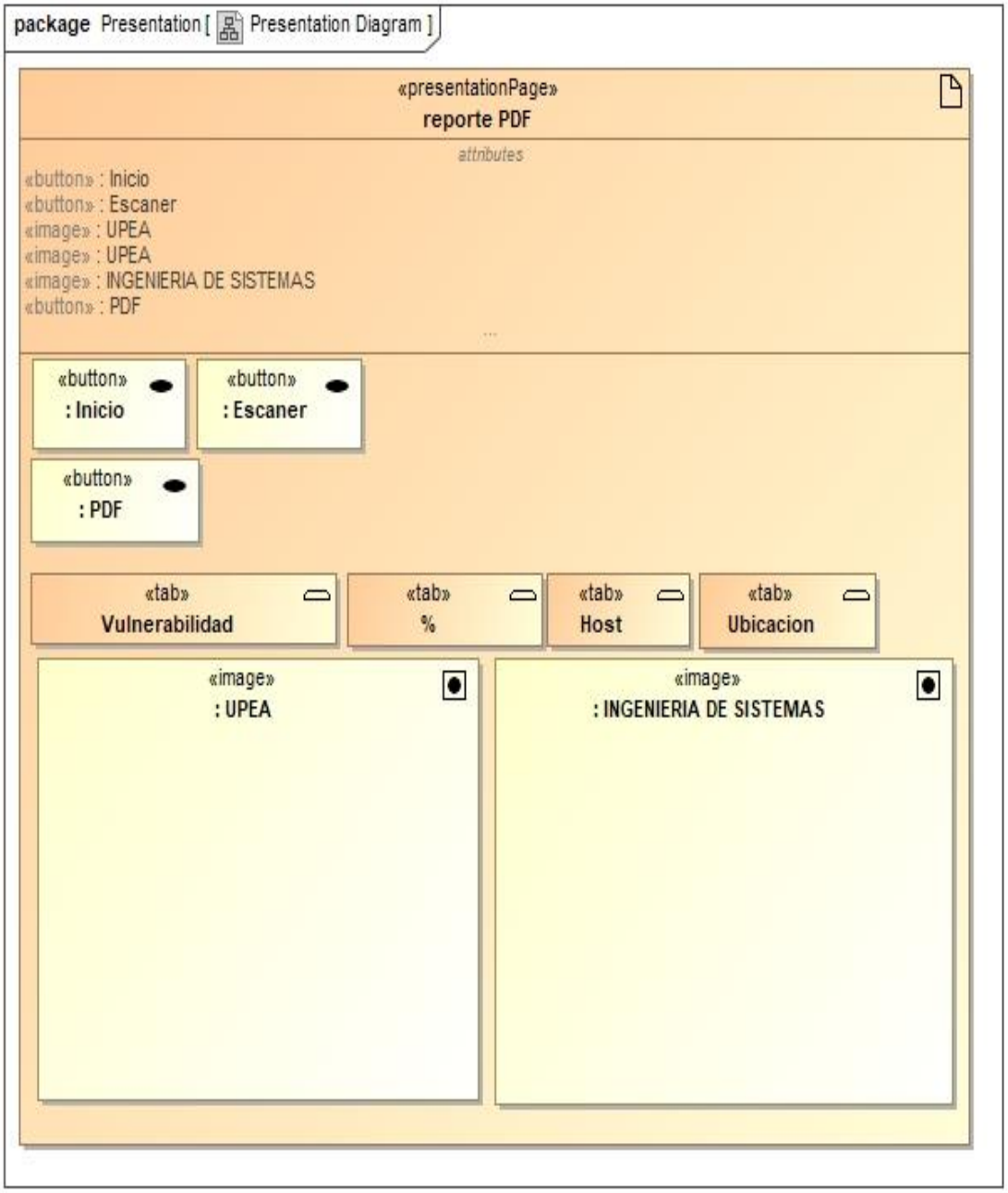


Figura: 3.10. diagrama de sacar reporte en PDF.

Fuente: [Elaboración propia]

En la figura 3.11. podrá visualizar la interfaz de reportes.

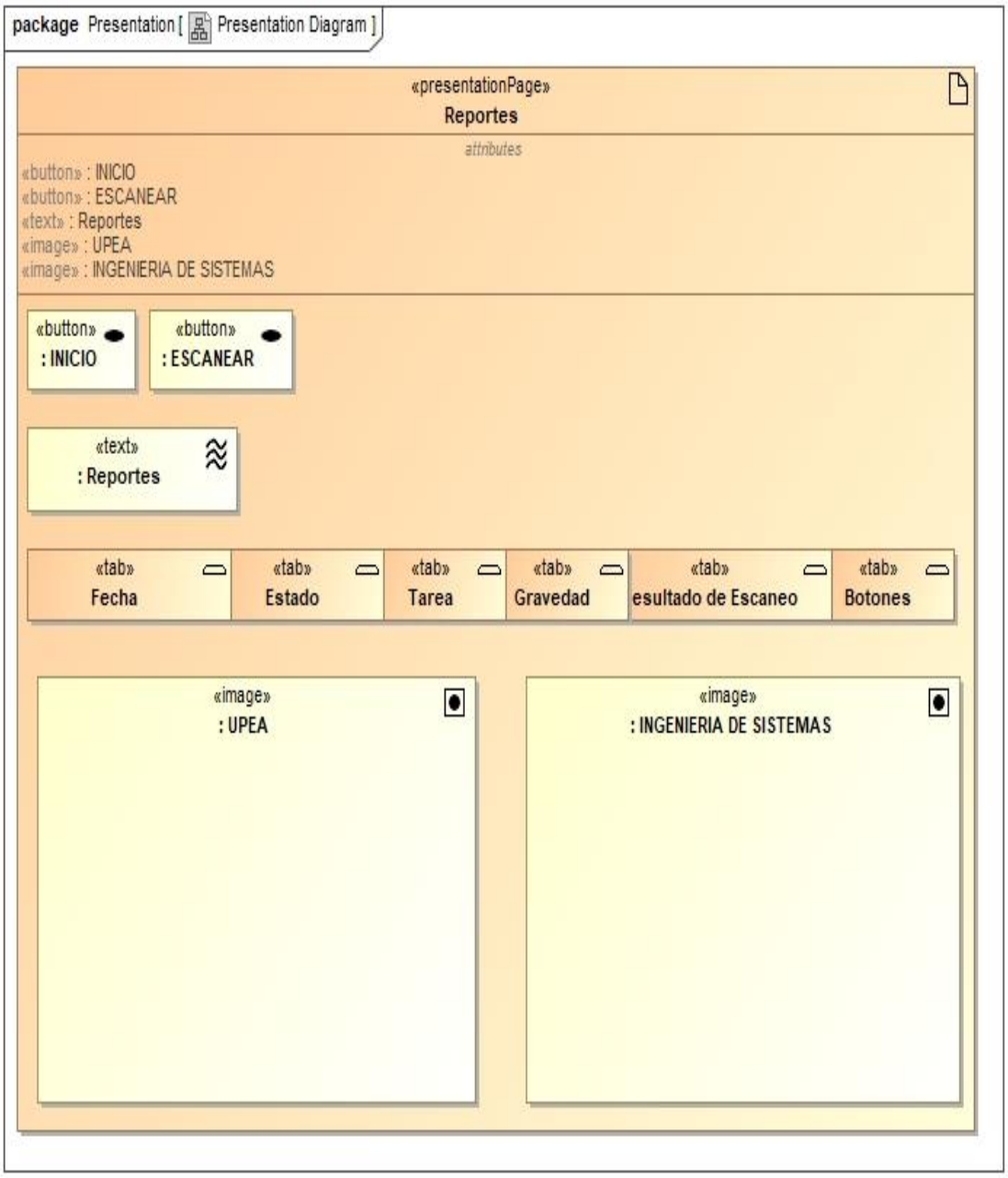


Figura: 3.11. diagrama de reportes.

Fuente: [Elaboración propia]

En la figura 3.12. podrá visualizar la interfaz de resultados.

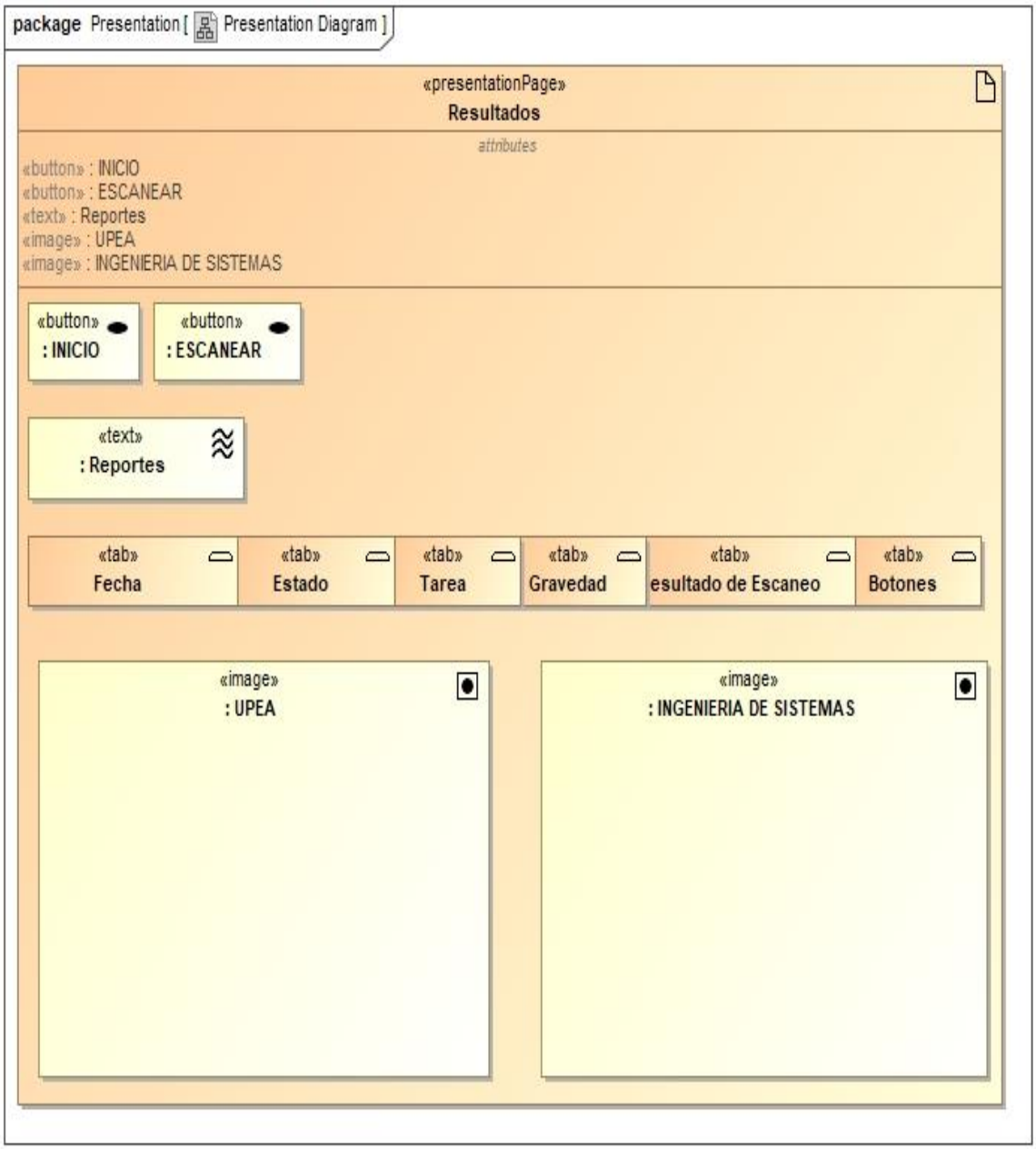


Figura: 3.12. diagrama de visualización de resultados.

Fuente: [Elaboración propia]

3.4. DESARROLLO E IMPLEMENTACIÓN

En el desarrollo e implementación se dar a conocer bocetos de cada interfaz del sistema.

En la figura 3.13. se muestra la figura de iniciar sesión.

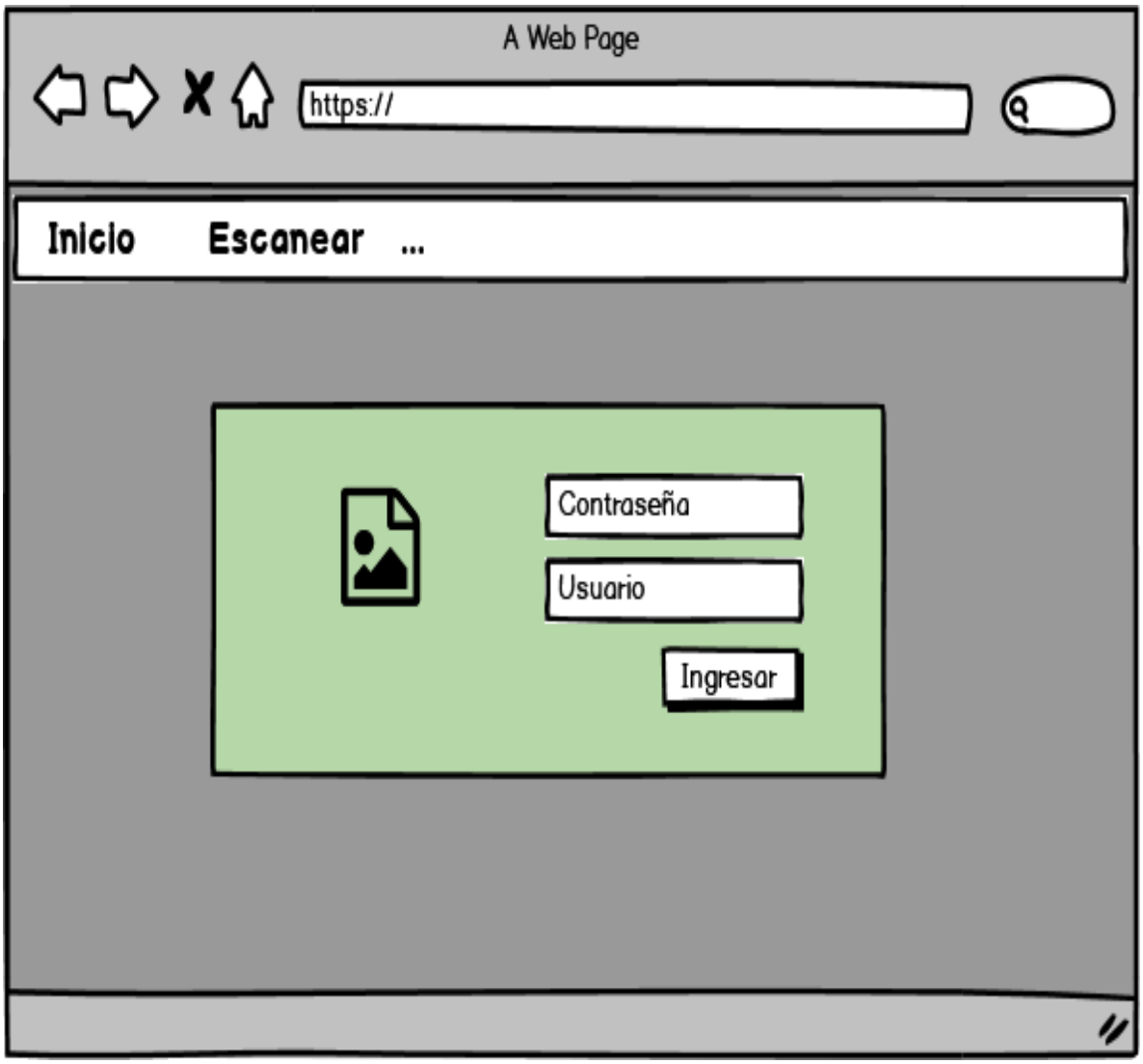


Figura: 3.13. boceto de interfaz de iniciar sesión.

Fuente: [Elaboración propia]

En la figura 3.14. se aprecia un boceto del inicio.

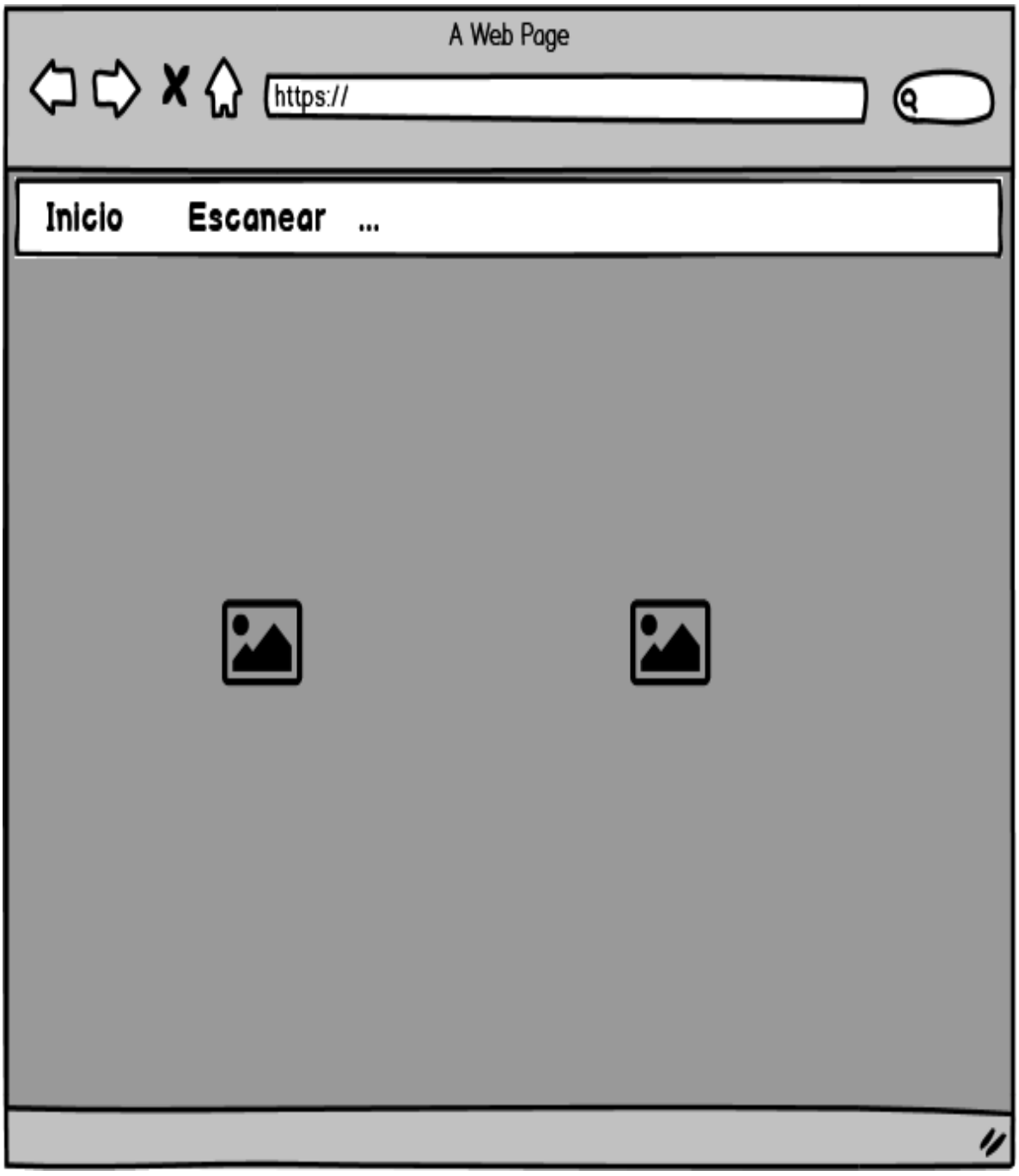


Figura: 3.14. boceto de interfaz de inicio.

Fuente: [Elaboración propia]

En la figura 3.15. se aprecia un boceto de tareas.

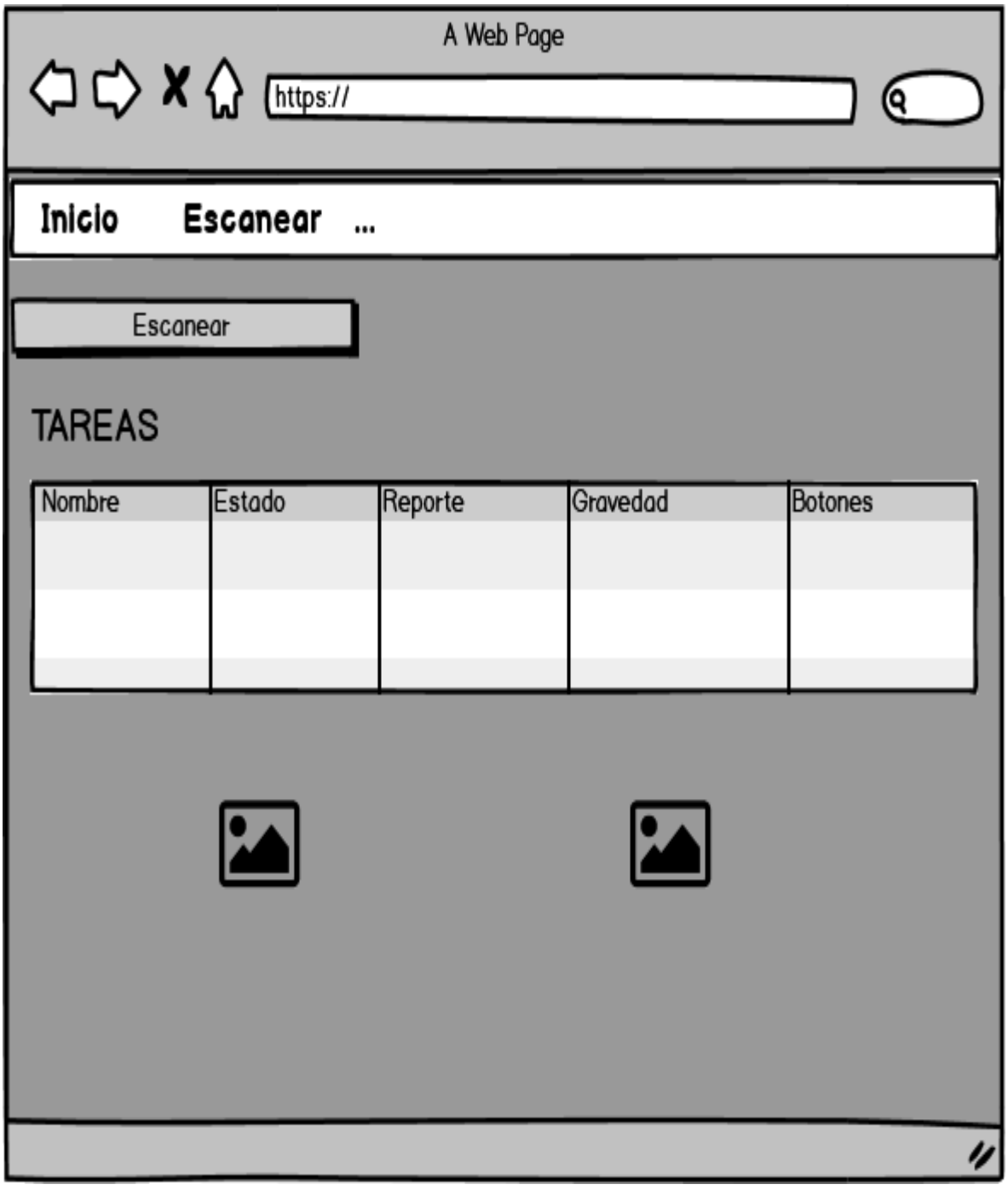


Figura: 3.15. boceto de interfaz de tarea.

Fuente: [Elaboración propia]

En la figura 3.16. se aprecia un boceto de reporte.

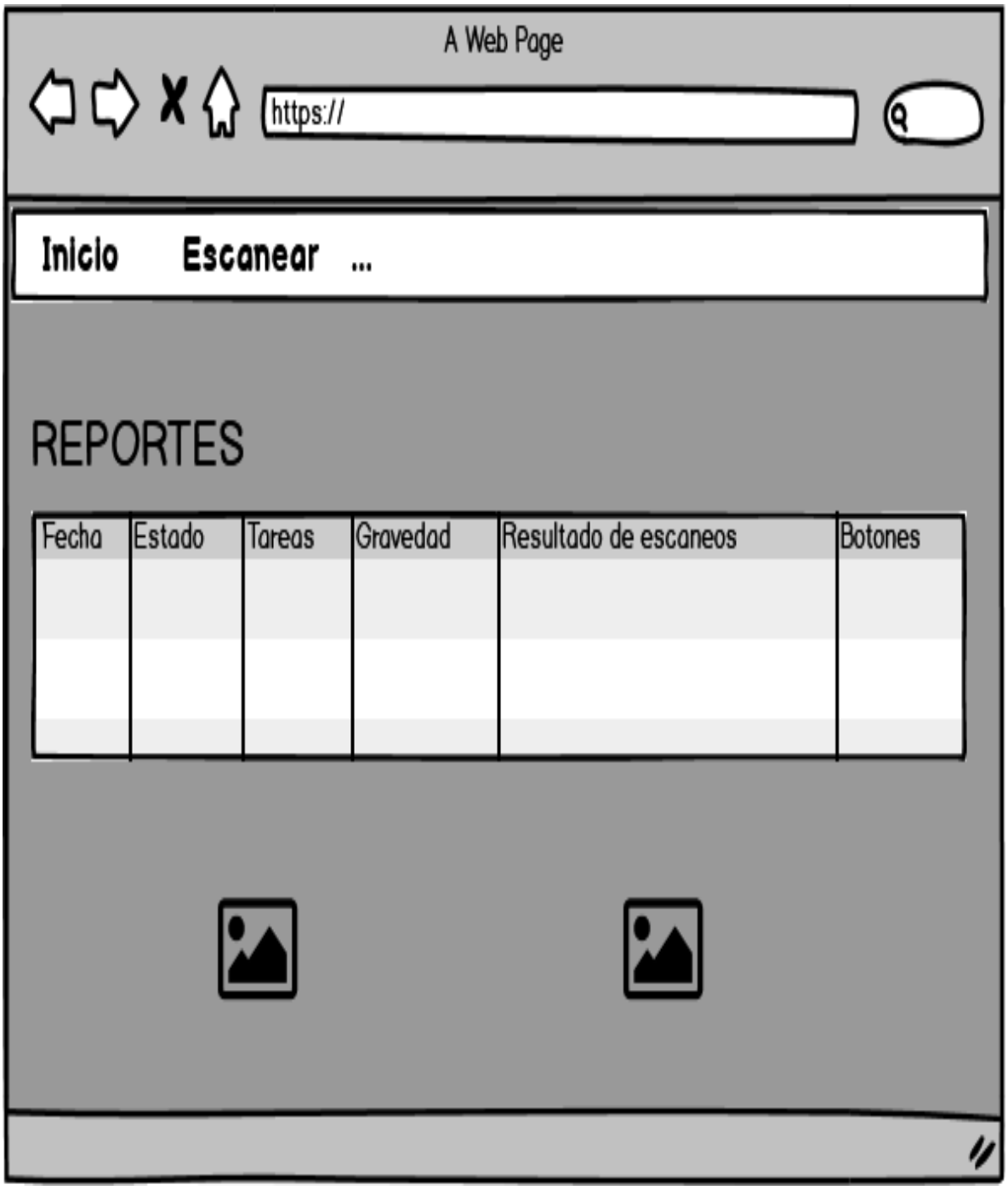


Figura: 3.16. boceto de interfaz de reporte.

Fuente: [Elaboración propia]

En la figura 3.17. se aprecia un boceto de resultado.

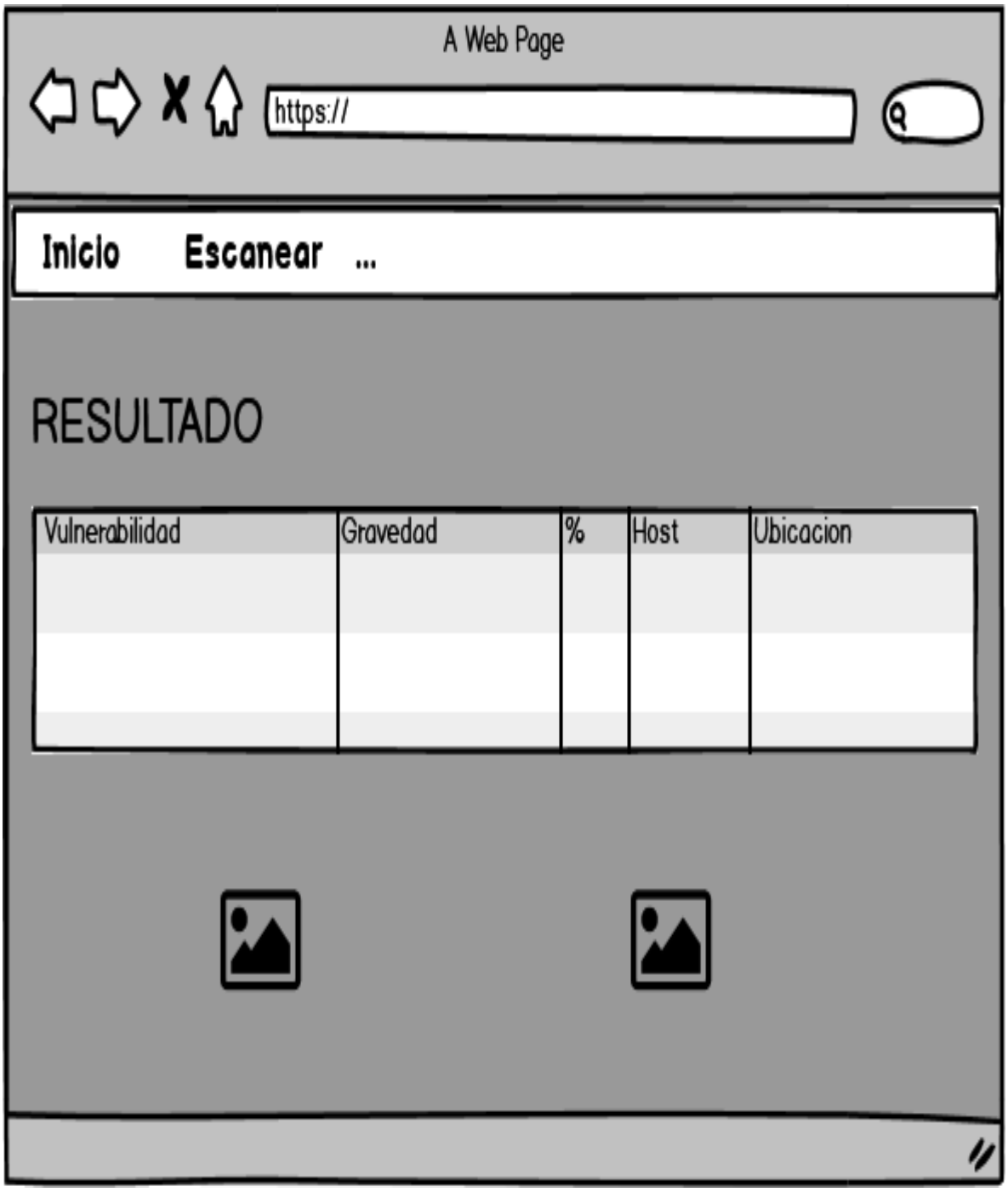


Figura: 3.17. boceto de interfaz de resultado.

Fuente: [Elaboración propia]

En la figura 3.18. se aprecia un boceto de impresión de PDF

Figura: 3.18. boceto de interfaz de Impresión de PDF.

Fuente: [Elaboración propia]

3.4.1. Implementación.

Se mostrará las capturas de pantalla del prototipo

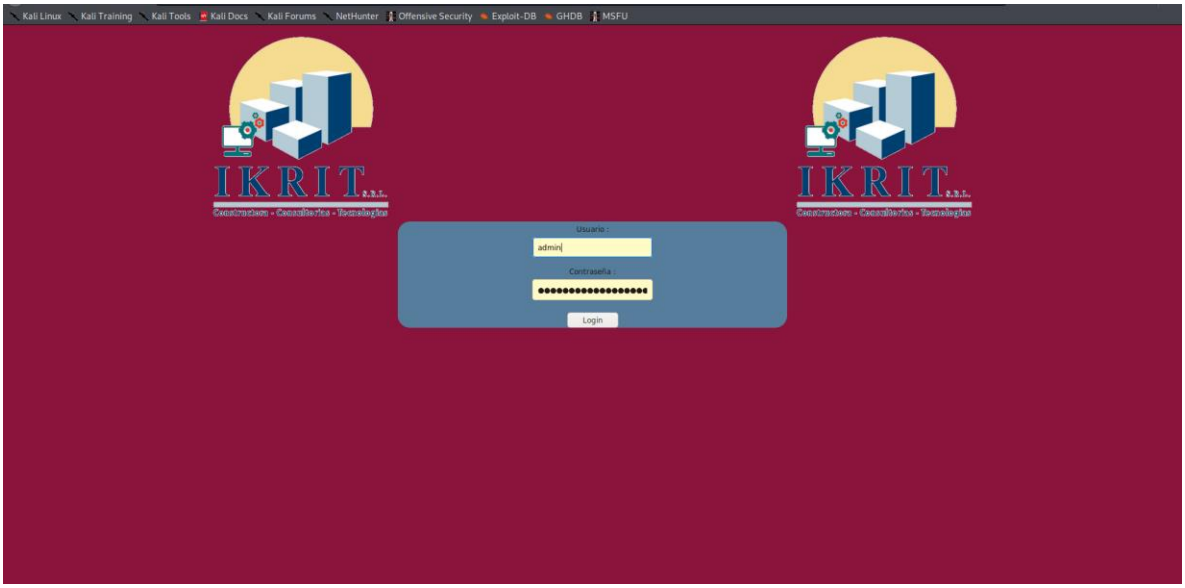


Figura: 3.19. en la siguiente figura se muestra donde tienen que ingresar el inicio de sesión.

Fuente: [Elaboración propia]

```
        <br/>
      </div>
    </div>
    <input type="submit" class="btn btn-success" tabindex="3" value="{gsa:i18n('Iniciar sesion', 'Action Verb')}" />
  </form>
```

Figura: 3.20. en la siguiente figura se muestra donde tienen que ingresar el inicio de sesión

Fuente: [Elaboración propia]

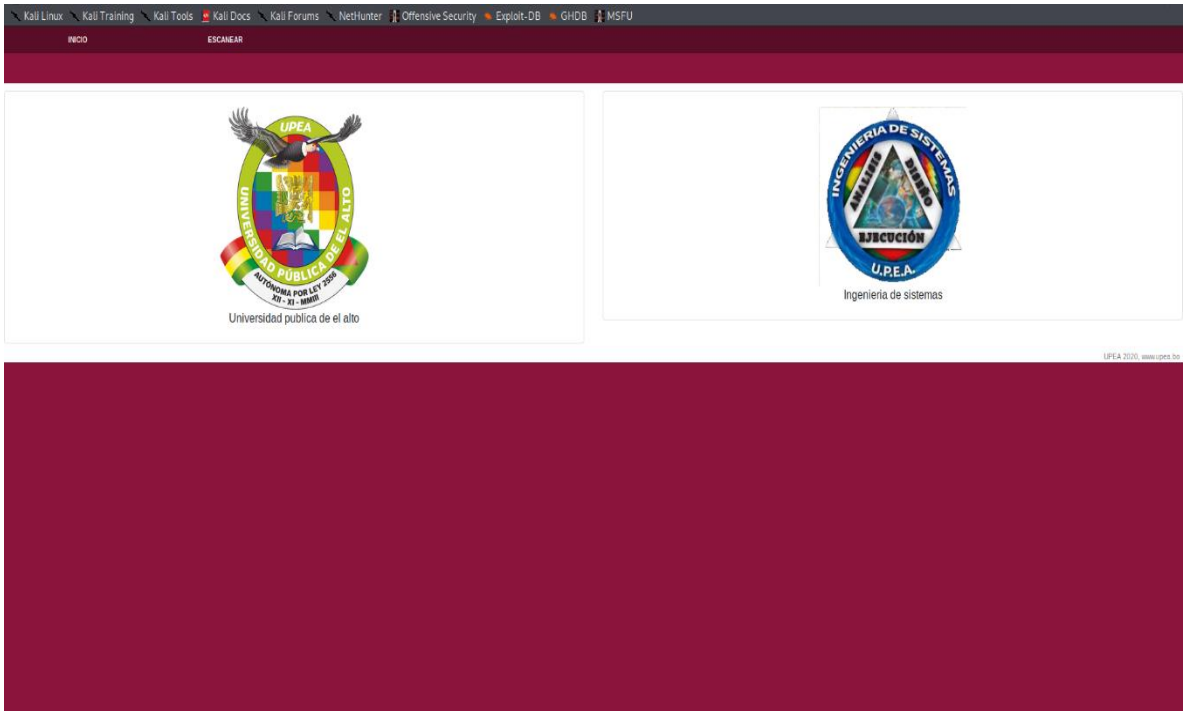


Figura: 3.21. en esta figura mostramos el inicio.

Fuente: [Elaboración propia]

```
<div class="card-body">
  <img class="card-img-top" src="/img/upea.png" alt="" style="width:15rem;"/>
  <p class="card-text">Universidad publica de el alto</p>
</div>
```

Figura: 3.22. en esta figura mostramos el inicio.

Fuente: [Elaboración propia]

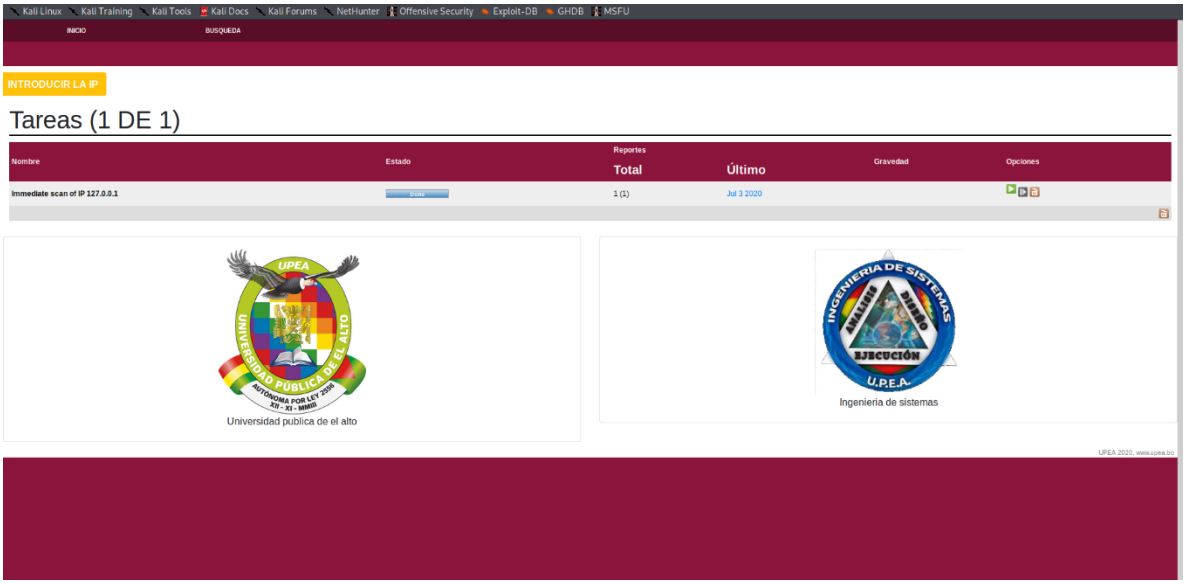


Figura: 3.23. en esta figura se muestra el inicio de la búsqueda.

Fuente: [Elaboración propia]

```
    <name><xsl:value-of select="gsa:i18n('Fecha')"/></name>
    <field>fecha</field>
    <sort-reverse/>
  </column>
  <column>
    <name><xsl:value-of select="gsa:i18n('Estado')"/></name>
    <field>estado</field>
  </column>
  <column>
    <name><xsl:value-of select="gsa:i18n('Tareas')"/></name>
    <field>tareas</field>
```

Figura: 3.24. en esta figura se muestra el inicio de la búsqueda.

Fuente: [Elaboración propia]

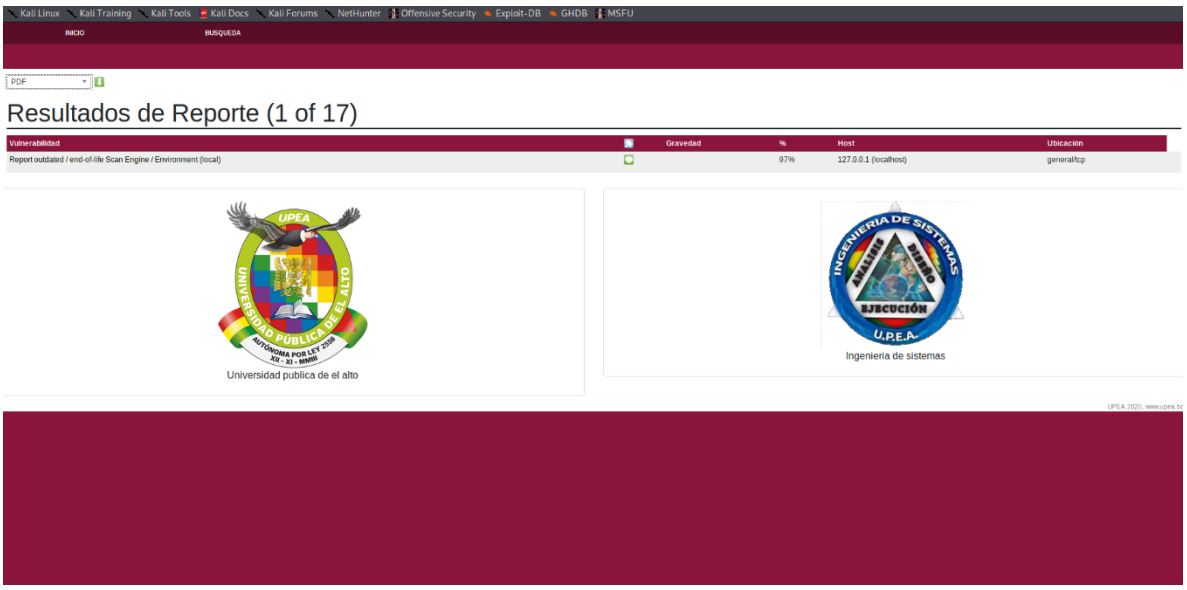


Figura: 3.25. en esa figura mostramos como puede descargar el informe en PDF

Fuente: [Elaboración propia]

```
<xsl:text>Resultados de Reporte (</xsl:text>
<xsl:choose>
  <xsl:when test="$full-count != ''">
    <xsl:value-of select="gsa-i18n:strformat (gsa:i18n ('%1 of %2'), $filtered-count, $full-count)"/>
  </xsl:when>
  <xsl:otherwise>
    <xsl:value-of select="$filtered-count"/>
  </xsl:otherwise>
</xsl:choose>
```

Figura: 3.26. en esa figura mostramos como puede descargar el informe en PDF.

Fuente: [Elaboración propia]

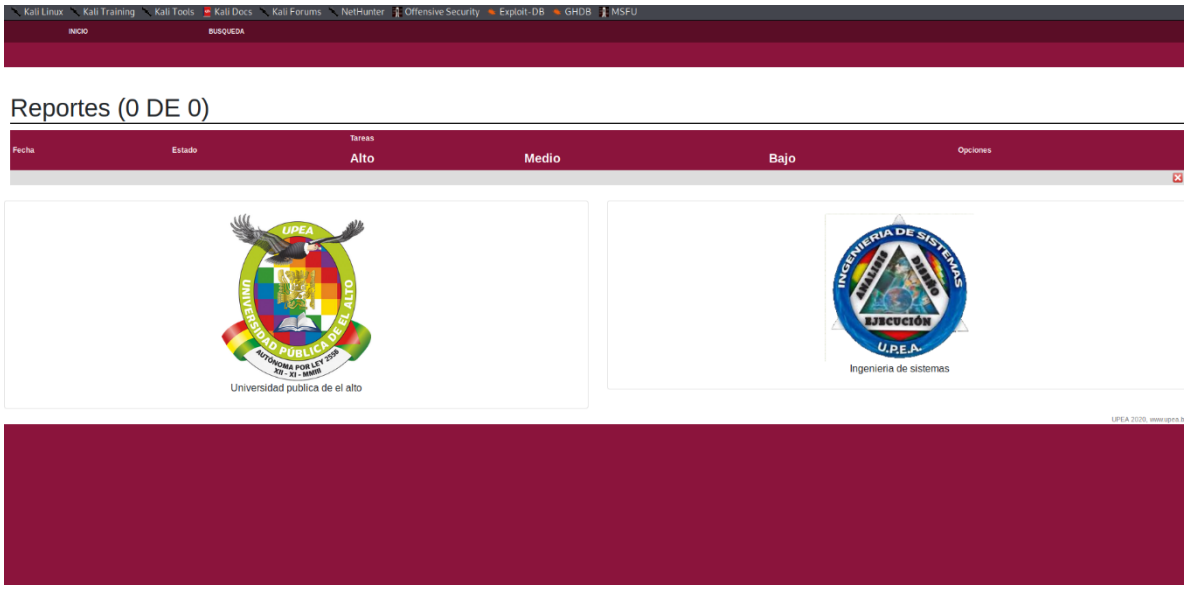


Figura: 3.27. en la siguiente figura se muestra los resultados.

Fuente: [Elaboración Propia]

```
<column>
  <name>Alto</name>
  <field>alto</field>
  <sort-reverse/>
</column>
<column>
  <name>Medio</name>
  <field>medio</field>
  <sort-reverse/>
</column>
<column>
  <name>Bajo</name>
  <field>bajo</field>
  <sort-reverse/>
</column>
```

Figura: 3.28. en la siguiente figura se muestra los resultados.

Fuente: [Elaboración propia]

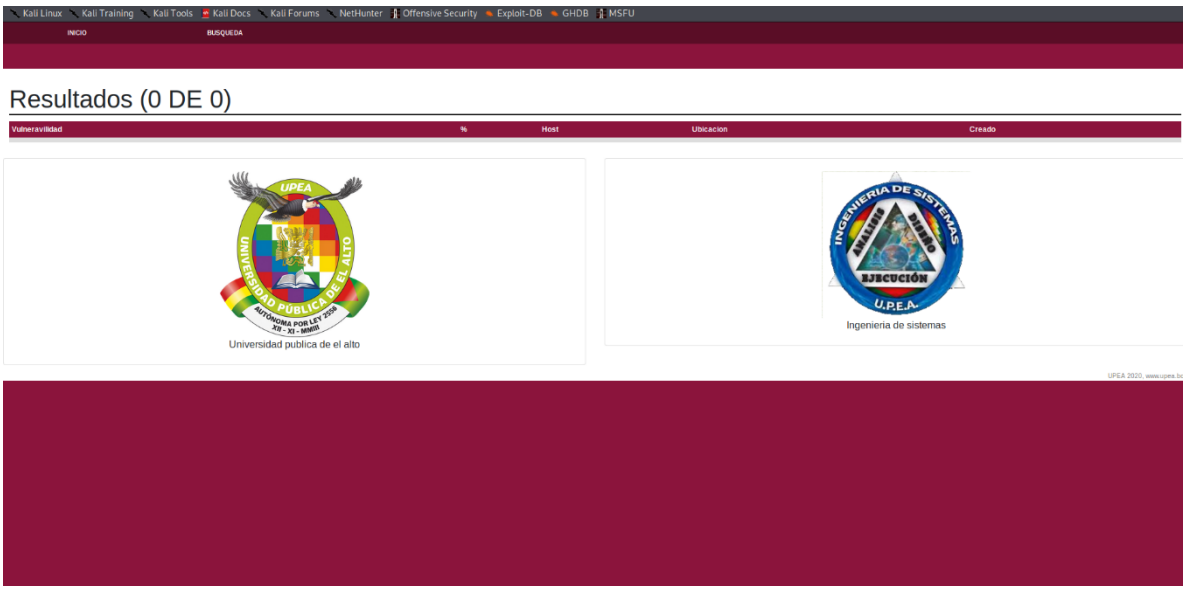


Figura: 3.29. en esta figura visualiza los resultados.

Fuente: [Elaboración Propia]

```
<column>
  <name><xsl:value-of select="gsa:i18n('%')"/></name>
  <field>%</field>
  <sort-reverse/>
</column>
<column>
  <name><xsl:value-of select="gsa:i18n('Host')"/></name>
  <field>host</field>
  <sort-reverse/>
</column>
<column>
  <name><xsl:value-of select="gsa:i18n('Ubicacion', 'Result')"/></name>
  <field>Ubicacion</field>
</column>
<column>
```

Figura: 3.30. en esta figura visualiza los resultados.

Fuente: [Elaboración Propia]

CAPITULO IV

METRICAS DE CALIDAD Y COSTOS

4.1. INTRODUCCION

Basado en el modelo 9126 se pretende aplicar la métrica de calidad ISO/25000 SQuaRE que consta de 8 características.

4.2. ISO/25000 SQuaRE.

4.2.1. Funcionalidad

La funcionalidad del sistema se mide a través de la complejidad, que permite un resultado medible y cuantificable con la siguiente formula.

PF = Cuenta Total * $[0{,}65 + 0.01 * \sum(Fi)]$

Para la medición de funcionabilidad, se tomará en cuenta las siguientes características:

Tabla: 4.1. *Puntos de función*

Parámetros de medida	**Cuenta**	**Factor de complejidad**	**Total**
Número de entradas de usuario	3	*3	9
Número de salidas de usuario	4	*2	8
Número de peticiones de usuario	8	*3	24
Número de archivos	1	*4	4
Número de interfaces	0	*5	0
Total			45

Fuente: Elaboración propia

Valores de la variable (Fi) se obtiene de los resultados a la tabla 4.3. que se muestra a continuación:

Tabla: 4.2. *Tabla de valores de la variable (Fi)*

Escala	**Complejidad**
0	Sin Influencia
1	Incidental
2	Moderado
3	Medio
4	Significativo
5	Esencial

Fuente: [Elaboración propia]

Tabla: 4.3. *Ajuste de complejidad punto función*

Preguntas	**Ponderación**
¿Se requiere comunicación de datos?	5
¿Existe funciones de procesamiento distribuido?	5
¿Requiere el sistema entrada de datos interactiva?	5
¿Existe complejidad en las entradas, las salidas, los archivos y peticiones?	5
¿Es complejo el procesamiento interno?	5
¿Se ha diseñado el código para ser reutilizable?	4
¿Están incluidos en el diseño la conversión y la instalación?	5

¿Sea diseñado el sistema para soportar múltiples instalación en diferentes organizaciones?	5
¿Se diseñó el prototipo para facilitar los cambios y para ser facialmente usada para el usuario?	5
¿Se actualizan los archivos maestros de forma interactivas?	4
¿se ejecuta en un entorno operativo existente y fuertemente utilizado?	5
¿Requiere el sistema copias de seguridad y de recuperación fiables?	3
Total	56

Fuente: Elaboración propia

Aplicando la fórmula para hallar PF y PF(Max)

$$PF = 45 *(0,65+0,01 * 56)$$

$$PF = 54.45$$

$$PF(Max) = 45 *(0,65+0,01 * 63)$$

$$PF(Max) = 57.6$$

Con los valores encontrados de PF y PF(Max), se tiene el siguiente resultado:

$$Funcionalidad = (54.45/57.6) *1000$$

$$Funcionalidad = 94\%$$

Por tanto, la funcionalidad del sistema se representa por el 94%. Lo que quiere decir que le sistema cumple con los requisitos funcionales de forma satisfactoria.

4.2.2. Usabilidad

Se espera que el sistema sea de fácil entendimiento y aprendizaje. La usabilidad está definida por los usuarios finales.

Para la medición de la usabilidad de tiene el siguiente cuestionario :

Tabla: 4.4. *Tabla de escala de ajustes de usabilidad*

Descripción	**Escala**
Pésimo	1
Malo	2
Regular	3
Bueno	4
Muy Bueno	5

Fuente: [Elaboración propia]

Tabla: 4.5. *Evaluación de usabilidad.*

Factor	**Valor**
¿Se ha satisfecho todos los requerimientos establecidos por el prototipo?	5
¿Es de sencillo manejo para el usuario?	5
¿Presenta suficiente ayuda durante el tiempo que accede al sistema?	4
¿Los informes son suficientemente claros?	4
¿El prototipo tiene la seguridad necesaria?	5
¿Está de acuerdo con el funcionamiento del prototipo?	5

¿El sistema facilitara el trabajo que realizo?	4
Total	32

Fuente: Elaboración propia

La usabilidad se calcula con la siguiente fórmula:

$$\text{Usabilidad} = [(\frac{\sum valor}{n} * 100)]/5$$

$$\text{Usabilidad} = \left[\left(\frac{32}{7} * 100\right)\right]/5$$

$$\text{Usabilidad} = 91\%$$

La usabilidad corresponde a un 91%.

4.2.3. Fiabilidad

Es un conjunto de atributos relacionados con la capacidad del software de mantener su nivel de prestación bajo condiciones establecidas durante un periodo establecido.

Identificación de variables

Tabla: 4.6. *Tabla de identificación de variables*

Tiempo de servicio	**Número de peticiones**	**Fallos encontrados**	**Probabilidad de fallo**
8 Hrs.	4	0	0
16 Hrs.	8	1	0.12
32 Hrs.	16	2	0.12
64 Hrs.	32	3	0.09

Fuente: [Elaboración propia]

Calculo de probabilidad de fallo periodos de tiempo de servicio (PFTS).

PFTS= $\sum(Probabilidaddefallo Periodo de tiempo de servicio)$

PFTS = 0.33/4

PFTS = 0.0825

Aplicamos la fórmula de Fiabilidad:

Fiabilidad = (1 - PFTS) * 100

Fiabilidad = (1 – 0.0825) * 100

Fiabilidad = 91.7%

Esto nos indica que el prototipo es 91% fiable.

4.2.4. Mantenibilidad

La mantenibilidad es la capacidad del sistema a ser modificado a nivel funcional, correcciones de mejoras y cambios en el entorno.

La fórmula para obtener la mantenibilidad es:

$$MS = \frac{Mt-(Fc+Fa+FE)}{Mt}$$

Reemplazando

$$MS = \frac{5-(1+0+0)}{5}$$

$$MS = 80\%$$

Descripción de fórmula:

Mt = número de módulos de la versión actual.

Fc = número de módulos de la versión actual que se cambiaron.

Fa = número de módulos de la versión actual que se añadieron.

FE = número de módulos de la versión actual que se eliminaron en la versión actual.

4.2.5. Portabilidad

La portabilidad es la capacidad que tiene el sistema para ser trasladado de un entorno a otro.

Para obtener la portabilidad, se tiene la siguiente fórmula:

$$\text{Portabilidad} = 1 - \left(\frac{numero\ de\ dia\ para\ portar\ el\ sistema}{numero\ de\ dias\ para\ implementarel\ sistema}\right)$$

Reemplazar la fórmula:

$$\text{Portabilidad} = 1\text{-}\left(\frac{1}{5}\right)$$

$$\text{Portabilidad} = 0.75 * 100\%$$

$$\text{Portabilidad} = 75\%$$

Eso nos indica que el prototipo es 75% portable.

4.2.6. Resultados

Tabla: 4.7. *Tabla de resultado de métricas de calidad*

Características	Resultados %
Funcionalidad	94%
Usabilidad	91%

Fiabilidad	92%
Mantenibilidad	80%
Portabilidad	75%
Total	86%

Fuente: [Elaboración propia]

La calidad del sistema corresponde al 86%, lo que se interpreta como la satisfacción que tiene un usuario al interactuar con el sistema.

4.2.7. Seguridad.

Debido a que el prototipo desarrollado contiene información privada, por esta razón estos son susceptibles a diferentes tipos de amenaza.

Es por este motivo que, dentro del sistema desarrollado, se implementó, seguridad a los datos de las siguientes formas:

4.3. COSTOS

4.3.1. Cócono II.

Es útil para estimar el costo total del sistema se tomarán en cuenta los siguientes costos: Costo de la elaboración del proyecto, costos del software desarrollado, costos de la implementación del sistema.

4.3.2. Punto de Función.

Primero se debe hallar el punto de función para poder obtener el costo del proyecto para ello vamos analizar cada una de las pantallas de nuestro sistema.

4.3.2.1. Número de entradas de usuario

Tabla: 4.8. *En la tabla se muestra las entradas al prototipo*

Nro.	Entradas de Usuario
1	Ingreso de usuario
2	Ingreso de IP

Fuente: [Elaboración propia]

4.3.2.2. Número de salida de usuario

Tabla: 4.9. *En la siguiente tabla proporciona información elaborada por el sistema que son gestionadas al usuario.*

Nro.	Salidas de usuario
1	Confirmación de datos de usuario.
2	Reporte de resultados de la búsqueda.
3	Reporte de la búsqueda

Fuente: [Elaboración propia]

4.3.2.3. Número de peticiones de usuario

Tabla: 4.10. *En esta tabla veremos las peticiones que hace el usuario al prototipo.*

Nro.	Peticiones de Usuario
1	Autenticación al usuario
2	Visualizar el resultado de la búsqueda
3	Visualizar reporte de la búsqueda

Fuente: [Elaboración propia]

4.3.2.4. Número de archivos

Tabla: 4.11. *En esta tabla mostramos las salidas lógicas del prototipo*

Nro.	**Archivos**
1	Información de la búsqueda realizada.
2	Información de las vulnerabilidades.

Fuente: [Elaboración propia]

Una vez contando todos los datos requeridos de nuestra aplicación, lo siguiente es agruparlos para tener el parámetro de medición.

Tabla: 4.12. *Interfaces parámetros de medición.*

Parámetros de medición	Cuentas	Factor de Ponderación			Totales
		Simple	Medio	Complejo	
Nro. De Entradas	2	3	4	6	6
Nro. De Salidas	3	4	5	7	12
Nro. De Peticiones	3	5	4	6	15
Nro. De Archivos	2	7	10	15	20
Totales de Cuentas					53

Fuente: [Elaboración propia]

4.3.2.5. Calculo de factores de ajustes de la complejidad

Tabla: 4.13. *Esta tabla tiene el factor de complejidad*

Factor de complejidad	Valor
Requiere copias de seguridad y recuperación	0

Necesita comunicación de datos	3
Se requiere entrada de datos en línea (on-line)	3
Transacción de salida en múltiples pantallas	2
Código diseñado para la reutilización	4
Conversión instalación en diseño	2
Aplicación diseñada para el cambio	3
Interface con el usuario	4
Actualización (on-line)	0
Procesamiento complejo	3
Facilidad de cambios	2
Volumen de transacciones	0
Total	26

Fuente: [Elaboración propia]

Se calculará el factor de ajuste

$$\text{Factor de Ajuste} = 0.65 + 0.01 * \sum fi()$$

$$\text{Factor de Ajuste} = 0.65 + 0.01 * 26$$

$$\text{Factor de Ajuste} = 0.91$$

Calculando el punto función con los datos obtenidos

$$\text{Punto Función} = \text{Cuenta Total} * \text{Factor de Ajustes}$$

$$\text{Punto Función} = 53 * 0.91$$

$$\text{Punto Función} = 48.23$$

4.3.3. Costo del software Desarrollado

Se utiliza como punto función (PF) PF = 48.23, realizaremos la conversión de punto función a mies de líneas de código mediante la siguiente tabla.

Tabla: 4.14. *Factor LCD/PF de lenguaje de programación*

Lenguaje	Factor LDC/PF
Java	53
JavaScript	47
Visual Basic	46
ASP	36
Visual C++	34
PHP	12
Ensamblador	320
C	150

Fuente: [QSM, 2017]

Aplicaremos las formulas asicas de esfuerzo, tiempo calendario y personal requerido, Las fórmulas de COCOMO II que utilizaremos serán las siguiente:

$$E_D = 2{,}4(KLDC)^{1.05}$$

$$T_D = 2{,}5(E_D)^{0.38}$$

Donde:

E_D: Esfuerzo aplicado en personas por mes.

T_D: tiempo de desarrollo en mes.

KLDC = número estimado de líneas de código distribuidas.

LCD = PF*Factor = LCD

LCD = 48.23*47 = 2265

KLDC = 2.26

Calculando el esfuerzo en personas mes:

$$E_D = 2.4 * (2.26)^{1.05} = 5.64 \text{ [personas/mes]}$$

Calculando el tiempo de desarrollo mes

$$T_D = 2.5 * (5.64)^{0.38} = 4.82 \text{ [meses]}$$

Calculando el personal requerido para el desarrollo del proyecto se obtiene con la siguiente formula:

$$Numero\ de\ programadores = \frac{E_D}{T_D} = \frac{5.64}{4.82} = 1.17$$

Por lo tanto, se necesita 1 programador para el desarrollo del prototipo. El salario de un programador es de 300 $us/mes. Por los tanto, con este dato la estimación del costo del software se calculará con la siguiente formula.

$$Costo\ Software = \#\ de\ programadores * salario\ de\ programador * \#\ de\ mes$$

$$Costo\ Software = 1 * 300 * 4 = 1200$$

Por lo tanto, el costo de desarrollo del software es de 1200 $us.

4.3.4. Costo de la elaboración del proyecto

Los costos de elaboración del proyecto se refieren a los costos de estudio del sistema en la etapa de análisis.

Tabla: 4.15. *Costo de elaboración del proyecto*

Descripción	Costo ($)	Costo (Bs)
Análisis y diseñado del proyecto	200	1400
Material de escritorio	50	350
Desarrollo del software	1200	8400
Otros	100	700
Total	1550 ($)	10850 (Bs)

Fuente: [Elaboración propia]

Por lo tanto, el costo total para la elaboración del proyecto es de 1550 $us y en bolivianos 10850.

CAPITULO V

PUEBAS Y RESULTADOS

5.1. INTRODUCCIÓN

En este capítulo el objetivo central es el de demostrar que la hipótesis planteada en el primer capítulo se cumplió, para esto usaremos herramientas de tipo estadístico.

Al usar el método estadístico se podrán realizar pruebas unitarias al sistema como también pruebas globales de todo su funcionamiento

5.2. PRUEVAS DEL MODELO

Una vez explicados los elementos que componen al sistema, su funcionalidad, su desarrollo y demás características es importante realizar una fase de pruebas las cuales se verán a continuación.

Como se ve en la figura 5.1. ya se tiene el prototipo del sistema, donde la primera vez poner administrador y contraseña que serán proporcionado.

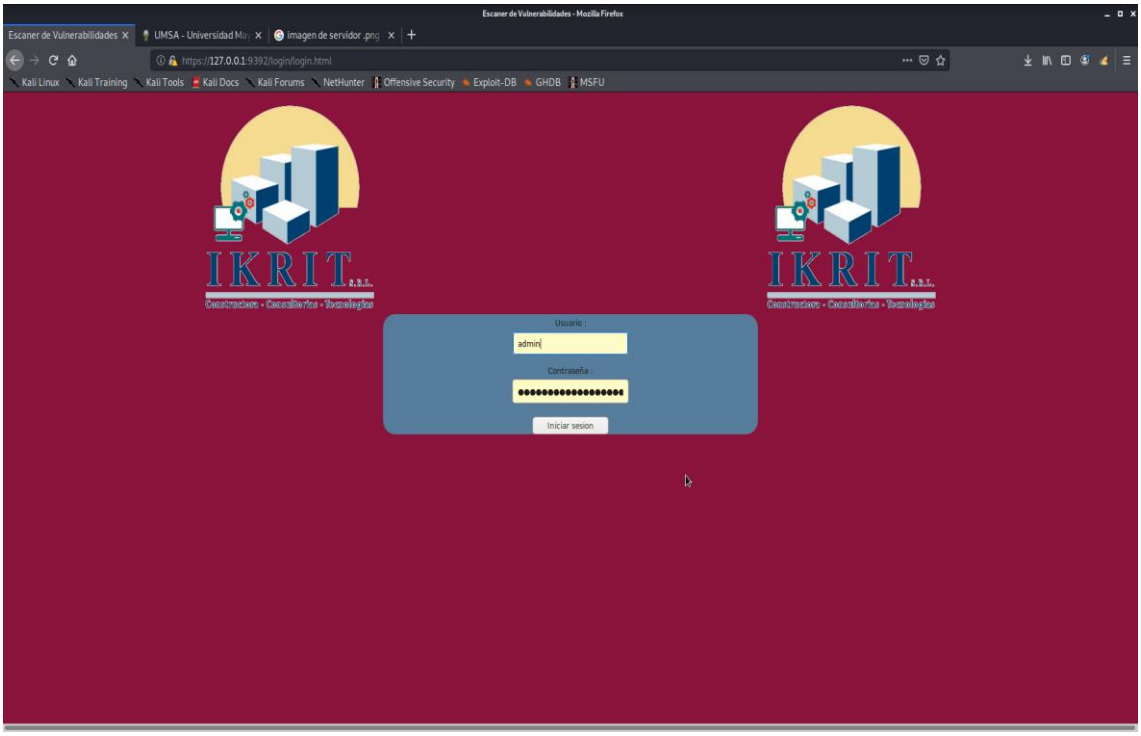


Figura 5.1. Pruebas del prototipo final.

Fuente: [Elaboración propia]

En la figura 5.2. comenzamos con las pruebas necesarias para verificar el prototipo.

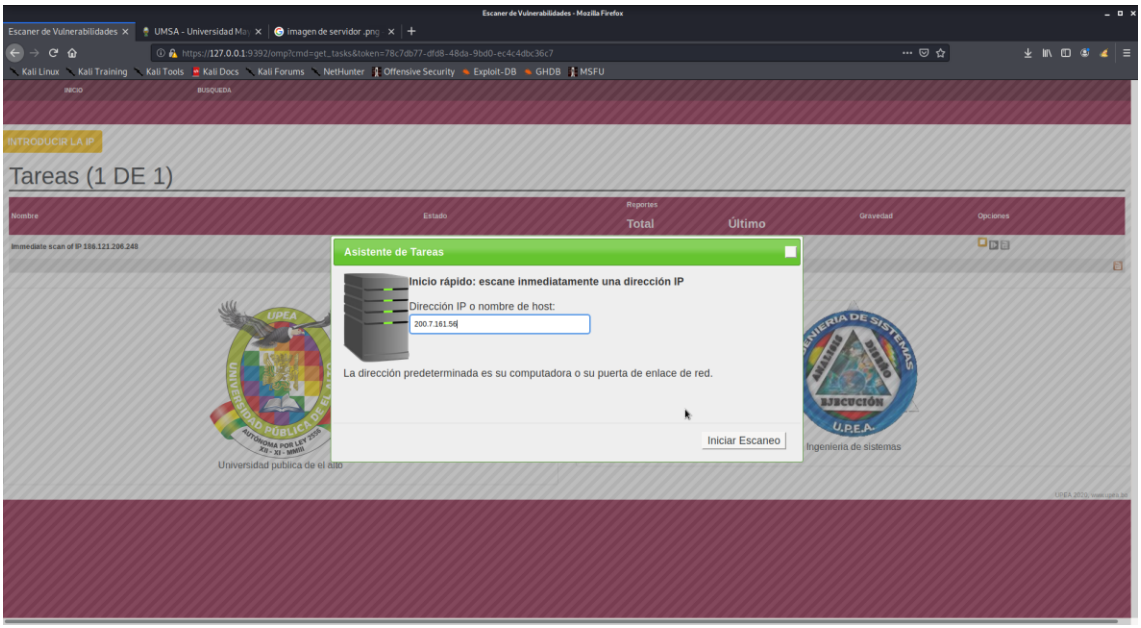


Figura: 5.2. Pruebas de prototipo.

Fuente: [Elaboración propia]

En la figura 5.3. esperamos que termine la búsqueda de vulnerabilidades.

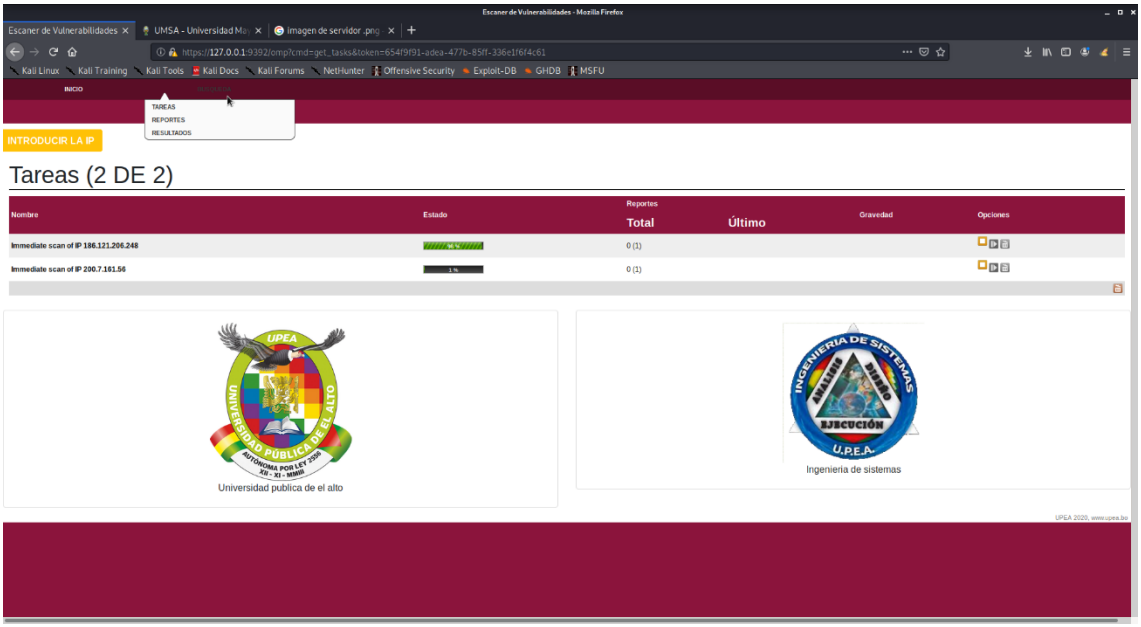


Figura: 5.3. Búsqueda de vulnerabilidades.

Fuente: [Elaboración propia]

Una vez terminado la búsqueda en la figura 5.4. podemos apreciar de como descargar un documento PDF que contiene las vulnerabilidades encontradas.

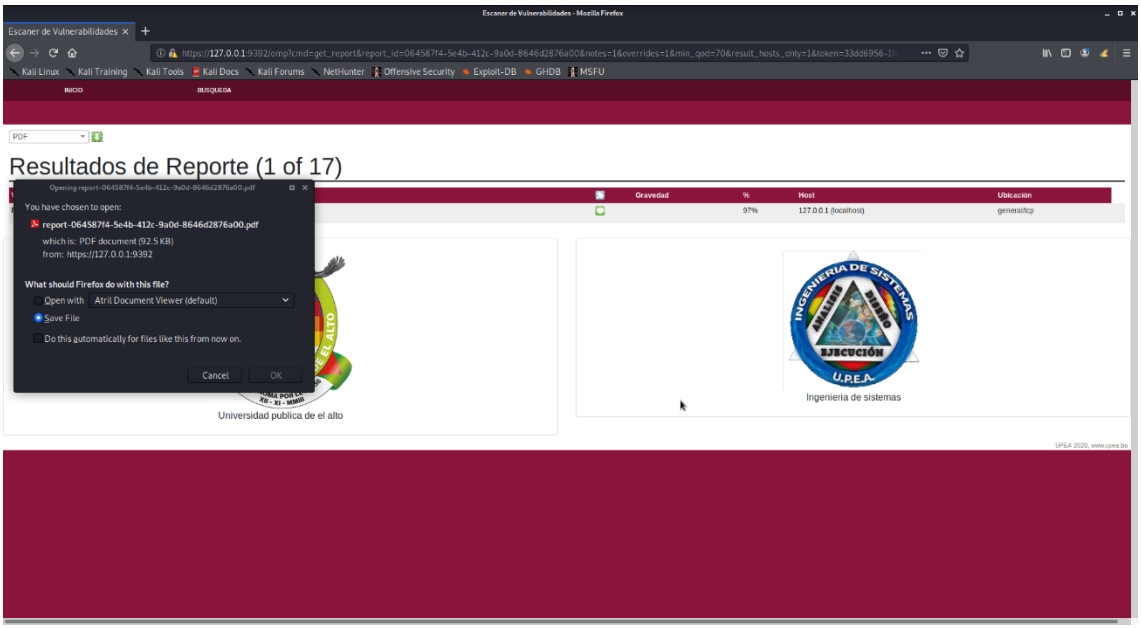


Figura: 5.4. Reporte en PDF.

Fuente: [Elaboración propia]

5.2.1. Documento recopilado de las pruebas.

5.2.1.1. IP 186.121.206.248

Reporte de Busqueda

July 7, 2020

Resumen

Este documento informa sobre los resultados de un análisis de seguridad automático. Todas las fechas se muestran usando la zona horaria “Coordinated Universal Time” , cual se abrevia UTC . La tarea era Immediate scan of IP 186.121.206.248 . El escaneo comenzó a las y terminó a las . los El informe primero resume los resultados encontrados. Luego, para cada host, El informe

describe cada problema encontrado. Por favor considere el consejos dados en cada descripción, para recti car el problema.

Contents

Resumen de resultados

Host	High	Medium	Low	Log	Falso positivo
186.121.206.248 static-186-121-206-248.acelerate.net	1	5	1	0	0
Total: 1	1	5	1	0	0

Las actualizaciones de seguridad del proveedor no son de con anza.
Las anulaciones están activadas. Cuando un resultado tiene una anulación, este informe utiliza la amenaza de la anulación.
La información sobre las anulaciones se incluye en el informe. Las notas se incluyen en el informe.
Es posible que este informe no muestre detalles de todos los problemas encontrados. Solo enumera los hosts que produjeron problemas.
Problemas con el nivel de amenaza sesión No se muestran. Problemas con el nivel de amenaza Depurar No se muestran. Problemas con el nivel de amenaza Falso positivo No se muestran. Solo resultados con una QoD mínima de 70 are shown.

Este informe contiene todos 7 resultados seleccionados por el ltrado descrito anteriormente. Antes de ltrar había 96 resultados.

Resultados por Host

2.1 186.121.206.248

Inicio de escaneo de host Fin
de escaneo del host

Servicio (Port)	Nivel de amenaza

2.1.1 High general/tcp

High (CVSS: 10.0) NVT: Report outdated / end-of-life Scan Engine / Environment (local)
Resumen This script checks and reports an outdated or end-of-life scan engine for the following environments: - Greenbone Source Edition (GSE) - Greenbone Community Edition (GCE) used for this scan.
NOTE: While this is not, in and of itself, a security vulnerability, a severity is reported to make you aware of a possible decreased scan coverage or missing detection of vulnerabilities on the target due to e.g.: - missing functionalities - missing bug xes - incompatibilities within the feed.
Resultado de detección de vulnerabilidad Installed GVM Libraries (gvm-libs) version: 9.0.3 Latest available GVM Libraries (gvm-libs) version: 10.0.2 Reference URL(s) for the latest available version: https://community.greenbone.n ,→et/t/gvm-11-stable-initial-release-2019-10-14/3674 / https://community.greenbo ,→ne.net/t/gvm-10-old-stable-initial-release-2019 04-05/208
Solución Tipo de solución: VendorFix Update to the latest available stable release for your scan environment. Please check the references for more information. If you're using packages provided by your Linux distribution please contact the maintainer of the used distribution / repository and request updated packages. If you want to accept the risk of a possible decreased scan coverage or missing detection of vulnerabilities on the target you can set a global override for this script as described in the linked manuals.
Método de detección de vulnerabilidad Detalles: Report outdated / end-of-life Scan Engine / Environment (local) OID:1.3.6.1.4.1.25623.1.0.108560 Versión utilizada: 2020-06-10T13:24:20+0000

References
Other:
URL:https://www.greenbone.net/en/install_use_gce/
URL:https://community.greenbone.net/t/gvm-9-end-of-life-initial-release-2017-
,→03-07/211
URL:https://community.greenbone.net/t/gvm-10-old-stable-initial-release-2019-
,→04-05/208
URL:https://community.greenbone.net/t/gvm-11-stable-initial-release-2019-10-1
,→4/3674
URL:https://docs.greenbone.net/GSM-Manual/gos-4/en/reports.html#creating-an-o
,→verride
URL:https://docs.greenbone.net/GSM-Manual/gos-5/en/reports.html#creating-an-o
,→verride
URL:https://docs.greenbone.net/GSM-Manual/gos-6/en/reports.html#creating-an-o
,→verride

[return to 186.121.206.248]

2.1.2 Medium 80/tcp

Medium (CVSS: 5.0)
NVT: Missing `httpOnly` Cookie Attribute

Resumen
The application is missing the 'httpOnly' cookie attribute

Resultado de detección de vulnerabilidad
The cookies:
Set-Cookie: ci_session=a%3A5%3A%7Bs%3A10%3A%22session_id%22%3Bs%3A32%3A%22c7c00c
,→897ac8891a9631e9f06c37b839%22%3Bs%3A10%3A%22ip_address%22%3Bs%3A15%3A%22181.18
,→8.160.161%22%3Bs%3A10%3A%22user_agent%22%3Bs%3A43%3A%22Mozilla%2F5.0+%5Ben%5D+
,→%28X11%2C+U%3B+OpenVAS-VT+9.0.3%29%22%3Bs%3A13%3A%22last_activity%22%3Bi%3A159
,→4130550%3Bs%3A9%3A%22user_data%22%3Bs%3A0%3A%22%22%3B%7Dec585c985e4440350df4cc
,→e1e2f9e3e9; expires=Tue, 07-Jul-2020 14:32:30 GMT; Max-Age=***replaced***; pat
,→h=/
Set-Cookie: counte=***replaced***; expires=Tue, 07-Jul-2020 15:04:10 GMT; Max-Ag
,→e=3700
are missing the "httpOnly" attribute.

Solución
Tipo de solución: Mitigation
Set the 'httpOnly' attribute for any session cookie.

Software / SO afectado
Application with session handling in cookies.

Perspectiva de vulnerabilidad
The aw is due to a cookie is not using the 'httpOnly' attribute. This allows a cookie to be accessed by JavaScript which could lead to session hijacking attacks.

Método de detección de vulnerabilidad
Check all cookies sent by the application for a missing 'httpOnly' attribute
Detalles: Missing `httpOnly` Cookie Attribute
OID:1.3.6.1.4.1.25623.1.0.105925
Versión utilizada: 2020-05-05T09:44:01+0000

References
Other:
URL:https://www.owasp.org/index.php/HttpOnly
URL:https://www.owasp.org/index.php/Testing_for_cookies_attributes_(OTG-SESS-
,→002)

Medium (CVSS: 4.8)
NVT: Cleartext Transmission of Sensitive Information via HTTP

Resumen
The host / application transmits sensitive information (username, passwords) in cleartext via HTTP.

Resultado de detección de vulnerabilidad
The following input fields where identified (URL:input name):
http://static-186-121-206-248.acelerate.net/admin:password

Impacto
An attacker could use this situation to compromise or eavesdrop on the HTTP communication between the client and the server using a man-in-the-middle attack to get access to sensitive data like usernames or passwords.

Solución
Tipo de solución: Workaround
Enforce the transmission of sensitive data via an encrypted SSL/TLS connection. Additionally make sure the host / application is redirecting all users to the secured SSL/TLS connection before allowing to input sensitive data into the mentioned functions.

Software / SO afectado
Hosts / applications which doesn't enforce the transmission of sensitive data via an encrypted SSL/TLS connection.

Método de detección de vulnerabilidad
Evaluate previous collected information and check if the host / application is not enforcing the transmission of sensitive data via an encrypted SSL/TLS connection.
The script is currently checking the following:
- HTTP Basic Authentication (Basic Auth)
- HTTP Forms (e.g. Login) with input eld of type 'password'
Detalles: Cleartext Transmission of Sensitive Information via HTTP
OID:1.3.6.1.4.1.25623.1.0.108440
Versión utilizada: 2020-05-08T08:34:44+0000

References
Other:
URL:https://www.owasp.org/index.php/Top_10_2013-A2-Broken_Authentication_and_S
,→ession_Management
URL:https://www.owasp.org/index.php/Top_10_2013-A6-Sensitive_Data_Exposure
URL:https://cwe.mitre.org/data/definitions/319.html

Medium (CVSS: 4.3)
NVT: jQuery < 1.9.0 XSS Vulnerability

Resultado de detección del producto
cpe:/a:jquery:jquery:1.8.3
Detected by jQuery Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.141622)

Resumen
jQuery before 1.9.0 is vulnerable to Cross-site Scripting (XSS) attacks. The jQuery(strInput) function does not di erentiate selectors from HTML in a reliable fashion. In vulnerable versions, jQuery determined whether the input was HTML by looking for the '<' character anywhere in the string, giving attackers more exibility when attempting to construct a malicious payload. In xed versions, jQuery only deems the input to be HTML if it explicitly starts with the '<' character, limiting exploitability only to attackers who can control the beginning of a string, which is far less common.

Resultado de detección de vulnerabilidad
Installed version: 1.8.3
Fixed version: 1.9.0
Installation
path / port: /https://www.upea.bo/assets/tabtheme/js

Solución
Tipo de solución: VendorFix
Update to version 1.9.0 or later.

Software / SO afectado
jQuery prior to version 1.9.0.

Método de detección de vulnerabilidad
Checks if a vulnerable version is present on the target host.
Detalles: jQuery < 1.9.0 XSS Vulnerability
OID:1.3.6.1.4.1.25623.1.0.141636
Versión utilizada: 2019-08-27T12:52:16+0000

Resultado de detección del producto
Producto: cpe:/a:jquery:jquery:1.8.3
Metodo: jQuery Detection (HTTP)
OID: 1.3.6.1.4.1.25623.1.0.141622)

References
CVE: CVE-2012-6708
Other:
URL:https://bugs.jquery.com/ticket/11290

[return to 186.121.206.248]

2.1.3 Medium 443/tcp

Medium (CVSS: 6.4)
NVT: SSL/TLS: Missing `secure` Cookie Attribute

Resumen
The host is running a server with SSL/TLS and is prone to information disclosure vulnerability.

Resultado de detección de vulnerabilidad
The cookies:
Set-Cookie: ci_session=dgiii79sqghn8t9g2eh4hdv0i5ut3jdh; expires=Tue, 07-Jul-202
,→0 16:04:34 GMT; Max-Age=***replaced***; path=/; HttpOnly
are missing the "secure" attribute.

Solución
Tipo de solución: Mitigation
Set the 'secure' attribute for any cookies that are sent over a SSL/TLS connection.

Software / SO afectado
Server with SSL/TLS.

Perspectiva de vulnerabilidad
The aw is due to cookie is not using 'secure' attribute, which allows cookie to be passed to the server by the client over non-secure channels (http) and allows attacker to conduct session hijacking attacks.

Método de detección de vulnerabilidad
Detalles: SSL/TLS: Missing `secure` Cookie Attribute
OID:1.3.6.1.4.1.25623.1.0.902661
Versión utilizada: 2020-05-11T11:32:41+0000

References
Other:
URL:https://www.owasp.org/index.php/SecureFlag
URL:http://www.ietf.org/rfc/rfc2965.txt
URL:https://www.owasp.org/index.php/Testing_for_cookies_attributes_(OWASP-SM-
,→002)

[return to 186.121.206.248]

2.1.4 Medium 21/tcp

Medium (CVSS: 4.8) NVT: FTP Unencrypted Cleartext Login
Resumen The remote host is running a FTP service that allows cleartext logins over unencrypted connections.
Resultado de detección de vulnerabilidad The remote FTP service accepts logins without a previous sent 'AUTH TLS' command ,→. Response(s): Non-anonymous sessions: 331 Please specify the password. Anonymous sessions: 331 Please specify the password.
Impacto An attacker can uncover login names and passwords by sni ng tra c to the FTP service.
Solución Tipo de solución: Mitigation Enable FTPS or enforce the connection via the 'AUTH TLS' command. Please see the manual of the FTP service for more information.
Método de detección de vulnerabilidad Tries to login to a non FTPS enabled FTP service without sending a 'AUTH TLS' command rst and checks if the service is accepting the login without enforcing the use of the 'AUTH TLS' command. Detalles: FTP Unencrypted Cleartext Login OID:1.3.6.1.4.1.25623.1.0.108528 Versión utilizada: 2020-03-24T12:27:11+0000

[return to 186.121.206.248]

2.1.5 Low general/tcp

Low (CVSS: 2.6) NVT: TCP timestamps
Resumen The remote host implements TCP timestamps and therefore allows to compute the uptime.
Resultado de detección de vulnerabilidad It was detected that the host implements RFC1323. The following timestamps were retrieved with a delay of 1 seconds in-between: Packet 1: 1136658470 Packet 2: 1136659039
Impacto A side e ect of this feature is that the uptime of the remote host can sometimes be computed.

Solución Tipo de solución: Mitigation To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime.
To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled' Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled. The default behavior of the TCP/IP stack on this Systems is to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment. See the references for more information.
Software / SO afectado TCP/IPv4 implementations that implement RFC1323.
Perspectiva de vulnerabilidad The remote host implements TCP timestamps, as de ned by RFC1323.
Método de detección de vulnerabilidad Special IP packets are forged and sent with a little delay in between to the target IP. The responses are searched for a timestamps. If found, the timestamps are reported. Detalles: TCP timestamps OID:1.3.6.1.4.1.25623.1.0.80091 Versión utilizada: 2020-03-21T13:23:23+0000
References Other: URL:http://www.ietf.org/rfc/rfc1323.txt URL:http://www.microsoft.com/en-us/download/details.aspx?id=9152

[return to 186.121.206.248]

Muchas gracias

5.2.1.2. IP 170.0.0.1

Reporte de Busqueda

July 9, 2020

Resumen

Este documento informa sobre los resultados de un análisis de seguridad automático. Todas las fechas se muestran usando la zona horaria Coordinated Universal Time , which is abbreviated

UTC . La tarea era Immediate scan of IP 127.0.0.1 . El escaneo comenzó a las y terminó a las . los El informe primero resume los resultados encontrados. Luego, para cada host, El informe describe cada problema encontrado. Por favor considere el consejos dados en cada descripción, para recti car el problema.

Contents

Resumen de resultados

Host	High	Medium	Low	Log	Falso positivo
127.0.0.1 localhost	1	0	0	0	0
Total: 1	1	0	0	0	0

Las actualizaciones de seguridad del proveedor no son de con anza.
Las anulaciones están activadas. Cuando un resultado tiene una anulación, este informe utiliza la amenaza de la anulación.
La información sobre las anulaciones se incluye en el informe. Las notas se incluyen en el informe.
Es posible que este informe no muestre detalles de todos los problemas encontrados. Solo enumera los hosts que produjeron problemas.
Problemas con el nivel de amenaza sesión No se muestran. Problemas con el nivel de amenaza Depurar No se muestran. Problemas con el nivel de amenaza Falso positivo No se muestran. Solo resultados con una QoD mínima de 70 are shown.

Este informe contiene resultado 1 del 1 resultados seleccionados por el ltrado arriba. Antes de ltrar había 17 resultados.

Resultados por Host

2.1 127.0.0.1

Inicio de escaneo de host Fin de escaneo del host

Servicio (Port)	Nivel de amenaza

2.1.1 High general/tcp

High (CVSS: 10.0)
NVT: Report outdated / end-of-life Scan Engine / Environment (local)

Resumen

This script checks and reports an outdated or end-of-life scan engine for the following environ- ments:
- Greenbone Source Edition (GSE)
- Greenbone Community Edition (GCE)
used for this scan.

NOTE: While this is not, in and of itself, a security vulnerability, a severity is reported to make you aware of a possible decreased scan coverage or missing detection of vulnerabilities on the target due to e.g.:
- missing functionalities
- missing bug xes
- incompatibilities within the feed.

Resultado de detección de vulnerabilidad

```
Installed GVM Libraries (gvm-libs) version:          9.0.3
Latest available GVM Libraries (gvm-libs) version: 10.0.2
Reference URL(s) for the latest available version:  https://community.greenbone.n
,→et/t/gvm-11-stable-initial-release-2019-10-14/3674 / https://community.greenbo
,→ne.net/t/gvm-10-old-stable-initial-release-2019 04-05/208
```

Solución

Tipo de solución: VendorFix
Update to the latest available stable release for your scan environment. Please check the refer- ences for more information. If you're using packages provided by your Linux distribution please contact the maintainer of the used distribution / repository and request updated packages.
If you want to accept the risk of a possible decreased scan coverage or missing detection of vulnerabilities on the target you can set a global override for this script as described in the linked manuals.

Método de detección de vulnerabilidad

Detalles: Report outdated / end-of-life Scan Engine / Environment (local)
OID:1.3.6.1.4.1.25623.1.0.108560
Versión utilizada: 2020-06-10T13:24:20+0000

References

```
Other:
  URL:https://www.greenbone.net/en/install_use_gce/
   URL:https://community.greenbone.net/t/gvm-9-end-of-life-initial-release-2017-
,→03-07/211
   URL:https://community.greenbone.net/t/gvm-10-old-stable-initial-release-2019-
,→04-05/208
   URL:https://community.greenbone.net/t/gvm-11-stable-initial-release-2019-10-1
,→4/3674
   URL:https://docs.greenbone.net/GSM-Manual/gos-4/en/reports.html#creating-an-o
,→verride
   URL:https://docs.greenbone.net/GSM-Manual/gos-5/en/reports.html#creating-an-o
,→verride
   URL:https://docs.greenbone.net/GSM-Manual/gos-6/en/reports.html#creating-an-o
,→verride
```

[return to 127.0.0.1]

Muchas gracias

5.2.1.3. IP 186.121.206.248

Reporte de Busqueda

July 7, 2020

Resumen

Este documento informa sobre los resultados de un análisis de seguridad automático. Todas las fechas se muestran usando la zona horaria Coordinated Universal Time , which is abbreviated UTC . La tarea era Immediate scan of IP 186.121.206.248 . El escaneo comenzó a las y terminó a las . los El informe primero resume los resultados encontrados. Luego, para cada host, El informe describe cada problema encontrado. Por favor considere el consejos dados en cada descripción, para recti car el problema.

Contents

Resumen de resultados

Host	High	Medium	Low	Log	Falso positivo
186.121.206.248 static-186-121-206-248.acelerate.net	1	5	1	0	0
Total: 1	1	5	1	0	0

Las actualizaciones de seguridad del proveedor no son de con anza.
Las anulaciones están activadas. Cuando un resultado tiene una anulación, este informe utiliza la amenaza de la anulación.
La información sobre las anulaciones se incluye en el informe. Las notas se incluyen en el informe.
Es posible que este informe no muestre detalles de todos los problemas encontrados. Solo enumera los hosts que produjeron problemas.
Problemas con el nivel de amenaza sesión No se muestran. Problemas con el nivel de amenaza Depurar No se muestran. Problemas con el nivel de amenaza Falso positivo No se muestran. Solo resultados con una QoD mínima de 70 are shown.

Este informe contiene todos 7 resultados seleccionados por el ltrado descrito anteriormente. Antes de ltrar había 96 resultados.

Resultados por Host

2.1 186.121.206.248

Inicio de escaneo de host Fin de escaneo del host

Servicio (Port)	Nivel de amenaza

2.1.1 High general/tcp

High (CVSS: 10.0) NVT: Report outdated / end-of-life Scan Engine / Environment (local)
Resumen This script checks and reports an outdated or end-of-life scan engine for the following environments: - Greenbone Source Edition (GSE) - Greenbone Community Edition (GCE) used for this scan.
NOTE: While this is not, in and of itself, a security vulnerability, a severity is reported to make you aware of a possible decreased scan coverage or missing detection of vulnerabilities on the target due to e.g.: - missing functionalities - missing bug xes - incompatibilities within the feed.
Resultado de detección de vulnerabilidad Installed GVM Libraries (gvm-libs) version: 9.0.3 Latest available GVM Libraries (gvm-libs) version: 10.0.2 Reference URL(s) for the latest available version: https://community.greenbone.n ,→et/t/gvm-11-stable-initial-release-2019-10-14/3674 / https://community.greenbo ,→ne.net/t/gvm-10-old-stable-initial-release-2019 04-05/208

Solución
Tipo de solución: VendorFix
Update to the latest available stable release for your scan environment. Please check the references for more information. If you're using packages provided by your Linux distribution please contact the maintainer of the used distribution / repository and request updated packages.
If you want to accept the risk of a possible decreased scan coverage or missing detection of vulnerabilities on the target you can set a global override for this script as described in the linked manuals.

Método de detección de vulnerabilidad
Detalles: Report outdated / end-of-life Scan Engine / Environment (local)
OID:1.3.6.1.4.1.25623.1.0.108560
Versión utilizada: 2020-06-10T13:24:20+0000

References
Other:
URL:https://www.greenbone.net/en/install_use_gce/
URL:https://community.greenbone.net/t/gvm-9-end-of-life-initial-release-2017-
,→03-07/211
URL:https://community.greenbone.net/t/gvm-10-old-stable-initial-release-2019-
,→04-05/208
URL:https://community.greenbone.net/t/gvm-11-stable-initial-release-2019-10-1
,→4/3674
URL:https://docs.greenbone.net/GSM-Manual/gos-4/en/reports.html#creating-an-o
,→verride
URL:https://docs.greenbone.net/GSM-Manual/gos-5/en/reports.html#creating-an-o
,→verride
URL:https://docs.greenbone.net/GSM-Manual/gos-6/en/reports.html#creating-an-o
,→verride

[return to 186.121.206.248]

2.1.2 Medium 80/tcp

Medium (CVSS: 5.0)
NVT: Missing `httpOnly` Cookie Attribute

Resumen
The application is missing the 'httpOnly' cookie attribute

Resultado de detección de vulnerabilidad

```
The cookies:
Set-Cookie: ci_session=a%3A5%3A%7Bs%3A10%3A%22session_id%22%3Bs%3A32%3A%22aca105
,→804275dfcdba42b6c8e7e3c717%22%3Bs%3A10%3A%22ip_address%22%3Bs%3A15%3A%22181.18
,→8.160.161%22%3Bs%3A10%3A%22user_agent%22%3Bs%3A43%3A%22Mozilla%2F5.0+%5Ben%5D+
,→%28X11%2C+U%3B+OpenVAS-VT+9.0.3%29%22%3Bs%3A13%3A%22last_activity%22%3Bi%3A159
,→4137564%3Bs%3A9%3A%22user_data%22%3Bs%3A0%3A%22%22%3B%7Dfacfe15566ebcad1405bc2
,→37c2af41b4; expires=Tue, 07-Jul-2020 16:29:24 GMT; Max-Age=***replaced***; pat
,→h=/
Set-Cookie: counte=***replaced***; expires=Tue, 07-Jul-2020 17:01:04 GMT; Max-Ag
,→e=3700
are missing the "httpOnly" attribute.
```

Solución

Tipo de solución: Mitigation

Set the 'httpOnly' attribute for any session cookie.

Software / SO afectado

Application with session handling in cookies.

Perspectiva de vulnerabilidad

The aw is due to a cookie is not using the 'httpOnly' attribute. This allows a cookie to be accessed by JavaScript which could lead to session hijacking attacks.

Método de detección de vulnerabilidad

Check all cookies sent by the application for a missing 'httpOnly' attribute

Detalles: `Missing `httpOnly` Cookie Attribute`

OID:1.3.6.1.4.1.25623.1.0.105925

Versión utilizada: 2020-05-05T09:44:01+0000

References

```
Other:
  URL:https://www.owasp.org/index.php/HttpOnly
   URL:https://www.owasp.org/index.php/Testing_for_cookies_attributes_(OTG-SESS-
,→002)
```

Medium (CVSS: 4.8)

NVT: Cleartext Transmission of Sensitive Information via HTTP

Resumen

The host / application transmits sensitive information (username, passwords) in cleartext via HTTP.

Resultado de detección de vulnerabilidad

```
The following input fields where identified (URL:input name):
http://static-186-121-206-248.acelerate.net/admin:password
```

Impacto

An attacker could use this situation to compromise or eavesdrop on the HTTP communication between the client and the server using a man-in-the-middle attack to get access to sensitive data like usernames or passwords.

Solución
Tipo de solución: Workaround
Enforce the transmission of sensitive data via an encrypted SSL/TLS connection. Additionally make sure the host / application is redirecting all users to the secured SSL/TLS connection before allowing to input sensitive data into the mentioned functions.

Software / SO afectado
Hosts / applications which doesn't enforce the transmission of sensitive data via an encrypted SSL/TLS connection.

Método de detección de vulnerabilidad
Evaluate previous collected information and check if the host / application is not enforcing the transmission of sensitive data via an encrypted SSL/TLS connection.
The script is currently checking the following:
- HTTP Basic Authentication (Basic Auth)
- HTTP Forms (e.g. Login) with input eld of type 'password'
Detalles: Cleartext Transmission of Sensitive Information via HTTP
OID:1.3.6.1.4.1.25623.1.0.108440
Versión utilizada: 2020-05-08T08:34:44+0000

References
Other:
URL:https://www.owasp.org/index.php/Top_10_2013-A2-Broken_Authentication_and_S
,→ession_Management
URL:https://www.owasp.org/index.php/Top_10_2013-A6-Sensitive_Data_Exposure
URL:https://cwe.mitre.org/data/definitions/319.html

Medium (CVSS: 4.3)
NVT: jQuery < 1.9.0 XSS Vulnerability

Resultado de detección del producto
cpe:/a:jquery:jquery:1.8.3
Detected by jQuery Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.141622)

Resumen
jQuery before 1.9.0 is vulnerable to Cross-site Scripting (XSS) attacks. The jQuery(strInput) function does not di erentiate selectors from HTML in a reliable fashion. In vulnerable versions, jQuery determined whether the input was HTML by looking for the '<' character anywhere in the string, giving attackers more exibility when attempting to construct a malicious payload. In xed versions, jQuery only deems the input to be HTML if it explicitly starts with the '<' character, limiting exploitability only to attackers who can control the beginning of a string, which is far less common.

Resultado de detección de vulnerabilidad
Installed version: 1.8.3
Fixed version: 1.9.0
Installation
path / port: /https://www.upea.bo/assets/tabtheme/js

Solución
Tipo de solución: VendorFix
Update to version 1.9.0 or later.

Software / SO afectado
jQuery prior to version 1.9.0.

Método de detección de vulnerabilidad
Checks if a vulnerable version is present on the target host.
Detalles: jQuery < 1.9.0 XSS Vulnerability
OID:1.3.6.1.4.1.25623.1.0.141636
Versión utilizada: 2019-08-27T12:52:16+0000

Resultado de detección del producto
Producto: cpe:/a:jquery:jquery:1.8.3
Metodo: jQuery Detection (HTTP)
OID: 1.3.6.1.4.1.25623.1.0.141622)

References
CVE: CVE-2012-6708
Other:
URL:https://bugs.jquery.com/ticket/11290

[return to 186.121.206.248]

2.1.3 Medium 443/tcp

Medium (CVSS: 6.4)
NVT: SSL/TLS: Missing `secure` Cookie Attribute

Resumen
The host is running a server with SSL/TLS and is prone to information disclosure vulnerability.

Resultado de detección de vulnerabilidad
The cookies:
Set-Cookie: ci_session=tbk8qi0f1r8v8690sk0hr26pg7o3lmj4; expires=Tue, 07-Jul-202
,→0 18:01:34 GMT; Max-Age=***replaced***; path=/; HttpOnly
are missing the "secure" attribute.

Solución
Tipo de solución: Mitigation
Set the 'secure' attribute for any cookies that are sent over a SSL/TLS connection.

Software / SO afectado
Server with SSL/TLS.

Perspectiva de vulnerabilidad
The aw is due to cookie is not using 'secure' attribute, which allows cookie to be passed to the server by the client over non-secure channels (http) and allows attacker to conduct session hijacking attacks.

Método de detección de vulnerabilidad
Detalles: SSL/TLS: Missing `secure` Cookie Attribute
OID:1.3.6.1.4.1.25623.1.0.902661
Versión utilizada: 2020-05-11T11:32:41+0000

References
Other:
URL:https://www.owasp.org/index.php/SecureFlag
URL:http://www.ietf.org/rfc/rfc2965.txt
URL:https://www.owasp.org/index.php/Testing_for_cookies_attributes_(OWASP-SM-
,→002)

[return to 186.121.206.248]

2.1.4 Medium 21/tcp

Medium (CVSS: 4.8)
NVT: FTP Unencrypted Cleartext Login

Resumen
The remote host is running a FTP service that allows cleartext logins over unencrypted connections.

Resultado de detección de vulnerabilidad
The remote FTP service accepts logins without a previous sent 'AUTH TLS' command
,→. Response(s):
Non-anonymous sessions: 331 Please specify the password.
Anonymous sessions: 331 Please specify the password.

Impacto
An attacker can uncover login names and passwords by sni ng tra c to the FTP service.

Solución
Tipo de solución: Mitigation
Enable FTPS or enforce the connection via the 'AUTH TLS' command. Please see the manual of the FTP service for more information.

Método de detección de vulnerabilidad
Tries to login to a non FTPS enabled FTP service without sending a 'AUTH TLS' command rst and checks if the service is accepting the login without enforcing the use of the 'AUTH TLS' command.
Detalles: FTP Unencrypted Cleartext Login
OID:1.3.6.1.4.1.25623.1.0.108528
Versión utilizada: 2020-03-24T12:27:11+0000

[return to 186.121.206.248]

2.1.5 Low general/tcp

Low (CVSS: 2.6) NVT: TCP timestamps
Resumen The remote host implements TCP timestamps and therefore allows to compute the uptime.
Resultado de detección de vulnerabilidad It was detected that the host implements RFC1323. The following timestamps were retrieved with a delay of 1 seconds in-between: Packet 1: 1138384904 Packet 2: 1138385181
Impacto A side e ect of this feature is that the uptime of the remote host can sometimes be computed.
Solución Tipo de solución: Mitigation To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime.
To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled' Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled. The default behavior of the TCP/IP stack on this Systems is to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment. See the references for more information.
Software / SO afectado TCP/IPv4 implementations that implement RFC1323.
Perspectiva de vulnerabilidad The remote host implements TCP timestamps, as de ned by RFC1323.
Método de detección de vulnerabilidad Special IP packets are forged and sent with a little delay in between to the target IP. The responses are searched for a timestamps. If found, the timestamps are reported. Detalles: TCP timestamps OID:1.3.6.1.4.1.25623.1.0.80091 Versión utilizada: 2020-03-21T13:23:23+0000
References Other: URL:http://www.ietf.org/rfc/rfc1323.txt URL:http://www.microsoft.com/en-us/download/details.aspx?id=9152

[return to 186.121.206.248]

5.2.1.4. IP 186.121.206.248

Reporte de Busqueda

July 7, 2020

Resumen

Este documento informa sobre los resultados de un análisis de seguridad automático. Todas las fechas se muestran usando la zona horaria Coordinated Universal Time , which is abbreviated UTC . La tarea era Immediate scan of IP 186.121.206.248 . El escaneo comenzó a las y terminó a las . los El informe primero resume los resultados encontrados. Luego, para cada host, El informe describe cada problema encontrado. Por favor considere el consejos dados en cada descripción, para recti car el problema.

Contents

Resumen de resultados

Host	High	Medium	Low	Log	Falso positivo
186.121.206.248 static-186-121-206-248.acelerate.net	1	5	1	0	0
Total: 1	1	5	1	0	0

Las actualizaciones de seguridad del proveedor no son de con anza.
Las anulaciones están activadas. Cuando un resultado tiene una anulación, este informe utiliza la amenaza de la anulación.
La información sobre las anulaciones se incluye en el informe. Las
notas se incluyen en el informe.

Es posible que este informe no muestre detalles de todos los problemas encontrados. Solo enumera los hosts que produjeron problemas.
Problemas con el nivel de amenaza sesión No se muestran. Problemas con el nivel de amenaza Depurar No se muestran. Problemas con el nivel de amenaza Falso positivo No se muestran. Solo resultados con una QoD mínima de 70 are shown.

Este informe contiene todos 7 resultados seleccionados por el ltrado descrito anteriormente. Antes de ltrar había 90 resultados.

Resultados por Host

2.1 186.121.206.248

Inicio de escaneo de host Fin de escaneo del host

Servicio (Port)	Nivel de amenaza

2.1.1 High general/tcp

High (CVSS: 10.0)
NVT: Report outdated / end-of-life Scan Engine / Environment (local)

Resumen
This script checks and reports an outdated or end-of-life scan engine for the following environments:
- Greenbone Source Edition (GSE)
- Greenbone Community Edition (GCE)
used for this scan.

NOTE: While this is not, in and of itself, a security vulnerability, a severity is reported to make you aware of a possible decreased scan coverage or missing detection of vulnerabilities on the target due to e.g.:
- missing functionalities
- missing bug xes
- incompatibilities within the feed.

Resultado de detección de vulnerabilidad

```
Installed GVM Libraries (gvm-libs) version:         9.0.3
Latest available GVM Libraries (gvm-libs) version: 10.0.2
Reference URL(s) for the latest available version:  https://community.greenbone.n
,→et/t/gvm-11-stable-initial-release-2019-10-14/3674 / https://community.greenbo
,→ne.net/t/gvm-10-old-stable-initial-release-2019 04-05/208
```

Solución
Tipo de solución: VendorFix
Update to the latest available stable release for your scan environment. Please check the references for more information. If you're using packages provided by your Linux distribution please contact the maintainer of the used distribution / repository and request updated packages.
If you want to accept the risk of a possible decreased scan coverage or missing detection of vulnerabilities on the target you can set a global override for this script as described in the linked manuals.

Método de detección de vulnerabilidad
Detalles: Report outdated / end-of-life Scan Engine / Environment (local)
OID:1.3.6.1.4.1.25623.1.0.108560
Versión utilizada: 2020-06-10T13:24:20+0000

References
Other:
URL:https://www.greenbone.net/en/install_use_gce/
URL:https://community.greenbone.net/t/gvm-9-end-of-life-initial-release-2017-
,→03-07/211
URL:https://community.greenbone.net/t/gvm-10-old-stable-initial-release-2019-
,→04-05/208
URL:https://community.greenbone.net/t/gvm-11-stable-initial-release-2019-10-1
,→4/3674
URL:https://docs.greenbone.net/GSM-Manual/gos-4/en/reports.html#creating-an-o
,→verride
URL:https://docs.greenbone.net/GSM-Manual/gos-5/en/reports.html#creating-an-o
,→verride
URL:https://docs.greenbone.net/GSM-Manual/gos-6/en/reports.html#creating-an-o
,→verride

[return to 186.121.206.248]

2.1.2 Medium 21/tcp

Medium (CVSS: 4.8)
NVT: FTP Unencrypted Cleartext Login

Resumen
The remote host is running a FTP service that allows cleartext logins over unencrypted connections.

Resultado de detección de vulnerabilidad
The remote FTP service accepts logins without a previous sent 'AUTH TLS' command
,→. Response(s):
Non-anonymous sessions: 331 Please specify the password.
Anonymous sessions: 331 Please specify the password.

Impacto
An attacker can uncover login names and passwords by sni ng tra c to the FTP service.

Solución
Tipo de solución: Mitigation
Enable FTPS or enforce the connection via the 'AUTH TLS' command. Please see the manual of the FTP service for more information.

Método de detección de vulnerabilidad
Tries to login to a non FTPS enabled FTP service without sending a 'AUTH TLS' command rst and checks if the service is accepting the login without enforcing the use of the 'AUTH TLS' command.
Detalles: FTP Unencrypted Cleartext Login
OID:1.3.6.1.4.1.25623.1.0.108528
Versión utilizada: 2020-03-24T12:27:11+0000

[return to 186.121.206.248]

2.1.3 Medium 80/tcp

Medium (CVSS: 5.0)
NVT: Missing `httpOnly` Cookie Attribute

Resumen
The application is missing the 'httpOnly' cookie attribute

Resultado de detección de vulnerabilidad
```
The cookies:
Set-Cookie: ci_session=a%3A5%3A%7Bs%3A10%3A%22session_id%22%3Bs%3A32%3A%22efd909
,→21bbb5e32535df732621ae43b5%22%3Bs%3A10%3A%22ip_address%22%3Bs%3A15%3A%22181.18
,→8.160.161%22%3Bs%3A10%3A%22user_agent%22%3Bs%3A43%3A%22Mozilla%2F5.0+%5Ben%5D+
,→%28X11%2C+U%3B+OpenVAS-VT+9.0.3%29%22%3Bs%3A13%3A%22last_activity%22%3Bi%3A159
,→4158557%3Bs%3A9%3A%22user_data%22%3Bs%3A0%3A%22%22%3B%7D92a3cc8f94e5acc76c3bae
,→31b187723a; expires=Tue, 07-Jul-2020 22:19:17 GMT; Max-Age=***replaced***; pat
,→h=/
Set-Cookie: counte=***replaced***; expires=Tue, 07-Jul-2020 22:50:57 GMT; Max-Ag
,→e=3700
are missing the "httpOnly" attribute.
```

Solución
Tipo de solución: Mitigation
Set the 'httpOnly' attribute for any session cookie.

Software / SO afectado
Application with session handling in cookies.

Perspectiva de vulnerabilidad
The aw is due to a cookie is not using the 'httpOnly' attribute. This allows a cookie to be accessed by JavaScript which could lead to session hijacking attacks.

Método de detección de vulnerabilidad
Check all cookies sent by the application for a missing 'httpOnly' attribute
Detalles: Missing `httpOnly` Cookie Attribute
OID:1.3.6.1.4.1.25623.1.0.105925
Versión utilizada: 2020-05-05T09:44:01+0000

References
Other:
URL:https://www.owasp.org/index.php/HttpOnly
URL:https://www.owasp.org/index.php/Testing_for_cookies_attributes_(OTG-SESS-
,→002)

Medium (CVSS: 4.8)
NVT: Cleartext Transmission of Sensitive Information via HTTP

Resumen
The host / application transmits sensitive information (username, passwords) in cleartext via HTTP.

Resultado de detección de vulnerabilidad
The following input fields where identified (URL:input name):
http://static-186-121-206-248.acelerate.net/admin:password

Impacto
An attacker could use this situation to compromise or eavesdrop on the HTTP communication between the client and the server using a man-in-the-middle attack to get access to sensitive data like usernames or passwords.

Solución
Tipo de solución: Workaround

Enforce the transmission of sensitive data via an encrypted SSL/TLS connection. Additionally make sure the host / application is redirecting all users to the secured SSL/TLS connection before allowing to input sensitive data into the mentioned functions.

Software / SO afectado
Hosts / applications which doesn't enforce the transmission of sensitive data via an encrypted SSL/TLS connection.

Método de detección de vulnerabilidad
Evaluate previous collected information and check if the host / application is not enforcing the transmission of sensitive data via an encrypted SSL/TLS connection.
The script is currently checking the following:
- HTTP Basic Authentication (Basic Auth)
- HTTP Forms (e.g. Login) with input eld of type 'password'
Detalles: Cleartext Transmission of Sensitive Information via HTTP
OID:1.3.6.1.4.1.25623.1.0.108440
Versión utilizada: 2020-05-08T08:34:44+0000

References
Other:
URL:https://www.owasp.org/index.php/Top_10_2013-A2-Broken_Authentication_and_S
,→ession_Management
URL:https://www.owasp.org/index.php/Top_10_2013-A6-Sensitive_Data_Exposure
URL:https://cwe.mitre.org/data/definitions/319.html

Medium (CVSS: 4.3)
NVT: jQuery < 1.9.0 XSS Vulnerability

Resultado de detección del producto
cpe:/a:jquery:jquery:1.8.3
Detected by jQuery Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.141622)

Resumen
jQuery before 1.9.0 is vulnerable to Cross-site Scripting (XSS) attacks. The jQuery(strInput) function does not di erentiate selectors from HTML in a reliable fashion. In vulnerable versions, jQuery determined whether the input was HTML by looking for the '<' character anywhere in the string, giving attackers more exibility when attempting to construct a malicious payload. In xed versions, jQuery only deems the input to be HTML if it explicitly starts with the '<' character, limiting exploitability only to attackers who can control the beginning of a string, which is far less common.

Resultado de detección de vulnerabilidad
Installed version: 1.8.3
Fixed version: 1.9.0
Installation
path / port: /https://www.upea.bo/assets/tabtheme/js

Solución
Tipo de solución: VendorFix
Update to version 1.9.0 or later.

Software / SO afectado
jQuery prior to version 1.9.0.

Método de detección de vulnerabilidad
Checks if a vulnerable version is present on the target host.
Detalles: jQuery < 1.9.0 XSS Vulnerability
OID:1.3.6.1.4.1.25623.1.0.141636
Versión utilizada: 2019-08-27T12:52:16+0000

Resultado de detección del producto
Producto: cpe:/a:jquery:jquery:1.8.3
Metodo: jQuery Detection (HTTP)
OID: 1.3.6.1.4.1.25623.1.0.141622)

References
CVE: CVE-2012-6708
Other:
URL:https://bugs.jquery.com/ticket/11290

[return to 186.121.206.248]

2.1.4 Medium 443/tcp

Medium (CVSS: 6.4)
NVT: SSL/TLS: Missing `secure` Cookie Attribute

Resumen
The host is running a server with SSL/TLS and is prone to information disclosure vulnerability.

Resultado de detección de vulnerabilidad
The cookies:
Set-Cookie: ci_session=vttt1c3u624pl148tj3j9uonl72mr66s; expires=Tue, 07-Jul-202
,→0 23:51:30 GMT; Max-Age=***replaced***; path=/; HttpOnly
are missing the "secure" attribute.

Solución
Tipo de solución: Mitigation
Set the 'secure' attribute for any cookies that are sent over a SSL/TLS connection.

Software / SO afectado
Server with SSL/TLS.

Perspectiva de vulnerabilidad
The aw is due to cookie is not using 'secure' attribute, which allows cookie to be passed to the server by the client over non-secure channels (http) and allows attacker to conduct session hijacking attacks.

Método de detección de vulnerabilidad
Detalles: SSL/TLS: Missing `secure` Cookie Attribute
OID:1.3.6.1.4.1.25623.1.0.902661
Versión utilizada: 2020-05-11T11:32:41+0000

References
Other:
URL:https://www.owasp.org/index.php/SecureFlag
URL:http://www.ietf.org/rfc/rfc2965.txt
URL:https://www.owasp.org/index.php/Testing_for_cookies_attributes_(OWASP-SM-
,→002)

[return to 186.121.206.248]

2.1.5 Low general/tcp

Low (CVSS: 2.6) NVT: TCP timestamps
Resumen The remote host implements TCP timestamps and therefore allows to compute the uptime.
Resultado de detección de vulnerabilidad It was detected that the host implements RFC1323. The following timestamps were retrieved with a delay of 1 seconds in-between: Packet 1: 1143652761 Packet 2: 1143653044
Impacto A side e ect of this feature is that the uptime of the remote host can sometimes be computed.
Solución Tipo de solución: Mitigation To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime. To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled' Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled.
The default behavior of the TCP/IP stack on this Systems is to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment. See the references for more information.
Software / SO afectado TCP/IPv4 implementations that implement RFC1323.
Perspectiva de vulnerabilidad The remote host implements TCP timestamps, as de ned by RFC1323.
Método de detección de vulnerabilidad Special IP packets are forged and sent with a little delay in between to the target IP. The responses are searched for a timestamps. If found, the timestamps are reported. Detalles: TCP timestamps OID:1.3.6.1.4.1.25623.1.0.80091 Versión utilizada: 2020-03-21T13:23:23+0000
References Other: URL:http://www.ietf.org/rfc/rfc1323.txt URL:http://www.microsoft.com/en-us/download/details.aspx?id=9152

[return to 186.121.206.248]

5.2.1.5. IP 95.111.232.17

Reporte de Busqueda

July 8, 2020

Resumen

Este documento informa sobre los resultados de un análisis de seguridad automático. Todas las fechas se muestran usando la zona horaria Coordinated Universal Time , which is abbreviated UTC . La tarea era Immediate scan of IP 95.111.232.17 . El escaneo comenzó a las y terminó a las . los El informe primero resume los resultados encontrados. Luego, para cada host, El informe describe cada problema encontrado. Por favor considere el consejos dados en cada descripción, para recti car el problema.

Contents

Resumen de resultados

Host	High	Medium	Low	Log	Falso positivo
95.111.232.17 vmi381303.contaboserver.net	3	0	1	0	0
Total: 1	3	0	1	0	0

Las actualizaciones de seguridad del proveedor no son de con anza.
Las anulaciones están activadas. Cuando un resultado tiene una anulación, este informe utiliza la amenaza de la anulación.
La información sobre las anulaciones se incluye en el informe. Las
notas se incluyen en el informe.
Es posible que este informe no muestre detalles de todos los problemas encontrados. Solo

enumera los hosts que produjeron problemas.
Problemas con el nivel de amenaza sesión No se muestran. Problemas con el nivel de amenaza Depurar No se muestran. Problemas con el nivel de amenaza Falso positivo No se muestran. Solo resultados con una QoD mínima de 70 are shown.

Este informe contiene todos 4 resultados seleccionados por el ltrado descrito anteriormente. Antes de ltrar había 108 resultados.

Resultados por Host

2.1 95.111.232.17

Inicio de escaneo de host Fin de escaneo del host

Servicio (Port)	Nivel de amenaza

2.1.1 High general/tcp

High (CVSS: 10.0)
NVT: Report outdated / end-of-life Scan Engine / Environment (local)

Resumen
This script checks and reports an outdated or end-of-life scan engine for the following environments:
- Greenbone Source Edition (GSE)
- Greenbone Community Edition (GCE)
used for this scan.

NOTE: While this is not, in and of itself, a security vulnerability, a severity is reported to make you aware of a possible decreased scan coverage or missing detection of vulnerabilities on the target due to e.g.:
- missing functionalities
- missing bug xes
- incompatibilities within the feed.

Resultado de detección de vulnerabilidad
Installed GVM Libraries (gvm-libs) version: 9.0.3
Latest available GVM Libraries (gvm-libs) version: 10.0.2
Reference URL(s) for the latest available version: https://community.greenbone.n
,→et/t/gvm-11-stable-initial-release-2019-10-14/3674 /https://community.greenbo
,→ne.net/t/gvm-10-old-stable-initial-release-2019 04-05/208

Solución
Tipo de solución: VendorFix
Update to the latest available stable release for your scan environment. Please check the references for more information. If you're using packages provided by your Linux distribution please contact the maintainer of the used distribution / repository and request updated packages.
If you want to accept the risk of a possible decreased scan coverage or missing detection of vulnerabilities on the target you can set a global override for this script as described in the linked manuals.

Método de detección de vulnerabilidad
Detalles: Report outdated / end-of-life Scan Engine / Environment (local)
OID:1.3.6.1.4.1.25623.1.0.108560
Versión utilizada: 2020-06-10T13:24:20+0000

References
Other:
URL:https://www.greenbone.net/en/install_use_gce/
URL:https://community.greenbone.net/t/gvm-9-end-of-life-initial-release-2017-
,→03-07/211
URL:https://community.greenbone.net/t/gvm-10-old-stable-initial-release-2019-
,→04-05/208
URL:https://community.greenbone.net/t/gvm-11-stable-initial-release-2019-10-1
,→4/3674
URL:https://docs.greenbone.net/GSM-Manual/gos-4/en/reports.html#creating-an-o
,→verride
URL:https://docs.greenbone.net/GSM-Manual/gos-5/en/reports.html#creating-an-o
,→verride
URL:https://docs.greenbone.net/GSM-Manual/gos-6/en/reports.html#creating-an-o
,→verride

[return to 95.111.232.17]

2.1.2 High 8009/tcp

High (CVSS: 7.5)
NVT: Apache JServ Protocol (AJP) Public WAN (Internet) Accessible

Resumen
The script checks if the target host is running a service supporting the Apache JServ Protocol (AJP) accessible from a public WAN (Internet).

Resultado de detección de vulnerabilidad
La vulnerabilidad se detectó de acuerdo con el Método de detección de vulnerabilidad.

Solución
Tipo de solución: Mitigation
Only allow access to the AJP service from trusted sources / networks.

Perspectiva de vulnerabilidad

When using the Apache JServ Protocol (AJP), care must be taken when trusting incoming connections to Apache Tomcat. Tomcat treats AJP connections as having higher trust than, for example, a similar HTTP connection. If such connections are available to an attacker, they can be exploited in ways that may be surprising (e.g. bypassing security checks, bypassing user authentication among others).

Método de detección de vulnerabilidad

Evaluate if the target host is running a service supporting the Apache JServ Protocol (AJP) accessible from a public WAN (Internet).

Detalles: Apache JServ Protocol (AJP) Public WAN (Internet) Accessible

OID:1.3.6.1.4.1.25623.1.0.108716

Versión utilizada: 2020-03-02T11:38:26+0000

References

Other:

URL:https://lists.apache.org/thread.html/r7c6f492fbd39af34a68681dbbba0468490ff
,→1a97a1bd79c6a53610ef%40%3Cannounce.tomcat.apache.org%3E

High (CVSS: 7.5)

NVT: Apache Tomcat AJP RCE Vulnerability (Ghostcat)

Resumen

Apache Tomcat is prone to a remote code execution vulnerability (dubbed 'Ghostcat') in the AJP connector.

Resultado de detección de vulnerabilidad

It was possible to read the file "/WEB-INF/web.xml" through the AJP connector.

Result:

AB w È 200 =JSESSIONID=C5881012D154214E7E0BD7F778D3591A; Path=/; HttpOnly
,→ text/html;charset=ISO-8859-1 1227 AB Ï Ë<?xml version="1.0" encoding
,→="UTF-8"?>
<!--

```
 Licensed to the Apache Software Foundation (ASF) under one or more
  contributor license agreements.  See the NOTICE file distributed with
  this work for additional information regarding copyright ownership.
  The ASF licenses this file to You under the Apache License, Version 2.0
  (the "License"); you may not use this file except in compliance with
  the License.  You may obtain a copy of the License at
      http://www.apache.org/licenses/LICENSE-2.0
  Unless required by applicable law or agreed to in writing, software
  distributed under the License is distributed on an "AS IS" BASIS,
  WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
  See the License for the specific language governing permissions and
  limitations under the License.
-->
<web-app xmlns="http://xmlns.jcp.org/xml/ns/javaee"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://xmlns.jcp.org/xml/ns/javaee
                      http://xmlns.jcp.org/xml/ns/javaee/web-app_4_0.xsd"
  version="4.0"
  metadata-complete="true">
  <display-name>Welcome to Tomcat</display-name>
  <description>
     Welcome to Tomcat
  </description>
</web-app>
 AB
```

Solución

Tipo de solución: VendorFix

Update Apache Tomcat to version 7.0.100, 8.5.51, 9.0.31 or later. For other products using Tomcat please contact the vendor for more information on xed versions.

Software / SO afectado

Apache Tomcat versions prior 7.0.100, 8.5.51 or 9.0.31 when the AJP connector is enabled. Other products like JBoss or Wild y which are using Tomcat might be a ected as well.

Perspectiva de vulnerabilidad

Apache Tomcat server has a le containing vulnerability, which can be used by an attacker to read or include any les in all webapp directories on Tomcat, such as webapp con guration les or source code.

Método de detección de vulnerabilidad

Sends a crafted AJP request and checks the response.

Detalles: Apache Tomcat AJP RCE Vulnerability (Ghostcat)

OID:1.3.6.1.4.1.25623.1.0.143545

Versión utilizada: 2020-05-11T07:16:09+0000

References

```
CVE: CVE-2020-1938
Other:
  URL:https://lists.apache.org/thread.html/r7c6f492fbd39af34a68681dbbba0468490ff
,→1a97a1bd79c6a53610ef%40%3Cannounce.tomcat.apache.org%3E
    URL:https://www.chaitin.cn/en/ghostcat
    URL:https://www.cnvd.org.cn/flaw/show/CNVD-2020-10487
    URL:https://github.com/YDHCUI/CNVD-2020-10487-Tomcat-Ajp-lfi
    URL:https://securityboulevard.com/2020/02/patch-your-tomcat-and-jboss-instanc
,→es-to-protect-from-ghostcat-vulnerability-cve-2020-1938-and/
    URL:https://tomcat.apache.org/tomcat-7.0-doc/changelog.html
    URL:https://tomcat.apache.org/tomcat-8.5-doc/changelog.html
    URL:https://tomcat.apache.org/tomcat-9.0-doc/changelog.html
```

[return to 95.111.232.17]

2.1.3 Low general/tcp

Low (CVSS: 2.6) NVT: TCP timestamps
Resumen The remote host implements TCP timestamps and therefore allows to compute the uptime.
Resultado de detección de vulnerabilidad It was detected that the host implements RFC1323. The following timestamps were retrieved with a delay of 1 seconds in-between: Packet 1: 949406682 Packet 2: 949407027
Impacto A side e ect of this feature is that the uptime of the remote host can sometimes be computed.
Solución Tipo de solución: Mitigation To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime. To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled' Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled. The default behavior of the TCP/IP stack on this Systems is to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment. See the references for more information.
Software / SO afectado TCP/IPv4 implementations that implement RFC1323.
Perspectiva de vulnerabilidad The remote host implements TCP timestamps, as de ned by RFC1323.

Método de detección de vulnerabilidad Special IP packets are forged and sent with a little delay in between to the target IP. The responses are searched for a timestamps. If found, the timestamps are reported. Detalles: TCP timestamps OID:1.3.6.1.4.1.25623.1.0.80091 Versión utilizada: 2020-03-21T13:23:23+0000
References Other: URL:http://www.ietf.org/rfc/rfc1323.txt URL:http://www.microsoft.com/en-us/download/details.aspx?id=9152

[return to 95.111.232.17]

Muchas gracias

5.3. PRUEBA DE HIPOTESIS

Una hipótesis es una proposición o supuesto sobre los parámetros de una o más poblaciones.

Para este tipo de aplicaciones se usan tipos de hipótesis de manera más formal esto se puede expresar como:

- Ho: Que representa hipótesis nula
- H1: Que representa hipótesis alternativa

Esta última puede ser una hipótesis alternativa bilateral o una hipótesis alternativa unilateral, eso depende de los valores que la misma pueda tomar.

Algo para tomar en cuenta, es que las hipótesis siempre son proposiciones sobre la población o sobre la muestra.

Un procedimiento que conduce a una decisión sobre una hipótesis en particular recibe el nombre de prueba de hipótesis. Los procedimientos de la prueba de hipótesis dependen del

empleo de la información contenida en la muestra aleatoria de la población de interés. Si esta información es consistente con la hipótesis, se concluye que esta es verdadera; por otra parte, si esta información es inconsistente con la hipótesis, se concluye que esta es falsa.

La hipótesis nula, representada por Ho, es la afirmación sobre una o más características de poblaciones que al inicio se supone es cierta para el investigador.

La hipótesis alternativa, representada por H1, es la afirmación contradictoria a Ho.

La hipótesis nula se rechaza a favor de la hipótesis alternativa, solo si la evidencia maestral sugiere que Ho es falso. Si la muestra no contradice decididamente a Ho, se continúa creyendo en la validez de la hipótesis nula. Entonces, las dos conclusiones posibles de un análisis por prueba de hipótesis son rechazar Ho o no rechazar Ho.

En el caso de que la hipótesis nula sea verdadera y se la rechazase, esto es llamado error del tipo uno, en caso de que la hipótesis nula sea falsa y no se la rechazase este procedimiento es llamado error de tipo dos.

5.3.1. Pasos de la prueba de hipótesis

Etapas para una prueba de hipótesis.

- Primero se define la hipótesis nula, en este caso la hipótesis del investigador.
- Se formula la hipótesis alternativa o también llamada contra-hipótesis.
- Se elige un nivel de significancia y a partir de este nivel se construye la zona de aceptación.
- Con la zona de aceptación surge la zona de rechazo la cual se llama región crítica y su área es el nivel de significación o aceptación.
- Se verifica la hipótesis extrayendo una muestra.

- Se evalúa con una prueba estadística.
- Mediante el proceso se evalúa el cumplimiento de la hipótesis.

Para fines de esta tesis se realizaron pruebas en distintas IP públicas.

5.3.1. Resultados

- En la primera prueba en lo que hacemos énfasis en la búsqueda de sus vulnerabilidades y da un reporte.

Tabla: 5.1. *Tabla de pruebas realizadas*

Descripción	**Nro. De Pruebas**	**Porcentaje**
Pruebas aceptadas	10	100%
Pruebas rechazadas	0	0%
Total de pruebas	10	100%

Fuente: [Elaboración propia]

- En la Segunda prueba en lo que hacemos énfasis en la búsqueda de sus vulnerabilidades y da un reporte.

Tabla: 5.2. *Tabla de pruebas realizadas*

Descripción	**Nro. De Pruebas**	**Porcentaje**
Pruebas aceptadas	10	100%
Pruebas rechazadas	0	0%
Total de pruebas	10	100%

Fuente: [Elaboración propia]

- En la Tercera prueba en lo que hacemos énfasis en la búsqueda de sus vulnerabilidades y da un reporte.

Tabla: 5.3. *Tabla de pruebas realizadas*

Descripción	**Nro. De Pruebas**	**Porcentaje**
Pruebas aceptadas	9	90%
Pruebas rechazadas	1	10%
Total de pruebas	10	100%

Fuente: [Elaboración propia]

5.3.2. Resultado Total

En la tabla 5.4. observamos el total de los resultados.

Tabla: 5.4. *En esta tabla apreciaremos los resultados totales de las pruebas realizadas.*

Descripción	**Nro. De Pruebas**	**Porcentaje**
Pruebas aceptadas	29	97%
Pruebas rechazadas	1	3%
Total de Pruebas	30	100%

Fuente: [Elaboración propia]

5.4. Evaluación de Resultados

En este punto ahora aplicaremos el método estadístico que se usara para el presente trabajo es el de proporciones.

Pruebas totales: 30

Pruebas aceptadas: 29

Pruebas reprobadas:	1
Porcentaje de éxitos:	97%
Porcentaje de fracasos:	3%

Como se observa en los resultados, el porcentaje de éxitos es mayor al 95% esperado al momento de plantearse la Hipótesis, pero para comprobar de manera cuantificable si este valor se asemeja al valor esperado, se realiza una prueba de hipótesis estadística.

Las variables usadas en dicha prueba serán las mismas mencionadas en la evaluación de casos de prueba:

Po = 95

qo = 5

p = 97

n = 30

N es el número total de sujetos en el espacio muestral y no se conoce. Además, que se tomará un nivel de significancia α del 5%.

Para el caso de la hipótesis se tiene los siguientes datos:

En este caso se espera que el porcentaje de éxitos sea igual o mayor a 95%:

$$H_o: P \geq P_o$$

$$H_1: P < P_o$$

Reemplazando:

$$H_o: P \geq 0.95$$

$$H_1: P < 0.95$$

5.5. DETERMINACION DE LA REGION CRITICA

La región critica para la hipótesis planteada es la siguiente:

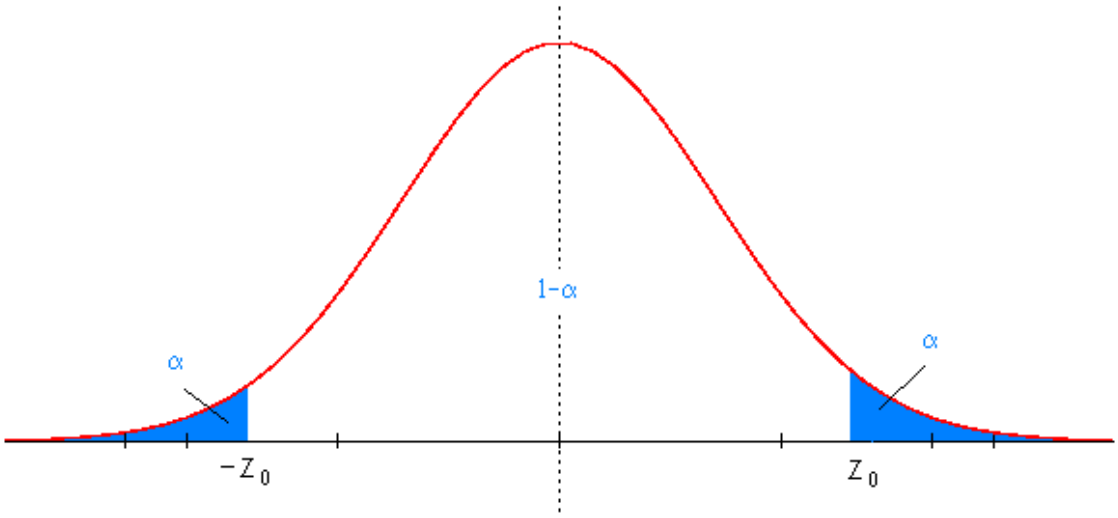


Figura: 5.5. Región critica para la hipotenusa.

Fuente: [Elaboración propia]

Como n se refiere en este caso al número de pruebas, en este caso 30, el punto crítico a usar es -Z_o y se determina mediante:

$$-Z_o = -Z_{1-\propto} = -Z_{1-0.05}$$

$$-Z_o = -Z_{0.05}$$

Este valor se halla de la tabla de la función de distribución normal. Para obtener el valor de z se elige de la tabla mencionada el valor más cercano a 0,95; el cual está ubicado en la fila 1,6 y columna 0,04.

Z	…	0.04
…		↓
1,6	→	0.94950

Figura: 5.6. Resultado tabla de la función de distribución normal.

Fuente: [Elaboración propia]

El valor de Z se obtiene sumando ambos valores:

$$Z_{0,95} = (1.6 + 0.04) = 1.64$$

Se relocalizará el cálculo estadístico con los valores que tenemos:

Como se conoce el número total de individuos en el espacio muestral, el valor del estadístico de la prueba se obtiene mediante la fórmula:

$$Z_c = \frac{p - p_o}{\sqrt{\frac{p_o q_o}{n}}} = \frac{0.97 - 0.95}{\sqrt{\frac{0.95 * 0.05}{30}}} = 0.502$$

Al comparar el valor de los estadísticos Z_0 y Z_c, se observa que el valor del estadístico de la prueba no se encuentra dentro de la región crítica, por lo tanto se acepta la hipótesis nula H_0.

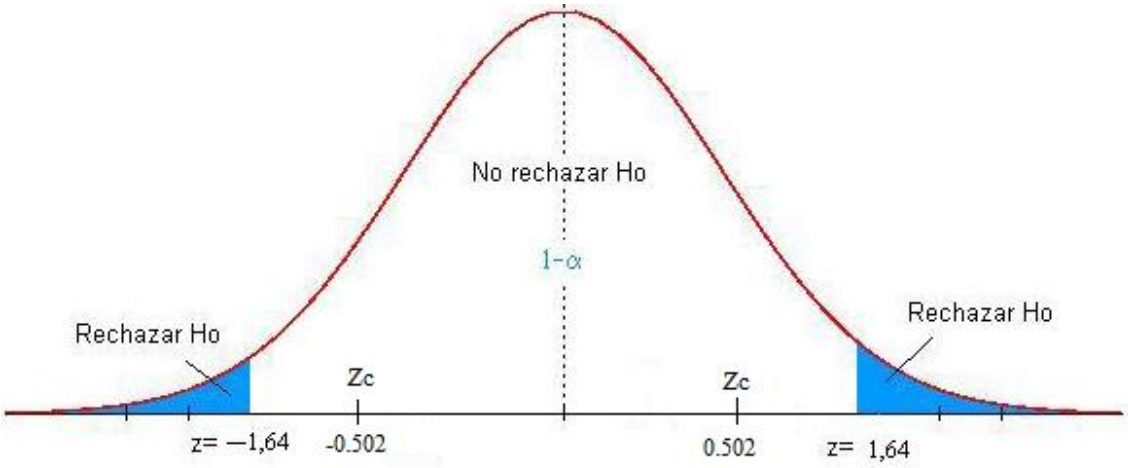


Figura: 5.7. distribución de Z_0 y Z_c en el grafico para a toma de decisiones.

Fuente: [Elaboración propia]

El promedio de éxito del prototipo al momento de reconocer las muestras se acerca al 95%. Por tanto, como no se rechaza *H*0 se podría concluir y afirmar la hipótesis *H*0: "CON EL APOYO DE HERRAMIENTAS Y METODOLOGIAS SE IMPLEMENTA UN MODELO PARA LA BUSQUEDA DE VULNERABILIDADES EN LA INFRAESTRUCTURA DE LA INFORMACION (SERVIDORES Y SERVICIOS) DE "IKRIT.SRL", CON UNA EFICIENCIA DE 95%"

5.6. ANTES Y DESPUES

Tabla: 5.5. *Tabla de un antes y un después de la institución "IKRIT.SRL"*

Antes	Después
No había control de puertos y servicios	Ahora se puede sacar un informe acerca de los puertos y servicios
No había un análisis de vulnerabilidades en el servidor.	Actualmente se puede realizar el análisis al servidor de la institución.
Antes no existía un reporte de vulnerabilidades.	Ahora existe un reporte de vulnerabilidades.

Fuente: [Elaboración propia]

CAPITULO VI

CONCLUCIONES Y RECOMENDACIONES

6.1. CONCLUCIONES

De acuerdo con los objetivos planteados y los resultados obtenidos durante el desarrollo de los capítulos anteriores de la presente tesis Se logro implementar un modelo de seguridad, que permite la búsqueda de vulnerabilidades y asi evitar usar las vulnerabilidades en contra de la institución.

6.2. RECOMENDACIONES

- Se recomienda a la institución que realice las gestiones necesarias para poder poner un Data center con las normas requeridas.
- Se recomienda a la institución que debe de ejecutar el test de seguridad al menos 6 veces al dia.
- Se recomienda a la institución de analizar las vulnerabilidades existentes si es que las hubiesen.
- Se recomienda a la institución de cada búsqueda de vulnerabilidad guardar los reportes.
- Se recomienda a la institución de que los reportes que ubiesen utilizar y apoyar en la toma de decisiones.

Bibliografía

Adastra. (02 de Agosto de 2011). *The HackerWay*. Obtenido de The HackerWay: https://thehackerway.com/2011/08/02/conceptos-basicos-avanzados-y-herramientas-de-footprintingfingerprinting-%E2%80%93-maltego/

Admin. (22 de Septiembre de 2014). *kalilinux.foroactivo*. Obtenido de kalilinux.foroactivo: https://kalilinux.foroactivo.com/t90-preguntas-frecuentes-dsniff

Alexalvarez0310. (13 de Mayo de 2009). *Entre Redes y servidores*. Obtenido de Entre Redes y Servidores: https://alexalvarez0310.wordpress.com/2009/05/13/puertos-bien-conocidos/

Amaya, J. (2 de Septiembre de 2016). *Nearsoft Jobs*. Obtenido de Nearsoft Jobs: https://blog.nearsoftjobs.com/qu%C3%A9-es-y-qu%C3%A9-no-es-un-patr%C3%B3n-de-dise%C3%B1o-487643d37a62

Anonimo. (29 de octubre de 2018). *NegociosdelWEB*. Obtenido de NegociosdelWEB: https://www.negociosdelweb.com/para-que-sirve-un-servidor-web/

anonimo. (19 de julio de 2019). *ConceptosDefinicion*. Obtenido de ConceptosDefinicion: https://conceptodefinicion.de/prototipo/

arlethparedes. (23 de Septiembre de 2012). *arlethparedes*. Obtenido de arlethparedes: https://arlethparedes.wordpress.com/2012/09/23/el-patron-mvc-modelo-vista-controlador/

Arsys. (30 de 12 de 2015). *Nosotros Programacion*. Obtenido de Nosotros Programacion: https://www.arsys.es/blog/programacion/protocolos-de-internet-http-y-ftp/

ARWEB. (26 de Septiembre de 2014). *ARWEB*. Obtenido de ARWEB: https://www.arweb.com/blog/%C2%BFque-es-bootstrap-y-como-funciona-en-el-diseno-web/

Axarnet. (31 de Octubre de 2017). *axarnet.es*. Obtenido de axarnet.es: https://axarnet.es/blog/bootstrap

B., G. (01 de Noviembre de 2019). *HOSTINGER*. Obtenido de HOSTINGER: https://www.hostinger.es/tutoriales/que-es-apache/

Barbosa, D. C. (02 de Enero de 2020). *WeliveSecurity by eseet*. Obtenido de WeliveSecurity by eseet: https://www.welivesecurity.com/la-es/2020/01/02/que-es-proxy-para-que-sirve/

Bembibre, V. (enero de 2009). *DefinicionABC*. Obtenido de DefinicionABC: https://www.definicionabc.com/tecnologia/http.php

Berenicemh10. (10 de enero de 2013). *SCRIBD*. Obtenido de SCRIBD: https://es.scribd.com/doc/119388599/Caracteristicas-e-Importancia-de-Los-Modelos-en-La-Ciencia

Borges, E. (12 de Marzo de 2019). *InfraNetworking*. Obtenido de InfraNetworking: https://blog.infranetworking.com/servidor-de-correo/#Conclusion

Borges, E. (17 de Marzo de 2019). *InfraNetworking*. Obtenido de InfraNetworking: https://blog.infranetworking.com/servidor-base-de-datos/

Borges, S. (2002-2020). *InfraNetworking*. Obtenido de InfraNetworking: https://blog.infranetworking.com/servidor-web/

Brito, A. M. (2008). Algoritmos Cualiativos. *CENTRO BIOTECNOLOGICO DEL CARIBE*, 1.

C., d. (2020). *HOSTINGER TUTORIALES*. Obtenido de HOSTINGER TUTORIALES: https://www.hostinger.es/tutoriales/que-es-ssh

Cansino, M. (20 de mayo de 2019). *techlandia*. Obtenido de techlandia: https://techlandia.com/tipos-sistemas-operativos-linux-sobre_37282/

capa8. (01 de septiembre de 2015). *capaocho*. Obtenido de capaocho: http://capaocho8.com/conoces-los-tipos-de-hacking/

Cloud, C. (2015). *Clinic Cloud*. Obtenido de Clinic Cloud: https://clinic-cloud.com/blog/protocolos-de-seguridad-de-la-informacion/

Conceptodefinicion.de. (17 de julio de 2019). *Conceptodefinicion.de*. Obtenido de Conceptodefinicion.de: https://conceptodefinicion.de/servicio/

creadpag. (22 de Mayo de 2018). *creadpag.com*. Obtenido de creadpag.com: https://www.creadpag.com/2018/05/aprendamos-usar-fuerza-bruta-con.html

Dongee. (10 de Noviembre de 2018). *Dongee*. Obtenido de Dongee: https://blog.dongee.com/las-7-vulnerabilidades-m%C3%A1s-comunes-de-sitios-web-que-no-puedes-pasar-por-alto-59f29c1c3aea

EHACKING. (29 de Abril de 2019). *EthicalHacking*. Obtenido de EthicalHacking: https://blog.ehcgroup.io/2019/04/29/15/18/28/5144/las-10-herramientas-hacking-de-fuerza-bruta-mas-populares/delitos-informaticos/ehacking/

Escobar, J. (10 de marzo de 2009). *Simple BLOG*. Obtenido de Simple BlLOG: http://ingenieriasimple.com/blog/blog/2009/03/09/el-diseno-en-ingenieria/

FM, Y. (31 de Mayo de 2017). *Xataka*. Obtenido de Xataca: https://www.xataka.com/basics/que-es-un-proxy-y-como-puedes-utilizarlo-para-navegar-de-forma-mas-anonima

Frutos, A. M. (12 de junio de 2016). *Computer hoy*. Obtenido de Computer hoy: https://computerhoy.com/noticias/internet/que-es-servidor-46228

g42roram. (2006-2020). *apr*. Obtenido de apr: https://www.aprenderaprogramar.com/index.php?option=com_content&view=article&id=542:que-es-un-servidor-y-cuales-son-los-principales-tipos-de-servidores-proxydns-webftppop3-y-smtp-dhcp&catid=57&Itemid=179

Garcia, G. (17 de Octubre de 2008). *es.scribd.com*. Obtenido de es.scribd.com: https://es.scribd.com/doc/6963842/NetCat-para-Ignorantes

Garcia, M. (05 de Octubre de 2017). *coding or not*. Obtenido de coding or not: https://codingornot.com/mvc-modelo-vista-controlador-que-es-y-para-que-sirve

Gomez , A. Lopez, M. Migani, S. (10 de Agosto de 2017). *COCOMO*. Obtenido de COCOMO: https://blogadmi1.files.wordpress.com/2010/11/cocom0llfull.pdf.

Herrero, H. (20 de Octubre de 2008). *Blog Bujarra*. Obtenido de Blog Bujarra: http://www.bujarra.com/uso-de-ettercap/

INCIBE. (20 de Marzo de 2017). *incibe_*. Obtenido de incibe_: https://www.incibe.es/protege-tu-empresa/blog/amenaza-vs-vulnerabilidad-sabes-se-diferencian

Informática, N. d. (27 de Junio de 2007). *Noticias de Seguridad Informática*. Obtenido de Noticias de Seguridad Informática: https://seguinfo.wordpress.com/2007/06/27/%C2%BFque-es-nmap/

Informatica, S. (27 de Junio de 2007). *seguinfo.wordpress.com*. Obtenido de seguinfo.wordpress.com: https://seguinfo.wordpress.com/2007/06/27/%C2%BFque-es-nmap/

Iniseg. (06 de agosto de 2018). *Ciberseguridad al dia*. Obtenido de Ciberseguridad al dia: https://www.iniseg.es/blog/ciberseguridad/que-es-el-hacking-etico/

INTEF. (2012). Aulas en red. Aplicaciones y Servicios. Linux Servidor DHCP y Servidor DNS. *Formacion en Red*, 3-5.

ISO25000. (2019). *iso25000.com*. Obtenido de iso25000.com: https://iso25000.com/index.php/normas-iso-25000?limit=4&limitstart=0

ITTGWEB. (28 de Mayo de 2016). *WORDPRESS*. Obtenido de WORDPRESS: https://ittgweb.wordpress.com/2016/05/28/3-5-diseno-de-software-de-arquitectura-arquitectura-cliente-servidor/

Jazz, E. (30 de Noviembre de 2014). *es.scribd.com*. Obtenido de es.scribd.com: https://es.scribd.com/document/248715839/Que-Es-Un-Metasploit

Jimenez, A. C. (31 de Marzo de 2017). *Cronicaseguridad.com*. Obtenido de Cronicaseguridad.com: https://cronicaseguridad.com/2017/03/31/seguridad-logica-gestion-la-informacion-confidencialidad-integridad-disponibilidad-estanqueidad/

KENDALL, K. E. (2011). Analisis y Diseño de Software. En K. E. KENDALL, *Analisis y Diseño de Software* (págs. 156-161). Mexico: PEARSON EDUCACION.

Kunar, P. (06 de Febrero de 2020). *LinuxTechi*. Obtenido de LinuxTechi: https://www.linuxtechi.com/nc-ncat-command-examples-linux-systems/

Linux, O. (01 de Septiembre de 2018). *Kali Linux para novatos*. Obtenido de Kali Linux para novatos: https://operslinux.blogspot.com/2018/09/que-es-nessus-y-como-se-instala-en-kali.html?m=0

Lockhart, T. (1996-9). *Manual del usuario de PostgreSQL.* Postgres Global Development Group.

Luz, S. D. (30 de Octubre de 2016). *redeszone.net*. Obtenido de redeszone.net: https://www.redeszone.net/2016/10/30/social-engineer-toolkit-sera-kit-herramientas-auditorias-usando-la-ingenieria-social/

marindelafuente. (29 de Abril de 2019). *marindelafuente*. Obtenido de marindelafuente: https://www.marindelafuente.com.ar/que-es-nmap-por-que-necesitas-este-mapeador-de-red/

Marquez, A. (15 de Marzo de 2020). *TESTER moderno*. Obtenido de TESTER moderno: https://www.testermoderno.com/caja-blanca-vs-caja-negra/

micarrerauniversitaria.com. (2019). *micarrerauniversitaria.com*. Obtenido de micarrerauniversitaria.com: https://micarrerauniversitaria.com/c-ingenieria/ingeniero-de-seguridad/

Montufar, L. S. (s.f.). Informatica II un enfoque constructivista. En L. S. Montufar, *Informatica II un enfoque constructivista* (pág. 5). mexico: PEARSON EDUCACION DE MEXICO.

OpenCloud. (08 de Diciembre de 2016). *OpenCloud*. Obtenido de OpenCloud: https://docs.opencloud.cl/tutoriales/servidores/lista-de-puertos-mas-comunmente-utilizados.html

Padilla, A. L. (s.f.). Guia de Seguridad en Servicios DNS. *INTECO*, 6-51.

Perez, L. (25 de Abril de 2016). *Prezi*. Obtenido de Prezi: https://prezi.com/m4txp3u8pmyu/protocolos-de-conexion-a-la-base-de-datos/

Perez, L. S. (04 de Septiembre de 2012). *Ingenieria de Software*. Obtenido de Ingenieria de Software: http://softwareverde.blogspot.com/2012/09/definicion-de-modelo.html

PowerData. (02 de Junio de 2016). *PowerData*. Obtenido de PowerData: https://blog.powerdata.es/el-valor-de-la-gestion-de-datos/metricas-de-calidad-de-software-una-solucion-excelente

Pressman, R. S. (2010). *Ingenieria de Software.* mexico: The McGraw-Hill.

Raffino, M. E. (11 de enero de 2019). *Concepto.de*. Obtenido de Concepto.de: https://concepto.de/algoritmo-en-informatica/

Ramos, I. M. (2011). Modelo para la deteccion de intrusos en la seguridad de sistemas informaticos aplicando logica difusa. *Modelo para la deteccion de intrusos en la seguridad de sistemas informaticos aplicando logica difusa*. La paz, Bolivia.

Resendiz, U. V. (21 de agosto de 2018). *SlideShare*. Obtenido de SlideShare: https://es.slideshare.net/UlisesVillanueva1/maquetado-110798534

ReYDeS. (19 de Junio de 2014). *Reydes*. Obtenido de Reydes: http://www.reydes.com/d/?q=Ataque_de_Envenenamiento_ARP_utilizando_Ettercap

Ricardo. (02 de marzo de 2011). *Ingenieria de Software 1*. Obtenido de Ingenieria de Software 1: http://rarguetaingesoft1.blogspot.com/2011/03/uweuml-based-web-engineering.html

Rizaldos, H. (22 de Octubre de 2018). *OpenWebinars*. Obtenido de OpenWebinars: https://openwebinars.net/blog/que-es-metasploit/

robles, f. (2019). *Lifeder.com*. Obtenido de Lifeder.com: https://www.lifeder.com/tipos-algoritmos/

Rojas, J. M. (19 de Mayo de 2015). *Prezi*. Obtenido de Prezi: https://prezi.com/su8d3ymeqgq1/algoritmo-cualitativo-y-cuantitativo/

Roque, D. d. (25 de Noviembre de 2014). *Gestiopolis*. Obtenido de Gestiopolis: https://www.gestiopolis.com/estimacion-de-costos-de-desarrollo-de-software/

Rosell, J. (24 de Octubre de 2017). *S2 Grupo*. Obtenido de S2 Grupo: https://s2grupo.es/es/los-10-errores-ciberseguridad-mas-comunes-las-pymes/

RUBENFA. (14 de Julio de 2014). *GENBETA*. Obtenido de GENBETA: https://www.genbeta.com/desarrollo/patrones-de-diseno-que-son-y-por-que-debes-usarlos

Saavedra, A. (13 de Febrero de 2018). *CLAVEi*. Obtenido de CLAVEi: https://www.clavei.es/blog/que-es-la-infraestructura-it/

Sanchez, G. (07 de Febrero de 2017). *SlideShare*. Obtenido de SlideShare: https://es.slideshare.net/GermnSnchezDomnguez/metodologa-uwe-umlbased-web-engineering

Sanz, J. (31 de Octubre de 2013). *AZ adsl zone*. Obtenido de AZ adsl zone: https://www.adslzone.net/lista-de-puertos-para-abrir-por-orden-numerico.html

SBuendia. (08 de Mayo de 2012). *MSBC*. Obtenido de MSBC: https://currmsbc.blogspot.com/2012/05/metricas-de-costos.html

SECURITYTRAILS. (04 de Diciembre de 2018). *SECURITYTRAILS*. Obtenido de SECURITYTRAILS: https://securitytrails.com/blog/kali-linux-penetration-testing-tools

Significados. (16 de Febrero de 2017). *Significados*. Obtenido de Significados: https://www.significados.com/informacion/

Significados.com. (16 de Febrero de 2017). *Significados.com*. Obtenido de Significados.com: https://www.significados.com/datos/

Significados.com. (28 de Febrero de 2017). *Significados.com.* . Obtenido de Significados.com. : https://www.significados.com/seguridad/

Solano, A. (01 de Enero de 2019). *OpenWebinars*. Obtenido de OpenWebinars: https://openwebinars.net/blog/que-es-php/

Solano, A. A. (01 de Enero de 2019). *OpenWebinars*. Obtenido de OpenWebinars: https://openwebinars.net/blog/que-es-php/

Solorzano, C. D. (24 de agosto de 2015). *utel BLOG*. Obtenido de utel BLOG: https://www.utel.edu.mx/blog/menu-profesional/que-es-el-ethical-hacking/

SON, D. (16 de Agosto de 2017). *Pruebas de Penetracion*. Obtenido de Pruebas de Penetracion: https://securityonline.info/yersinia-framework-layer-2-attacks/

Song, D. (2020). *elmonton.net*. Obtenido de elmonton.net: http://www.elmonton.net/hacking/programas/suits/dsniff/3018/

Toro, M. F. (30 de Junio de 2017). *HostDimeBlog*. Obtenido de HostDimeBlog: https://www.hostdime.com.pe/blog/servidores-dedicados-juegos-online-que-debes-saber/

U.I.V. (21 de 03 de 2018). *Ciencias y tecnologia*. Obtenido de Ciencias y tecnologia: https://www.universidadviu.com/tres-tipos-seguridad-informatica-debes-conocer/

Upgrade. (01 de Octubre de 2019). *TECH & JOB*. Obtenido de TECH & JOB: https://upgrade-hub.com/protocolo-dns/

Valdes, D. P. (03 de jULIO de 2007). *MAESTROS DEL WEB*. Obtenido de MAESTROS DEL WEB: http://www.maestrosdelweb.com/que-es-javascript/

Valenzuela, J. C. (21 de Octubre de 2011). *Monografias plus*. Obtenido de Monografias plus: https://www.monografias.com/docs/Medidas-de-seguridad-para-un-equipo-de-F3Z9LCAZBY

Vega, V. (02 de Mayo de 2012). *SCRIBD*. Obtenido de SCRIBD: https://es.scribd.com/document/92143434/Modelo-UWE

Virguez, M. d. (2019). *Lifeder.com*. Obtenido de Lifeder.com: https://www.lifeder.com/algoritmos-computacionales/

Wikipedia. (02 de Marzo de 2020). *Wikipedia*. Obtenido de Wikipedia: https://es.wikipedia.org/wiki/Restaurar_sistema

Wikipedia. (13 de febrero de 2020). *Wikipedia*. Obtenido de Wikipedia: https://es.wikipedia.org/wiki/Distribuci%C3%B3n_Linux

Wikipedia. (17 de febrero de 2020). *Wikipedia*. Obtenido de Wikipedia: https://es.wikipedia.org/wiki/M%C3%B3dulo_(inform%C3%A1tica)

Wikipedia. (10 de Mayo de 2020). *Wikipedia*. Obtenido de Wikipedia: https://es.wikipedia.org/wiki/JavaScript

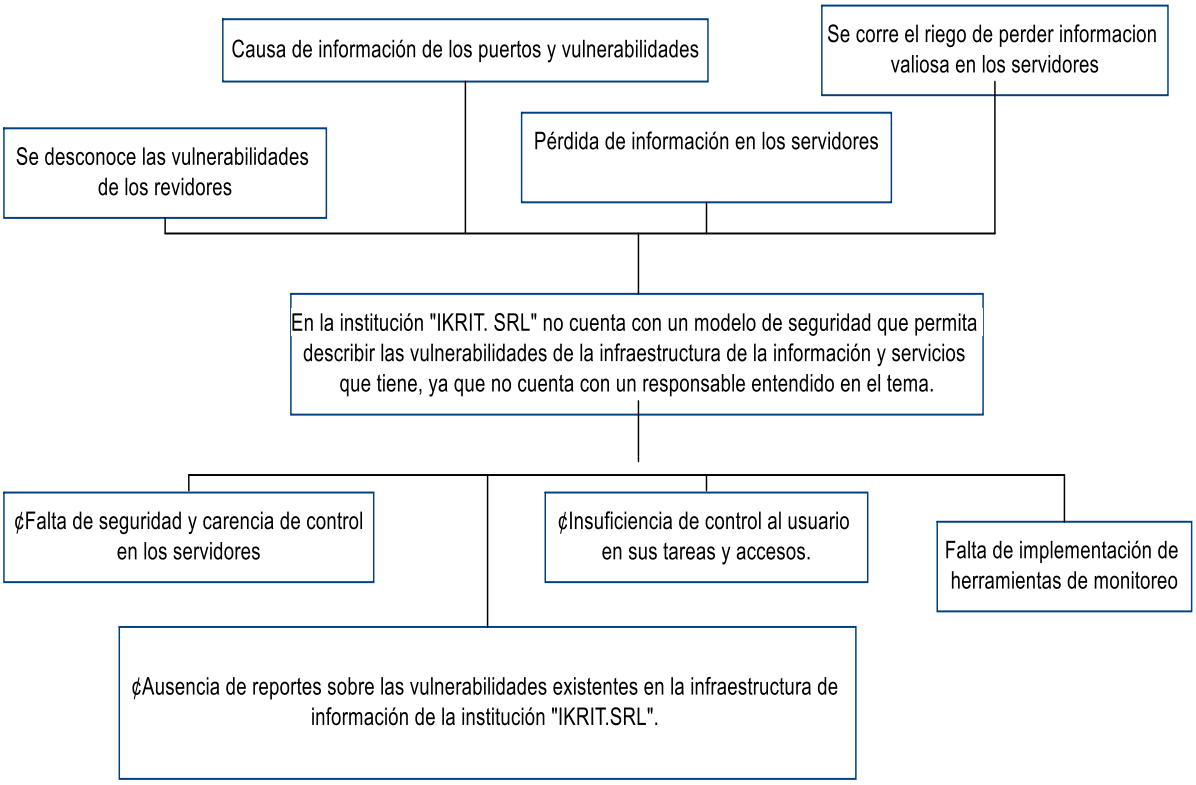
Xavi. (02 de Octubre de 20113). *Proyectos de Guerrilla*. Obtenido de Proyectos de Guerrilla: http://proyectosguerrilla.com/blog/2013/02/las-cinco-etapas-en-la-ingenieria-del-software/

XERALNET. (06 de Febrero de 2018). *vegagestion*. Obtenido de vegagestion: https://vegagestion.es/la-infraestructura-tecnologica-definicion-tipos-e-importancia/

ANEXOS

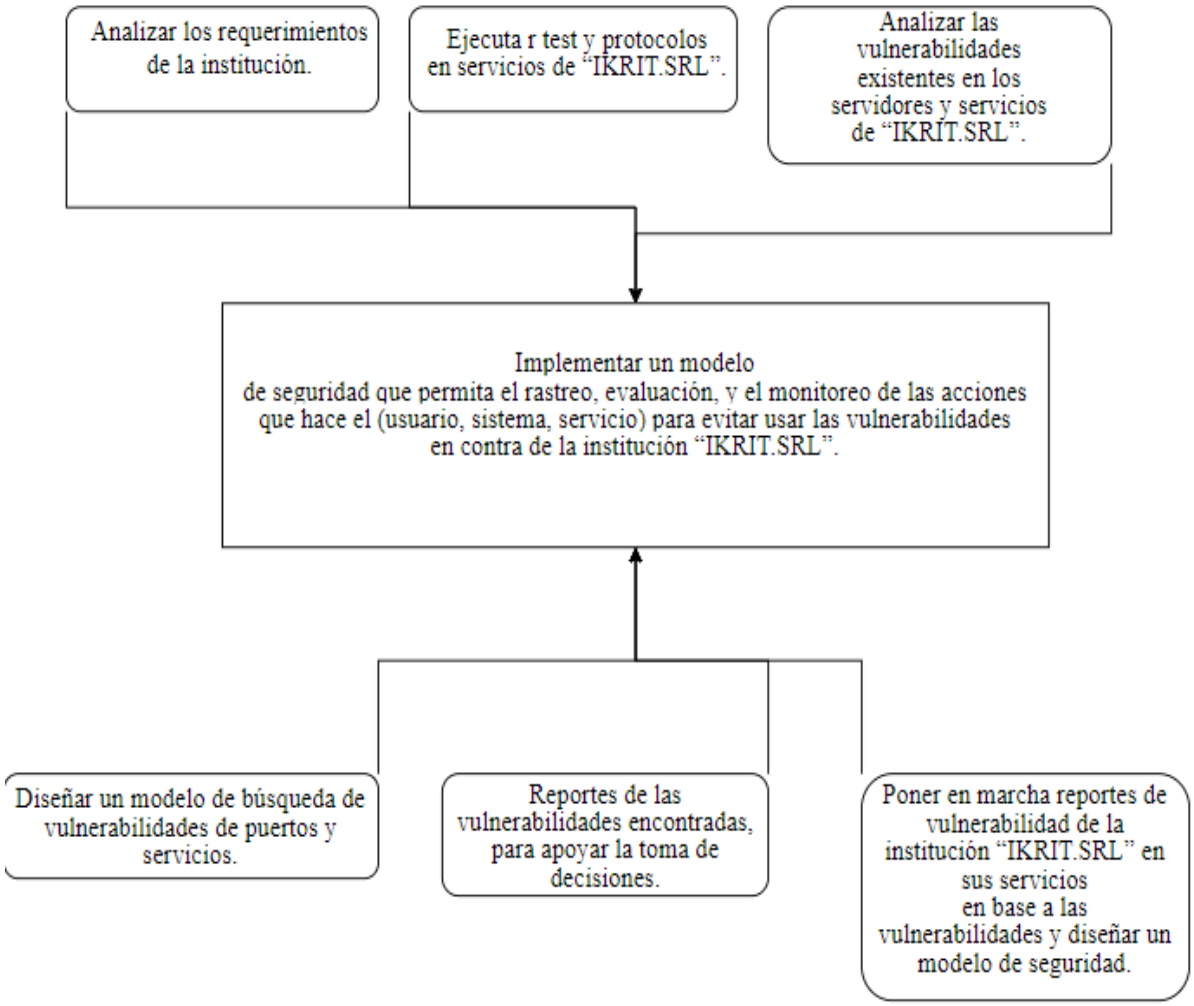
Anexo A

Árbol de problemas



Anexo B

Arbol de objetivos



Anexo C

Avales

La Paz – El Alto 08 de julio de 2020

Señor:

M.Sc. Ing. Enrique Flores Baltazar
TUTOR METODOLOGICO TALLER II

Presente. –

REF: Aval de Conformidad

Distinguido Ingeniero,

Mediante la presente tengo a bien comunicarle mi conformidad de la tesis de grado **"MODELO DE SEGURIDAD PARA INFRAESTRUCTURA DE INFORMACION"** caso **"IKRIT.SRL".** que propone el postulante Univ. Álvaro Chamizo Gutiérrez, con cedula de identidad 9944848 LP. Para su defensa publica, evaluación correspondiente a la materia taller de licenciatura II, de acuerdo a reglamento vigente de la carrera de Ingeniería de Sistemas de la Universidad Pública de El Alto

Sin otro particular, reciba saludos cordiales.

Atentamente.

Lic. Fredy Alanoca Coareti
TUTOR ESPECIALISTA

La Paz – El Alto 09 de julio de 2020

Señor:

M.Sc. Ing. Enrique Flores Baltazar
TUTOR METODOLOGICO TALLER II
CARRERA INGENIERIA DE SISTEMAS – U.P.E.A.

Presente. –

REF: Aval de Conformidad

Distinguido Ingeniero,

Mediante la presente tengo a bien comunicarle mi conformidad de la tesis de grado **"MODELO DE SEGURIDAD PARA INFRAESTRUCTURA DE INFORMACION"** caso **"IKRIT.SRL".** que propone el postulante Univ. Álvaro Chamizo Gutiérrez, con cedula de identidad 9944848 LP. Para su defensa publica, evaluación correspondiente a la materia taller de licenciatura II, de acuerdo a reglamento vigente de la carrera de Ingeniería de Sistemas de la Universidad Pública de El Alto

Sin otro particular, reciba saludos cordiales.

Atentamente.

ING. KATYA MARICELA PEREZ MARTINEZ
TUTOR REVISOR

La Paz – El Alto, julio de 2020

Señor:
Ing. David Carlos Mamani Quispe
DIRECTOR DE CARRERA INGENEIRIA DE SISTEMAS
Presente. –

REF: Aval de conformidad

Distinguido Ingeniero,

Mediante la presente tengo a bien comunicarle mi conformidad de la tesis de grado **"MODELO DE SEGURIDAD PARA INFRAESTRUCTURA DE INFORMACION"** caso **"IKRIT.SRL"**. que propone el postulante Univ. Álvaro Chamizo Gutiérrez, con cedula de identidad 9944848 LP., para su defensa publica, evaluación correspondiente a la materia de taller de licenciatura II, de acuerdo al reglamento vigente de la carrera de Ingeniería de Sistemas de la Universidad Pública de El Alto.

Sin otro particular, reciba saludos cordiales.

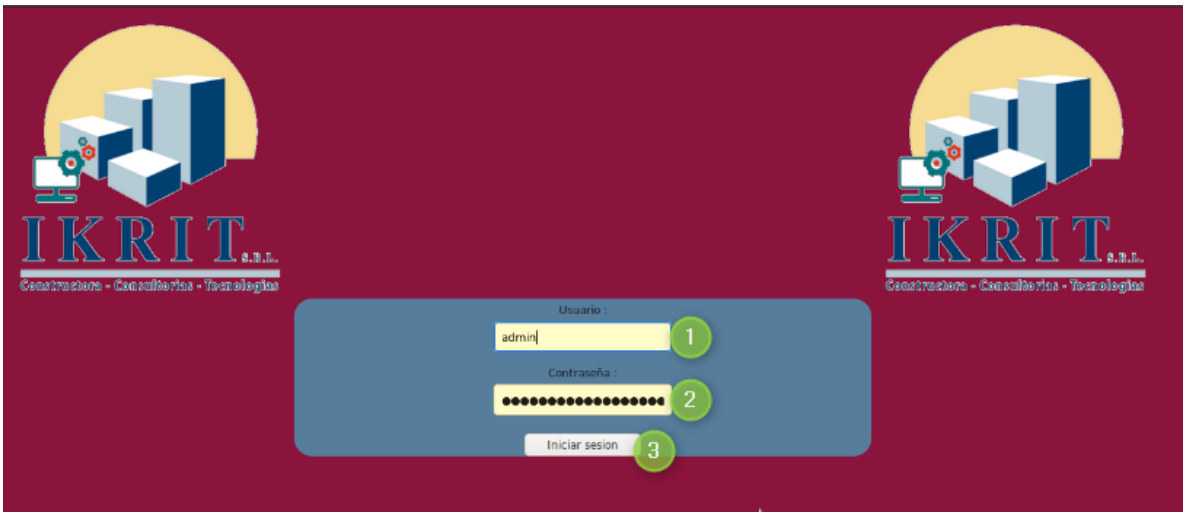
Atentamente.

M.Sc. Ing. Enrique Flores Baltazar
TUTOR METODOLOGICO TALLER II

Anexo D

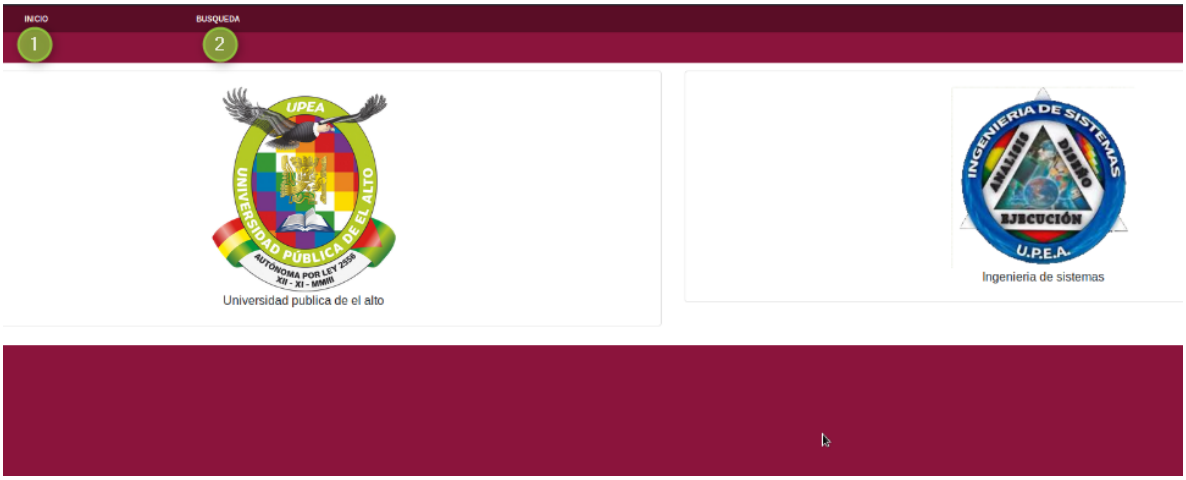
MANUAL DE USUARIO

Ingreso al Sistema



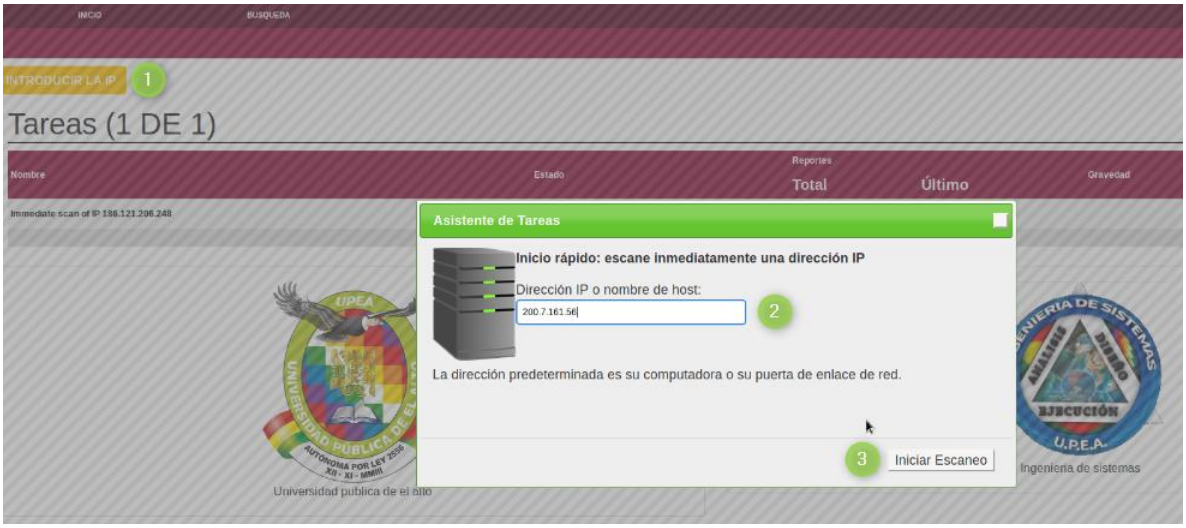
1. Ingresar nombre de usuario: admin
2. Ingresar la contraseña de usuario: 3c486541-0fca-4e67-9343-66d2c735184f
3. Iniciar sesión.

Si se ingresado los datos del usuario correctamente se ingresa a la pantalla principal siguiente:



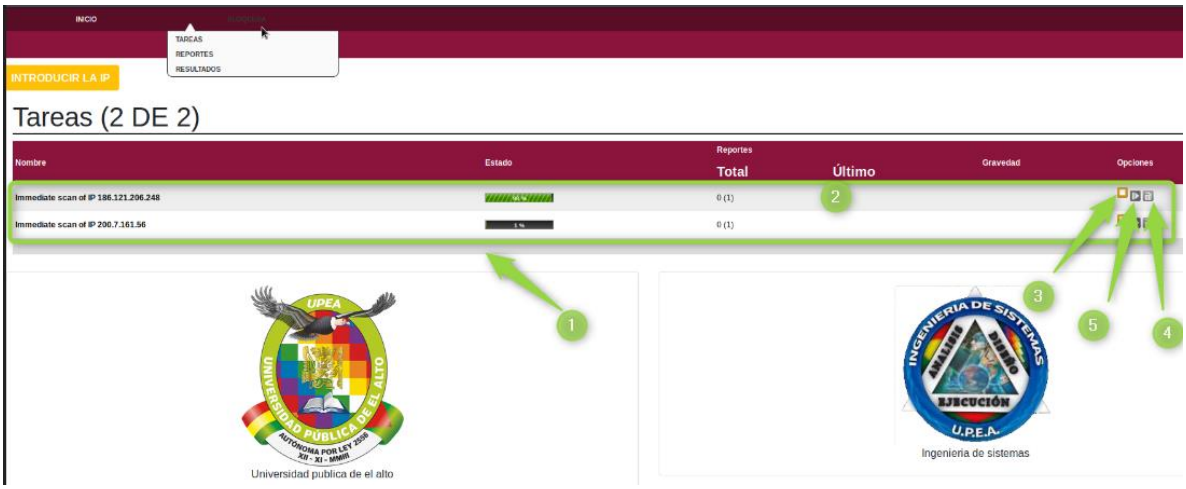
1. En esta opción se puede visualizar la pantalla principal.
2. En esta opción se puede ver los tareas, resultados y reportes.

La opción tareas



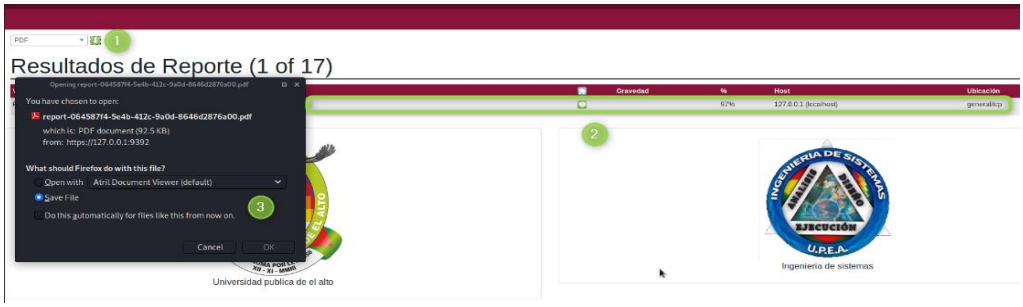
1. Para realizar una nueva tarea clic en el botón y aparecerá la venta siguiente opción 2.
2. En este campo se tiene que introducir la ip del servidor que se desea realizar el escaneo.
3. Una vez ingresado la ip del servidor clic en este botón para iniciar el escaneo correspondiente.

La opción para descargar el pdf:



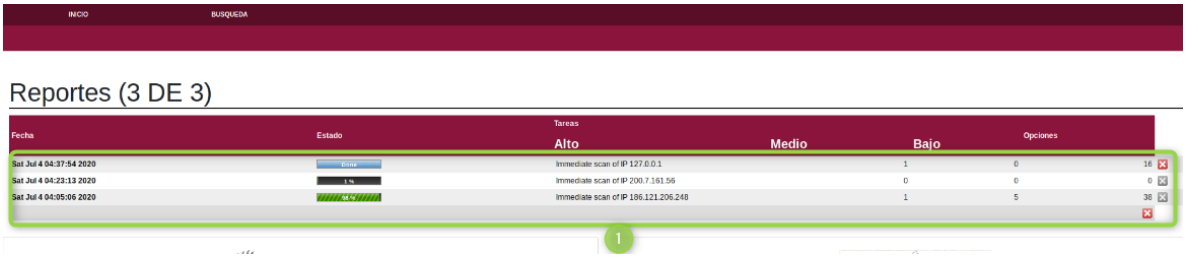
1. Listado de las tareas en ejecución.
2. Una vez terminado la búsqueda de vulnerabilidades aparece el botón para descargar el reporte.
3. Para la ejecución de la tarea seleccionada.
4. Para pausar y reanudar la ejecución seleccionada.
5. Elimina la búsqueda.

La opción resultados de reporte:



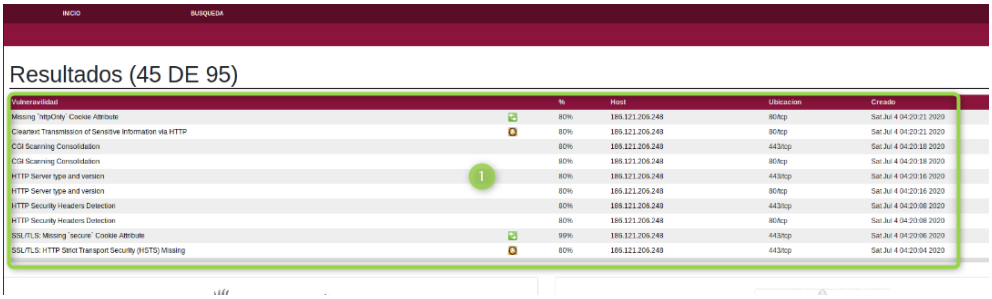
1. Se selecciona el formato PDF del informe y clic en botón.
2. Se visualiza los resultados de los escaneos una vez terminado la tarea correspondiente.
3. Una vez hecho clic en el botón opción 1 aparece la siguiente ventana donde se debe seleccionar Save File y posteriormente en la opción Ok para descargar el reporte.

Opción de estado de búsqueda



1. Se visualiza el estado y el porcentaje en que se encuentra el análisis de búsqueda de vulnerabilidades.

Opción de resultado



1. Se visualiza el listado de las tareas realizadas

Anexo E

Reporte

Reporte de Busqueda

July 8, 2020

Resumen

Este documento informa sobre los resultados de un análisis de seguridad automático. Todas las fechas se muestran usando la zona horaria Coordinated Universal Time , which is abbreviated UTC . La tarea era Immediate scan of IP 95.111.232.17 . El escaneo comenzó a las y terminó a las . los El informe primero resume los resultados encontrados. Luego, para cada host, El informe describe cada problema encontrado. Por favor considere el consejos dados en cada descripción, para recti car el problema.

Contents

Resumen de resultados

Host	High	Medium	Low	Log	Falso positivo
95.111.232.17 vmi381303.contaboserver.net	3	0	1	0	0
Total: 1	3	0	1	0	0

Las actualizaciones de seguridad del proveedor no son de con anza.
Las anulaciones están activadas. Cuando un resultado tiene una anulación, este informe utiliza la amenaza de la anulación.
La información sobre las anulaciones se incluye en el informe. Las

notas se incluyen en el informe.
Es posible que este informe no muestre detalles de todos los problemas encontrados. Solo enumera los hosts que produjeron problemas.
Problemas con el nivel de amenaza sesión No se muestran. Problemas con el nivel de amenaza Depurar No se muestran. Problemas con el nivel de amenaza Falso positivo No se muestran. Solo resultados con una QoD mínima de 70 are shown.

Este informe contiene todos 4 resultados seleccionados por el ltrado descrito anteriormente. Antes de ltrar había 108 resultados.

Resultados por Host

2.1 95.111.232.17

Inicio de escaneo de host Fin de escaneo del host

Servicio (Port)	Nivel de amenaza

2.1.4 High general/tcp

High (CVSS: 10.0) NVT: Report outdated / end-of-life Scan Engine / Environment (local)
Resumen This script checks and reports an outdated or end-of-life scan engine for the following environments: - Greenbone Source Edition (GSE) - Greenbone Community Edition (GCE) used for this scan.

NOTE: While this is not, in and of itself, a security vulnerability, a severity is reported to make you aware of a possible decreased scan coverage or missing detection of vulnerabilities on the target due to e.g.: - missing functionalities - missing bug xes - incompatibilities within the feed.
Resultado de detección de vulnerabilidad Installed GVM Libraries (gvm-libs) version: 9.0.3 Latest available GVM Libraries (gvm-libs) version: 10.0.2 Reference URL(s) for the latest available version: https://community.greenbone.n ,→et/t/gvm-11-stable-initial-release-2019-10-14/3674 /https://community.greenbo ,→ne.net/t/gvm-10-old-stable-initial-release-2019 04-05/208

Solución
Tipo de solución: VendorFix
Update to the latest available stable release for your scan environment. Please check the references for more information. If you're using packages provided by your Linux distribution please contact the maintainer of the used distribution / repository and request updated packages.
If you want to accept the risk of a possible decreased scan coverage or missing detection of vulnerabilities on the target you can set a global override for this script as described in the linked manuals.

Método de detección de vulnerabilidad
Detalles: Report outdated / end-of-life Scan Engine / Environment (local)
OID:1.3.6.1.4.1.25623.1.0.108560
Versión utilizada: 2020-06-10T13:24:20+0000

References
Other:
URL:https://www.greenbone.net/en/install_use_gce/
URL:https://community.greenbone.net/t/gvm-9-end-of-life-initial-release-2017-
,→03-07/211
URL:https://community.greenbone.net/t/gvm-10-old-stable-initial-release-2019-
,→04-05/208
URL:https://community.greenbone.net/t/gvm-11-stable-initial-release-2019-10-1
,→4/3674
URL:https://docs.greenbone.net/GSM-Manual/gos-4/en/reports.html#creating-an-o
,→verride
URL:https://docs.greenbone.net/GSM-Manual/gos-5/en/reports.html#creating-an-o
,→verride
URL:https://docs.greenbone.net/GSM-Manual/gos-6/en/reports.html#creating-an-o
,→verride

[return to 95.111.232.17]

2.1.5 High 8009/tcp

High (CVSS: 7.5)
NVT: Apache JServ Protocol (AJP) Public WAN (Internet) Accessible

Resumen
The script checks if the target host is running a service supporting the Apache JServ Protocol (AJP) accessible from a public WAN (Internet).

Resultado de detección de vulnerabilidad
La vulnerabilidad se detectó de acuerdo con el Método de detección de vulnerabilidad.

Solución
Tipo de solución: Mitigation
Only allow access to the AJP service from trusted sources / networks.

Perspectiva de vulnerabilidad

When using the Apache JServ Protocol (AJP), care must be taken when trusting incoming connections to Apache Tomcat. Tomcat treats AJP connections as having higher trust than, for example, a similar HTTP connection. If such connections are available to an attacker, they can be exploited in ways that may be surprising (e.g. bypassing security checks, bypassing user authentication among others).

Método de detección de vulnerabilidad

Evaluate if the target host is running a service supporting the Apache JServ Protocol (AJP) accessible from a public WAN (Internet).

Detalles: Apache JServ Protocol (AJP) Public WAN (Internet) Accessible

OID:1.3.6.1.4.1.25623.1.0.108716

Versión utilizada: 2020-03-02T11:38:26+0000

References

Other:

URL:https://lists.apache.org/thread.html/r7c6f492fbd39af34a68681dbbba0468490ff
,→1a97a1bd79c6a53610ef%40%3Cannounce.tomcat.apache.org%3E

High (CVSS: 7.5)

NVT: Apache Tomcat AJP RCE Vulnerability (Ghostcat)

Resumen

Apache Tomcat is prone to a remote code execution vulnerability (dubbed 'Ghostcat') in the AJP connector.

Resultado de detección de vulnerabilidad

It was possible to read the file "/WEB-INF/web.xml" through the AJP connector.

Result:

AB w È 200 =JSESSIONID=C5881012D154214E7E0BD7F778D3591A; Path=/; HttpOnly
,→ text/html;charset=ISO-8859-1 1227 AB Ï Ë<?xml version="1.0" encoding
,→="UTF-8"?>
<!--

```
 Licensed to the Apache Software Foundation (ASF) under one or more
  contributor license agreements.  See the NOTICE file distributed with
  this work for additional information regarding copyright ownership.
  The ASF licenses this file to You under the Apache License, Version 2.0
  (the "License"); you may not use this file except in compliance with
  the License.  You may obtain a copy of the License at
      http://www.apache.org/licenses/LICENSE-2.0
  Unless required by applicable law or agreed to in writing, software
  distributed under the License is distributed on an "AS IS" BASIS,
  WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
  See the License for the specific language governing permissions and
  limitations under the License.
-->
<web-app xmlns="http://xmlns.jcp.org/xml/ns/javaee"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://xmlns.jcp.org/xml/ns/javaee
                      http://xmlns.jcp.org/xml/ns/javaee/web-app_4_0.xsd"
  version="4.0"
  metadata-complete="true">
  <display-name>Welcome to Tomcat</display-name>
  <description>
     Welcome to Tomcat
  </description>
</web-app>
 AB
```

Solución

Tipo de solución: VendorFix

Update Apache Tomcat to version 7.0.100, 8.5.51, 9.0.31 or later. For other products using Tomcat please contact the vendor for more information on xed versions.

Software / SO afectado

Apache Tomcat versions prior 7.0.100, 8.5.51 or 9.0.31 when the AJP connector is enabled. Other products like JBoss or Wild y which are using Tomcat might be a ected as well.

Perspectiva de vulnerabilidad

Apache Tomcat server has a le containing vulnerability, which can be used by an attacker to read or include any les in all webapp directories on Tomcat, such as webapp con guration les or source code.

Método de detección de vulnerabilidad

Sends a crafted AJP request and checks the response.

Detalles: Apache Tomcat AJP RCE Vulnerability (Ghostcat)

OID:1.3.6.1.4.1.25623.1.0.143545

Versión utilizada: 2020-05-11T07:16:09+0000

References

```
CVE: CVE-2020-1938
Other:
  URL:https://lists.apache.org/thread.html/r7c6f492fbd39af34a68681dbbba0468490ff
,→1a97a1bd79c6a53610ef%40%3Cannounce.tomcat.apache.org%3E
    URL:https://www.chaitin.cn/en/ghostcat
    URL:https://www.cnvd.org.cn/flaw/show/CNVD-2020-10487
    URL:https://github.com/YDHCUI/CNVD-2020-10487-Tomcat-Ajp-lfi
    URL:https://securityboulevard.com/2020/02/patch-your-tomcat-and-jboss-instanc
,→es-to-protect-from-ghostcat-vulnerability-cve-2020-1938-and/
    URL:https://tomcat.apache.org/tomcat-7.0-doc/changelog.html
    URL:https://tomcat.apache.org/tomcat-8.5-doc/changelog.html
    URL:https://tomcat.apache.org/tomcat-9.0-doc/changelog.html
```

[return to 95.111.232.17]

2.1.6 Low general/tcp

Low (CVSS: 2.6) NVT: TCP timestamps
Resumen The remote host implements TCP timestamps and therefore allows to compute the uptime.
Resultado de detección de vulnerabilidad It was detected that the host implements RFC1323. The following timestamps were retrieved with a delay of 1 seconds in-between: Packet 1: 949406682 Packet 2: 949407027
Impacto A side e ect of this feature is that the uptime of the remote host can sometimes be computed.
Solución Tipo de solución: Mitigation To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime. To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled' Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled. The default behavior of the TCP/IP stack on this Systems is to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment. See the references for more information.
Software / SO afectado TCP/IPv4 implementations that implement RFC1323.
Perspectiva de vulnerabilidad The remote host implements TCP timestamps, as de ned by RFC1323.

Método de detección de vulnerabilidad
Special IP packets are forged and sent with a little delay in between to the target IP. The responses are searched for a timestamps. If found, the timestamps are reported.
Detalles: TCP timestamps
OID:1.3.6.1.4.1.25623.1.0.80091
Versión utilizada: 2020-03-21T13:23:23+0000

References
Other:
URL:http://www.ietf.org/rfc/rfc1323.txt
URL:http://www.microsoft.com/en-us/download/details.aspx?id=9152

[return to 95.111.232.17]

Muchas gracias