UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA

FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

CARRERA DE TECNOLOGÍAS DE LA INFORMACIÓN

MODALIDAD: EXAMEN COMPLEXIVO

Componente Práctico, previo a la obtención del Título de:

INGENIERO EN TECNOLOGÍAS

DE LA INFORMACIÓN

TEMA:

"ESTUDIO DE LA SEGURIDAD INFORMÁTICA A LOS SERVIDORES DE UNA COOPERATIVA DE TRANSPORTE DE LA PROVINCIA DE SANTA ELENA"

AUTOR:

BORBOR TOALA JOSEPH ANDRES

LA LIBERTAD – ECUADOR

PAO 2022-1

APROBACIÓN DEL TUTOR

En mi calidad de tutora del trabajo de componente práctico del examen de carácter complexivo: "ESTUDIO DE LA SEGURIDAD INFORMÁTICA DE UNA COOPERATIVA DE TRASPORTE DE LA PROVINCIA DE SANTA ELENA"., elaborado por el Sr. BORBOR TOALA JOSEPH ANDRES, de la carrera de Tecnología de la Información de la Universidad Estatal Península de Santa Elena, me permito declarar que luego de haber orientado, estudiado y revisado, la apruebo en todas sus partes.

La libertad, 27 de Julio del 2022.

Firmado electrónicamente por:
LIDICE
VICTORIA

Ing. Lídice Haz López, Msi.

DECLARACIÓN

El contenido del presente componente practico del examen de carácter complexivo es de mi responsabilidad; el patrimonio intelectual del mismo pertenece a la Universidad Estatal Península de Santa Elena.

Borbor Toala Joseph Andres

AGRADECIMIENTO

Agradezco en primer lugar a Dios, por permitirme llegar a esta parte de mi vida en donde estoy a punto de culminar y cumplir uno de mis grandes objetivos.

A mi familia por darme cada día los consejos y las fuerzas necesarias para seguir adelante y no rendirme durante este proceso.

Agradezco a la Universidad Estatal Península de Santa Elena por acogerme en sus aulas y darme la oportunidad de ser parte de la institución durante mis años de estudio. y mis distinguidos docentes por compartir conmigo sus enseñanzas y experiencias que me servirán de mucha ayuda en mi etapa de profesional, en especial a mi docente guía y a mi docente tutor de proyecto por ayudarme a cumplir con veracidad la documentación de la propuesta tecnológica.

Agradezco a mi grupo de amigos LA BANDITA que desde el pre universitario venimos luchando y apoyándonos mutuamente en cualquier situación que se nos presentaba, gracias por permitirme se parte de este leal y afectuoso grupo y estaré feliz verlos cumplir todas las metas propuestas.

Joseph Andres Borbor Toala

DEDICATORIA

Dedico este trabajo a Dios, así como todos mis logros, a mis padres por la confianza y el apoyo incondicional en cada decisión que he tomado para futuro, a mis hermanos y mi cuñada por los consejos y la paciencia que me han tenido en mis momentos de ausencia, a mi sobrina quien llegó hace cuatro años y es lo más preciado que tengo, por último, a mis amigos y amigas quienes me brindaron su sincera amistad formando un lazo importante para el resto de mi vida.

Joseph Andres Borbor Toala

TRIBUNAL DE GRADO

Ing. Jaime Orozco, Mgt

DIRECTOR DE LA CARRERA DE TECNOLOGÍAS DE LA INFORMACIÓN

Ing. Walter Orozco I, Mgt

DOCENTE ESPECIALISTA

Ing. Lidice Haz López, Msi

DOCENTE TUTOR

Ing. Marjorie Coronel, MgT

DOCENTE GUÍA UIC

RESUMEN

Esta propuesta tecnológica tiene como finalidad el estudio de la seguridad informática en los servidores de una cooperativa de transporte de la provincia de Santa Elena, ya que se considera uno de los activos de información más importantes para dicha empresa, este estudio se centra en la obtención de vulnerabilidades y busca contrarrestar los futuros riesgos a los que pueden estar sometidos a través de la propuesta de soluciones para poner fin a dichas vulnerabilidades.

Para el cumplimiento de cada objetivo se utilizó herramientas gratuitas quienes fueron seleccionada después de un análisis comparativo entre varias verificando así la más factible para el desarrollo del proyecto, además también se utilizó una herramienta de pago con ayuda de una licencia de prueba.

Se utilizó parte de las fases de la metodología OSSTMM y del hacking ético que permitieron un mejor desarrollo del proyecto, las fases que se utilizaron se resumieron en la recolección de información, el escaneo y enumeración, el análisis de vulnerabilidades y reporte.

TABLA DE CONTENIDOS

ÍNDICE DE FIGURAS

ITEM DESCRIPCIÓN PÁGINA

LISTA DE TABLAS

N.- DESCRIPCIÓN **PÁGINA**

LISTA DE ANEXOS

INTRODUCCIÓN

La seguridad informática es la disciplina basada en políticas y estándares internos y externos de una empresa u organización, se encarga de proteger la integridad y privacidad de la información, además de la propia seguridad de la misma, contra cualquier tipo de amenazas, reduciendo los riesgos tanto físicos como lógicos, a los que está expuesta [1]. La información que maneja algún aparato tecnológico es de gran importancia para los usuarios comunes o para empresas públicas y privadas por lo que se debe considerar de mayor importancia la seguridad informática de cualquier infraestructura tecnológica.

La empresa en donde se realizó la propuesta tecnológica maneja información confidencial e importante de usuarios dentro y fuera de la institución, como es una cooperativa de transporte la influencia de la información es mayor por lo que es importante la seguridad informática de los activos e infraestructura tecnológica. Este trabajo se centró en la infraestructura de servidores ya que se considera un activo importante de la organización, en ellos se ejecutan sistemas y servicios que ayudan al cumplimiento de los objetivos estratégicos además de la misión y visión de la empresa. Por ello se debe detectar con anticipación las vulnerabilidades informáticas que pongan en peligro estos recursos tecnológicos a través de un estudio que evidencie todos los problemas a los que están sujetos los ya nombrados activos de información.

En el primer capítulo se plantea la fundamentación en el que se incluye los antecedentes, descripción del proyecto, objetivos, justificación y alcance; el segundo capítulo contiene el marco conceptual en el que incluye los conceptos más importantes sobre seguridad informática y herramientas a ejecutar para el desarrollo, además está el marco teórico con las teorías y estudios referente al tema del proyecto; el tercer capítulo contiene la propuesta del proyecto con el desarrollo de las fases de la metodología en la que se evidencia las pruebas de la ejecución de las herramientas como de los resultados obtenidos y por último las posibles soluciones a las vulnerabilidades obtenidas.

CAPÍTULO I

1.1 ANTECEDENTES

Hoy en día se convive con un manejo masivo de información, que cada día está más interconectado a todos los niveles productivos, financieros y de salud en la sociedad actual. Esto seguirá incrementándose por todas las ventajas que se ofrece a cada sector de la sociedad; pero es muy claro también que todas estas ventajas de intercambio y manejo de información masivo no son más importantes que el mejorar el manejo de los riesgos y enfocarnos en la continuidad de los negocios contra los ataques informáticos que, en la actualidad, son cada vez más frecuentes a nivel global. De aquí la importancia de la seguridad consiste en prever la ocurrencia de un ataque informático, en el monitoreo de la información y sistemas críticos, y la protección de la información que es el activo más importante en una organización [2].

El último informe presentado por Security Report Latinoamérica (ESET) en el 2020, indica que la infección con códigos maliciosos sigue siendo la mayor preocupación en materia de seguridad de la información para las empresas Latinoamericanas. Este tipo de ataque suele ser más rentables para los atacantes quienes también usas otros métodos para evadir la seguridad de la información en las empresas. [3]

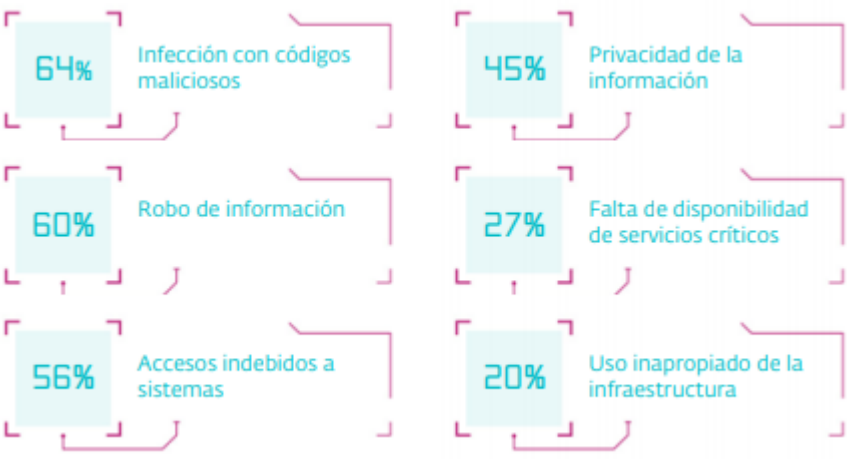


Figura 1. Preocupaciones de seguridad en empresas Latinoamericanas [3].

Las empresas ecuatorianas no suelen invertir en recursos humanos y tecnológicos para mejor la seguridad de información, por ello, sufren varios incidentes que les ha

significado enormes pérdidas por no estar preparadas para afrontar ataques cibernéticos. En la actualidad, Ecuador se encuentra en el puesto 36 a escala mundial de ataques cibernéticos según la compañía Kaspersky. [4]

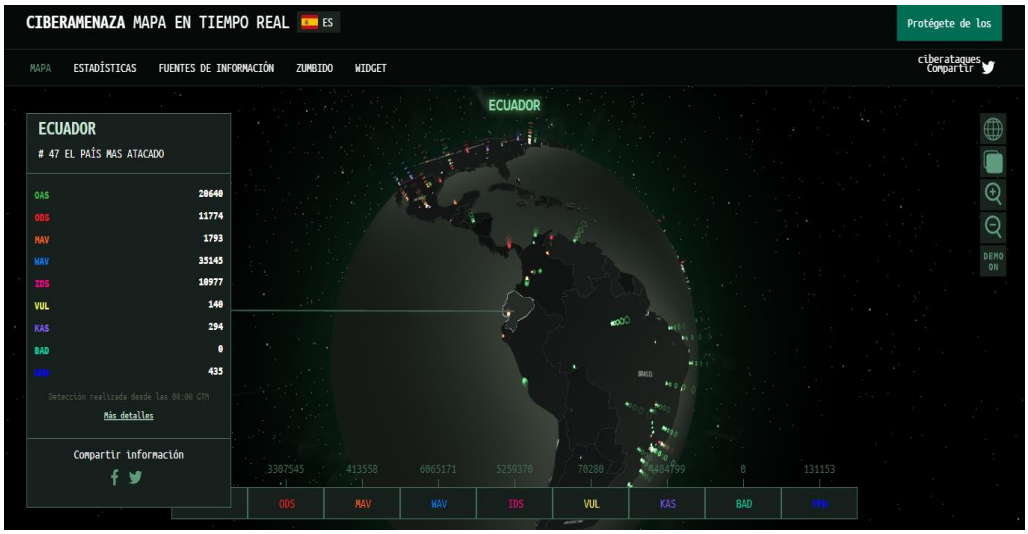


Figura 2. Kaspersky - Monitoreo en tiempo de real de ataques hacia Ecuador [4].

La cooperativa de transporte se encuentra en un constante desarrollo e innovación de servicios para brindar mejores experiencias de viajes a los usuarios del transporte terrestre para cada provincia en donde está presente la institución, promueve el progreso sostenido y sustentable, económico y productivo de la sociedad. Para el cumplimiento de los objetivos la cooperativa ha desarrollado mejoramiento de servicios, proporcionando una mejor atención al cliente, ofrece calidad, eficiencia, responsabilidad, honestidad y transparencia tanto en los medios de transporte como en el trato con el cliente [5].

Los habitantes del cantón hacen uso del servicio que ofrece la cooperativa a diario debido a los diferentes recorridos que ofrece, siendo su matriz la de mayor importancia por la gran información almacenada los servidores. Se presentan problemas en la seguridad informática de estos activos, detentando accesos indebidos a los sistemas, accesos remotos no autorizados y perdida de información, por ello, se han presentado problemas con la eficacia y disponibilidad de los servicios

Para el levantamiento de información de forma general se procederá hacer una entrevista (Anexo1) al director o encargado del departamento de TI para así evidenciar posibles vulnerabilidades y amenazas que lleguen a existir en los servidores de la cooperativa.

En un trabajo de investigación de Perú trata sobre los mecanismos para contrarrestar ataques en servidores web y base de datos se identificó los incidentes de seguridad de la información, encontrando entre ellos a los ataques informáticos con mayor impacto en servidores. Estos fueron analizados y posteriormente se implementó sus mecanismos de seguridad en el diseño de la red establecida. Se implementaron los mecanismos de seguridad, establecidos por los investigadores, el primer mecanismo constó con la clonación de una red espejo virtual (Honeynet) autocontenida, así mismo se implementó el segundo mecanismo Snort en Kali Linux [6].

El análisis de vulnerabilidades en este proyecto de tesis está aplicado a una empresa comercializadora de prendas de vestir y tiene como objetivo realizar un estudio para determinar los puntos vulnerables y grados de acceso que tendría un atacante en la organización, así como incidentes que involucren la fuga o perdida de información que pueden ser accidentales o provocados, siendo esto de vital importancia para la continuidad de los servicios que presta la empresa. Con los resultados obtenidos de este análisis podremos establecer medidas de seguridad que nos permitan minimizar riesgos en la operatividad de la organización evitando así la fuga de información sensible lo que puede desencadenar en daños incalculables [7].

A nivel local existe un trabajo que está basado en detectar amenazas, vulnerabilidades, que se encuentran en los activos de información, ya que la clínica no cuenta con un control de seguridad informática antes ataques de cibernéticos, y esto puede generar perdida de información importante como historias clínicas, citas, tratamiento por paciente. Se propone elaborar un plan de seguridad informático alineado con los controles de normativa ISO 27002, para conocer el estado organizacional respecto a la seguridad informática, nos apoyamos en la herramienta informática Kali Linux con herramientas de análisis de vulnerabilidades NMAP, NIKTO, OWASP y aplicamos el estándar ISO para el control de posibles riesgos [8].

Cada uno de los trabajos citados anteriormente buscan detectar vulnerabilidades y amenazas en servidores de diferentes empresas haciendo uso de varias herramientas y software. Los peligros que hoy en día están expuestos las organizaciones hacen evidente la preocupación de dueños y profesionales en esta área que buscan protegerse y tener una mejor visión de los riesgos y obtener una mirada más amplia con respecto al estado de

seguridad de datos y posteriormente proponer un tratamiento suficiente para disminuir los riesgos a niveles dignos para la organización.

Con todo lo antes expuesto es necesario realizar con más frecuencia un estudio de seguridad informática a servidores quienes manejan mucha información para detecta así vulnerabilidades y amenazas que pueden afectar incluso todos los procesos de la organización. Dentro de la institución existen diversos procesos y servicios que corren peligro de ser afectados si no se detecta aquellos filtros que permitan el ingreso de virus e intrusos por ello haciendo uso de la metodología OSSTMM se podrá saber la eficiencia de la seguridad informática en la infraestructura de servidores en el departamento de TI.

1.2 DESCRIPCIÓN DEL PROYECTO

En la cooperativa de transporte se emplean varios procesos y servicios a beneficios tanto de los empleados de la institución como de la ciudadanía, se evidencia diversos datos e información manejados y almacenados en los servidores para mayor eficacia y organización. Esta información es vulnerable si se exponen a ataques de usuarios mal intencionados quienes podrían alterar datos y tomar el control de los servicios, afectando así a otros usuarios, por lo tanto, es fundamental realizar un análisis de seguridad informática a los servidores y así evitar posibles ataques.

La técnica de Caja Blanca se ejecutará con el respectivo permiso de la cooperativa con el fin de tener acceso a la infraestructura de servidores, por ello, esta técnica la más completa y forma parte integral del estudio. A través de un punto de red con direccionamiento IP válida se obtendrá información relevante acerca del objeto de estudio, así simularemos ser un usuario más de la empresa y tener mayor facilidad a la hora de ejecutar herramientas de análisis y seguridad informática.

El presente trabajo busca un análisis correcto de vulnerabilidades en los servidores por ello la estructura de este proyecto es hibrida entre las fases de Ethical Hacking y la metodología OSSTMM, obteniendo principalmente las siguientes fases:

1.2.1 Fase de inducción - Recolección de información

Para esta primera fase se procede a recolectar toda la información sobre las posibles vulnerabilidades o peligros que existan en los servidores de la cooperativa de transporte.

Para ello se utilizará Caja Blanca como técnica esencial para el desarrollo del proyecto, este proceso nos permitirá obtener una visión más amplia de los diferentes mecanismos de seguridad que existan, siendo toda la información recolectada puntos clave para el desarrollo del proyecto. La información a obtener será encontrada a través de la ejecución de técnicas y herramientas como:

- Comparación de las diferentes herramientas de testeo.
- Selección entre todas las herramientas las más adecuadas al proyecto.
- Ejecución y utilización de las herramientas para la obtención de información del objetivo planteado.
- Identificación de servidores con sus respectivas características, estado y utilidad.

1.2.2 Fase de Interacción - Scanning y enumeración

En esta fase estableceremos un horario adecuado para no poner en peligros los procesos que se ejecutan en la Cooperativa de Transporte y así obtener el alcance de las pruebas de desarrollar, por ello, hará uso de herramientas de testeo, se planificará el proceso de identificación de vulnerabilidades para ello se realizará:

- Con el permiso necesario se procede al uso de herramientas de testeo Open Source de forma eficaz.
- Verificación de softwares que contienen y servicios que prestan a través del uso y eficiencia.
- Verificación de la visibilidad de los objetos propensos a ataques cibernéticos.
- La información a recolectar se obtendrá por medio de las herramientas de escaneo ya valoradas anteriormente.
- Instalación y ejecución de herramienta para la obtención de vulnerabilidades para cada servidor.
- Se procede a enumerar las vulnerabilidades encontradas en otro cuadro comparativo para cada servidor.

1.2.3 Fase de Investigación - Análisis de vulnerabilidades

Se evaluarán todos los procesos y resultados obtenidos de la fase anterior, se procede a realizar el respectivo análisis y se lista las vulnerabilidades encontradas dentro de

plantillas o tablas comparativas. Este proceso se lo realizara para cada uno de los servidores que se encuentren en el departamento de TI. Obteniendo lo siguiente:

- Identificación los falsos positivos y falsos negativos.
- Clasificación de los resultados obtenidos dependiendo el nivel de riesgo y tipo de vulnerabilidad encontrada.
- Verificación de la totalidad de amenazas, estás deben ser igual al registradas con el uso de las herramientas.
- Determinar el alcance del daño que se puede obtener en cada vulnerabilidad encontrada.
- Demostración de los peligros y asignar responsabilidades al departamento de TI.
- Dadas las vulnerabilidades se comenzará en la búsqueda de las posibles soluciones, esto dependerá de los resultados obtenidos en fases anteriores.

1.2.4 Fase de Reporte

Una vez cumplida las fases anteriores, se procede a documentar en un informe todo el proceso realizado y los resultados obtenidos, dicho informe será dirigido al director del departamento de Tecnologías de la Información de la Cooperativa de Transporte. En el informe se manejará la siguiente información:

- Resumen técnico sobre el proceso empleado para la detención, procesamiento y análisis de vulnerabilidades.
- Registro de fecha y hora en el que se realiza cada testeo.
- La totalidad de amenazas encontradas en forma de lista.
- Información estadística permitiendo la comparación de las vulnerabilidades entre servidores.
- Se establecerán medidas preventivas brindando el correcto control y protección a los servidores de la Cooperativa de Transporte.

Las herramientas que se utilizaran para el desarrollo de este proyecto son:

Kali Linux: es una distribución de Linux de código abierto basada en Debian orientada a diversas tareas de seguridad de la información, como pruebas de penetración, investigación de seguridad, informática forense e ingeniería inversa [9].

Nmap: es un código abierto y gratuito (licencia) utilidad para el descubrimiento de redes y la auditoría de seguridad [10].

Dmitry: es una aplicación de línea de comandos UNIX / GNU LINUX codificada en C. Tiene la capacidad de recopilar tanta información como sea posible sobre un host. Se utiliza para recopilar posibles subdominios, direcciones de correo electrónico, información de tiempo de actividad y escaneo de puertos [11].

Metasploit: es un proyecto de código abierto que nos ayuda a investigar las vulnerabilidades de seguridad siendo 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 [12].

Nexpose: es un software creado y mantenido por la compañía RAPID7, que permite detectar y evaluar las vulnerabilidades que existen dentro de una infraestructura de red; el software Nexpose se instala "on-premise" es decir, en las instalaciones de la compañía que lo adquiere [13].

Este proyecto contribuirá a la línea de investigación relacionada con temas de Tecnología y Sistemas de la Información (TSI) asociadas a las empresas u organizaciones a nivel nacional, además se rige a la sub línea de investigación sobre Ingeniería y gestión de Tecnologías y Sistemas de la Información con la finalidad de dar soporte y seguridad en tiempo real a las empresas que lo requieran [14].

1.3 OBJETIVOS DEL PROYECTO

1.3.1 Objetivo General

- Identificar las vulnerabilidades de los servidores del departamento de TI de la Cooperativa de Transporte, mediante el uso de la metodología OSSTMM y herramientas de análisis de seguridad, con la finalidad de mejorar la seguridad informática de la organización.

1.3.2 Objetivo Específicos

- Comparar las diferentes herramientas de análisis de seguridad para efectuar escaneos en los servidores del departamento de TI.
- Identificar las amenazas más críticas que existan en los servidores a través de la ejecución de herramientas y métodos de seguridad.
- Documentar el proceso y resultados obtenidos en el escaneo de vulnerabilidades y la incidencia de inseguridad de la información en los servidores de la Cooperativa para evidenciar los peligros y amenazas.
- Proponer soluciones a las vulnerabilidades y amenazas encontrados en el análisis de seguridad para salvaguardar la información en los servidores.

1.4 JUSTIFICACIÓN

En la actualidad todas las instituciones públicas logran adaptarse a los cambios tecnológicos, por ello, las Tecnologías de la Información y Comunicación son herramientas imprescindibles para el cumplimiento de la gestión institucional e interinstitucional de la Administración Pública en tal virtud, deben cumplir con estándares de seguridad que garanticen la confidencialidad, integridad y disponibilidad de la información. [15]

La seguridad de la información es de suma importancia debido a que desarrollo de las tecnologías que van cambiando el manejo de actividades diarias por parte de instituciones públicas. El querer disminuir los procesos y mejorar la eficiencia trae consigo la actualización de infraestructura tecnológica, con llevando a la aparición de varias amenazas para los sistemas de información.

Las Cooperativas de Transportes son instituciones que se relacionan directamente con la ciudadanía por lo que están sujetas a peligros y ataques cibernéticos poniendo en riesgo la seguridad e integridad de estos, por ello, se debe garantizar la seguridad y el manejo de todo dato e información dentro de la institución.

El estudio de seguridad informática a los servidores de la cooperativa evidenciara los problemas o desafíos en las que podrían estar involucrada dicha institución. Actualmente el departamento de TI cuenta con algunas normativas de seguridad pero que en ciertos

casos han demostrado no ser suficientes para mantener la seguridad poniendo en peligro los procesos que se manejan en los servidores, por ello, se realizará un análisis de vulnerabilidades a los servidores mediante herramientas de testeo y de una metodología hibrida eficiente que lleve al cumplimiento de los objetivos establecidos anteriormente.

En la detección de estas vulnerabilidades se evidenciará los peligros en los que se encuentran los bines y servicios de la institución afectando directamente a todo proceso y actividad que trabajadores y clientes (ciudadanía) efectúen a diario dentro y fuera del municipio.

Los resultados del estudio se los evidenciarán en un informe y que al mismo tiempo se podrá recomendar posibles soluciones que corrijan o disminuyan las vulnerabilidades encontradas, garantizando una guía efectiva para miembros del departamento de TI, además de facilitar a las posibles auditorias informáticas por parte de la Cooperativa.

El tema propuesto está alineado a los objetivos del Plan de Creación de Oportunidades específicamente al siguiente eje:

Eje 2: Eje Social

Objetivo 5: Proteger a las familias, garantizar sus derechos y servicios, erradicar la pobreza y proveer la inclusión social [16].

> **Política 5.5:** Mejorar la conectividad digital y el acceso a nuevas tecnologías de la población [16].

Objetivo 7: Potenciar las capacidades de la ciudadanía y promover una educación innovadora, inclusiva y de calidad en todos los niveles [16].

> **Lineamiento Territoriales**
>
> **Pol.7.4 - G8.** Generar redes de conocimiento vinculadas a la educación superior, que promuevan espacios territoriales de innovación adaptados a las necesidades de la sociedad y el sector productivo local [16].

1.5 ALCANCE DEL PROYECTO

La implementación de un estudio de seguridad informática en el departamento de TI de la Cooperativa, permitirá la detección de vulnerabilidades y amenazas que puedan poner en peligro a los servidores. Se realizará un estudio completo que incluye información confidencial de los servidores tales como rango de direcciones, dominios, subdominios, nombre de servidores, puertos abiertos, servicios que ejecutan, con el fin de establecer conclusiones precisas, adecuadas y acorde al problema encontrado.

Para su desarrollo se utilizarán herramientas de testeo Open Source buscando así una mejor efectividad para el análisis de las vulnerabilidades por ello se implementará un análisis comparativo de cada herramienta a utilizar.

El presente proyecto abarcará las siguientes fases:

- Fase de inducción - Recolección de información

En esta primera fase es fundamental el manejo de información veraz y acertada, por ello, los métodos utilizados en la recolección de información serán ejecutados efectivamente y las herramientas pasaran por comparaciones entre ellas para determinar cuál es la más eficiente en el desarrollo del proyecto. La técnica principal a utilizar es la técnica de Caja Blanca, permitiendo el acceso directo al objeto de estudio, aumentando la veracidad de los resultados y un eficaz desarrollo de cada una de las fases, además se identificarán los activos de información que son servidores de la institución.

- Fase de Interacción - Scanning y enumeración

Se ejecutarán las herramientas Open Source a utilizar en cada servidor para saber características y servicios que ofrecen, además de la utilización de comandos para encontrar vulnerabilidades y amenazas informáticas verificando las posibles brechas de seguridad identificadas en los servidores. Se procede a enumerar las vulnerabilidades encontradas en cada servidor y las evidencias necesarias a través de capturas de pantalla.

- Fase de Investigación - Análisis de vulnerabilidades

Ya obtenidos los resultados en la fase anterior, se organizarán las vulnerabilidades encontradas por nivel de riesgo, nombre, descripción y lugar, esta información ira dentro de una tabla comparativa. El análisis de vulnerabilidades permitirá dar recomendaciones

a los problemas o amenazas encontradas en la fase anterior, cabe recalcar que las recomendaciones dadas no serán ejecutadas si no presentadas dentro de informe en la fase siguiente.

- Fase de Reporte

Los resultados de esta detección de vulnerabilidades serán presentados a través de reportes técnicos al director y miembros del departamento de TI conllevando a la toma de decisiones de los sistemas de información.

No será posible la demostración en tiempo real de las vulnerabilidades de los servidores, debido a que son equipos que prestan servicios actualmente y es recomendable no realizar ningún tipo de ataque. Cabe indicar que el proyecto a realizar no está direccionado a crear softwares o sistemas para contrarrestar las vulnerabilidades en los servidores ni la implementación de ningún control, sin embargo, se detallaran varias recomendaciones a cada problema encontrado.

CAPITULO II

2.1 MARCO CONCEPTUAL

2.1.1 Seguridad Informática

Es el proceso de prevenir y detectar el uso no autorizado de un sistema informático e incluye el proceso de protección contra piratas informáticos que utilizan nuestros recursos informáticos con fines maliciosos o lucrativos, o incluso la capacidad de acceder a ellos a través de Crash; además incluye una serie de medidas de seguridad, como software antivirus, firewalls, y otras medidas que dependen del usuario, como habilitar o deshabilitar la funcionalidad de ciertos programas, como Java y scripts ActiveX que soportan el uso de computadoras, redes o recursos de Internet [17].

2.1.2 Vulnerabilidad Informática

Es aquel fallo de diseño de procedimiento o de recursos que permite que una amenaza pueda afectar a un recurso, por lo general se da en sistemas informáticos ineficientes que aún no han sido actualizados o están mal configurados permitiendo que agentes externos

accedan sin permisos apropiados al recurso o información que dicho sistema gestiona [18].

2.1.3 Herramienta de análisis

El uso de herramientas eficaces para la obtención de información y a su vez el análisis de vulnerabilidades es de gran importancia para salvaguardar la seguridad informática en equipos tecnológicos, entre las herramientas a utilizar tenemos:

Nmap

De acuerdo con lo descrito en [24] Nmap es una fuente gratuita y código abierto de gran utilidad para el descubrimiento de redes y la auditoría de seguridad. Entre sus características se encuentran las siguientes:

- Flexible: Admite docenas de técnicas avanzadas para mapear redes llenas de filtros IP, firewalls, enrutadores y otros obstáculos [19].
- Potente: Nmap es utilizado para escanear redes enormes de literalmente cientos de miles de máquinas [19].
- Portátil: La mayoría de los sistemas operativos son compatibles [19].
- Gratis: Los objetivos principales del Proyecto Nmap son ayudar a que Internet sea un poco más seguro y proporcionar a los administradores/auditores/hackers una herramienta avanzada para explorar sus redes [19].
- Compatible: Cuenta con el respaldo de una comunidad dinámica de desarrolladores y usuarios [19].

Dmitry

Es una aplicación de línea de comandos de UNIX/(GNU)Linux escrita en C. DMitry puede encontrar posibles subdominios, direcciones de correo electrónico, información de tiempo de actividad, realizar escaneos de puertos tcp, búsquedas whois y más [20].

Kali Linux

Kali Linux es una distribución de Linux de código abierto basada en Debian orientada a diversas tareas de seguridad de la información, como pruebas de penetración, investigación de seguridad, informática forense e ingeniería inversa [21].

Metasploit

Ayuda a los equipos de seguridad a hacer más que solo verificar vulnerabilidades, administrar evaluaciones de seguridad y mejorar la conciencia de seguridad; empodera y arma a los defensores para estar siempre un paso (o dos) por delante del juego [22].

Nexpose

Permite el análisis constante del entorno en busca de vulnerabilidades recientemente descubiertas, indicando prioridad en relación con lo que debe tratarse en función de la criticidad de la vulnerabilidad, además de tener el enfoque que necesita la empresa, ya que, al ser administrada por el responsable de la seguridad de la misma, quien interactúa constantemente con el ambiente, este puede definir en qué entorno se realizarán más pruebas [23].

2.2 MARCO TEÓRICO

2.2.1 Seguridad Informática en las Pymes

De acuerdo con el estudio realizado por Kaspersky Lab, en los últimos 12 meses más de un tercio de los negocios, es decir el 38% han sido afectados por virus y malware causando gran pérdida en la productividad, el 36% se da por el uso inapropiado de recursos por parte de los empleados, de igual manera, uno de cada 5, es decir el 21% han experimentado pérdida de información debido a los ataques de los cuales han sido víctimas; se considera que este tipo de sector se ha convertido en un blanco fácil de ciberataques dada la poca seguridad que dichas organizaciones implementan sobre sus infraestructuras o aplicaciones, se contemplan a continuación algunos de los ataques o eventos más comunes dirigidos a este tipo de organizaciones y su posible mitigación [24].

- **Phishing:** Es uno de los ataques más comunes en las pymes, básicamente este tipo de ataque se da cuando el ciberdelincuente falsifica la página de una de estas organizaciones para que usuarios al momento de ingresar a la plataforma entreguen sus credenciales de acceso y posteriormente hacer de las suyas con la información recolectada [24].

- **Malware:** El ataque por medio de malware consiste en infectar directamente la máquina o equipo de un usuario dentro de la misma organización, en su mayoría las infecciones se dan con la ejecución de códigos maliciosos, los cuales pretenden robar información [24].
- **Ingeniería Social:** Es usada como el inicio de una cadena de ataques dirigidos a determinado tipo de organizaciones cuyo propósito inicial es el de obtener información clave de las mismas y posteriormente llegar a ejecutar un ataque más estructurado [24].

2.2.2 Importancia del análisis de vulnerabilidades en la infraestructura tecnológica

El análisis de vulnerabilidades se puede utilizar para evaluar posibles vulnerabilidades de seguridad en la infraestructura de TI de una organización que un atacante podría aprovechar. Esto incluye escanear computadoras, redes internas y externas y equipos de telecomunicaciones. Escanea varios objetivos de infraestructura en busca de vulnerabilidades conocidas y configuraciones incorrectas; como resultado del análisis, se genera un informe bastante útil que te ayudará a identificar y reforzar los puntos débiles de seguridad [25].

2.2.2.1 Fases del análisis de vulnerabilidades

- **Descubrimiento**: Este primer paso recopila toda la información relacionada con los activos protegidos y la infraestructura de TI asociada, esto le dará una mejor comprensión de su entorno y le ayudará a determinar el mejor método de análisis [25].
- **Identificación de vulnerabilidades:** Se puede usar las herramientas y los métodos adecuados para escanear e identificar vulnerabilidades en activos previamente identificados, de modo que pueda realizar escaneos con o sin credenciales, según lo que desee lograr [25].
- **Evaluación:** Llegado este momento ya se han identificado todas las posibles vulnerabilidades, por lo que ahora deben evaluarse y clasificarse de acuerdo con el nivel de riesgo que suponen para los activos y la organización [25].

- **Elaboración de informe y remediación:** Finalmente, el experto en ciberseguridad genera un informe en el que se describen las vulnerabilidades, sus causas y una serie de recomendaciones para mitigarlas [25].

2.2.2.2 Modalidades de Hacking Ético

Hacking de Caja Negra: Este modo se aplica a las pruebas de penetración externa. Se llama porque el cliente solo le presenta al consultor el nombre de la empresa a auditar para que trabaje a ciegas, y la infraestructura de la organización es la caja negra para él. Este tipo de piratería ética es más práctico, ya que los atacantes que eligen a una empresa como víctima generalmente no tienen más información que el nombre de la organización que fue atacada [26].

Hacking de Caja Blanca: Se aplica únicamente a las pruebas de penetración interna, se llama así porque la empresa proporciona al hacker información completa sobre la red y su sistema para ser probado, además de brindarle acceso a la información de configuración de la red y del dispositivo, al igual que en una prueba de caja gris, el verificador obtiene información adicional como gráficos de red, listas de dispositivos; debe verificar, incluido el nombre, la plataforma, los servicios proporcionados, la dirección IP y la información de la subred remota y más [26].

Hacking de Caja Gris: Es utilizado para pruebas de penetración interna, algunos evaluadores también lo definen como una prueba externa en la que un cliente proporciona información limitada sobre los elementos generales de la red que se evalúan, cuando se trata de pruebas internas, se conocen como cajas grises porque el auditor solo tiene acceso si un empleado de la empresa tiene los mismos privilegios que él [26].

2.2.3 Amenazas y vulnerabilidades informática más comunes encontradas en servidores empresariales

2.2.3.1 Amenazas de Malware

Los programas maliciosos son una de las mayores ciberamenazas a las que están subjetas las empresas. Dentro del malware existen distintos tipos de amenazas, siendo las principales.

- Virus: Los virus informáticos son un software que se instalan en un dispositivo con el objetivo de ocasionar problemas en su funcionamiento; para que un virus infecte un sistema es necesaria la intervención de un usuario (intencionada o inintencionadamente) [27].
- Gusanos: Es uno de los malware más comunes que infectan los equipos y sistemas de una empresa, ya que no requieren de la intervención del usuario ni de la modificación de algún archivo para poder infectar un equipo. El objetivo de los gusanos es el de replicarse e infectar el mayor número de dispositivos posibles utilizando la red para ello. Son una amenaza para las redes empresariales, porque un solo equipo infectado puede hacer que la red entera se vea afectada en un espacio corto de tiempo [27].
- Troyanos: Los troyanos son programas que se instalan en un equipo y pasan desapercibidos para el usuario siendo su objetivo el de ir abriendo puertas para que otro tipo de software malicioso se instale [27].
- Ransomware: El ransomware se ha convertido en el malware más temido en la actualidad por las empresas. Consiste en encriptar toda la información de la empresa, impidiendo el acceso a los datos y los sistemas y se pide un rescate para poder liberar la información (normalmente en criptomonedas como bitcoins) [27].
- Keyloggers: Se instalan a través de troyanos y se encargan de robar datos de acceso a plataformas web, sitios bancarios y similares [27].

2.2.3.2 Vulnerabilidades del sistema

Los sistemas y aplicaciones informáticos siempre tienen algún error en su diseño, estructura o código que genera alguna vulnerabilidad. Por muy pequeño que sea ese error,

siempre podrá generar una amenaza sobre los sistemas y la información, siendo la puerta de entrada para recibir ataques externos o internos [27].

2.2.3.3 Amenazas de ataques de denegación de servicio

Un ataque de denegación de servicio distribuido (DDoS) se produce cuando un servidor recibe muchas peticiones de acceso, sobrecargando el sistema y haciendo que el servidor caiga o funcione de forma incorrecta (acceso lento o rebotando mensajes de errores). Para realizar este tipo de ataques se utilizan muchos ordenadores (bots) que de forma automatizada hacen peticiones a ese servidor [27].

2.2.3.4 Vulnerabilidades producidas por contraseñas

Con el teletrabajo y la computación en la nube la gestión de contraseñas se ha convertido en uno de los elementos más importantes de la ciberseguridad ya que se utiliza un usuario y contraseña para acceder a la plataforma, sin embargo, el uso de una contraseña débil crea una vulnerabilidad del sistema dando la oportunidad a que una tercera persona fácilmente pueda robar, cambiar o eliminar información, vulnerar configuraciones si tiene los permisos adecuados o apagar su computadora si su contraseña se descifra fácilmente; la generación de contraseñas seguras es una de las claves para incrementar el nivel de ciberseguridad de las empresas [27].

2.2.3.5 Vulnerabilidades producidas por usuarios

El error humano es otra causa de riesgos en ciberseguridad. El usuario siempre tiene el riesgo de cometer un error que pueda generar una vulnerabilidad que suponga una amenaza informática. Por eso en ciberseguridad se tiende a automatizar procesos críticos para minimizar o eliminar el factor de riesgo del error humano. Las prácticas fraudulentas y la falta de capacitación en seguridad cibernética también pueden generar vulnerabilidades, como abrir archivos de fuentes sospechosas, hacer trampa con anuncios falsos y abrir correos electrónicos maliciosos. Estas acciones son una amenaza a sufrir ataques como el phishing (suplantación de identidad) o similares [27].

2.3 METODOLOGÍA

2.3.1 Metodología de la Investigación

2.3.1.1 Metodología de la investigación diagnóstica

La metodología de investigación diagnostica es la interpretación de una realidad, por ello expresa y explica las características de su funcionamiento y evolución. Esta interpretación aporta suficientes elementos y antecedentes para definir líneas y estrategias de acción [28]. Se utilizará esta metodología de investigación a través de entrevista al director del departamento de TI sobre temas relacionados a la seguridad de la información e implementación de técnicas y herramientas de seguridad. Con esta información se analizará el estudio de seguridad informática a los servidores.

Variable

- Identificación de riesgos y vulnerabilidades existente en los servidores de la Cooperativa de Trasporte.

2.3.1.2 Metodología de la investigación exploratoria

La metodología investigación exploratoria tiene por objeto definir o clarificar conceptos, conocer el problema con mayor profundidad y generar hipótesis o propuestas explicativas relacionadas con el fenómeno objeto de estudio [29]. Esta metodología de investigación se cumple en este proyecto bajo la revisión bibliográfica de proyectos similares a nivel local, nacional e internacional, dichos proyectos servirán de comparación con el proyecto a realizar. Por ello, es indiscutible el desarrollo de este tipo de investigación ya que son pocos los estudios de seguridad informática realizados mediante metodologías hibridas y en Cooperativas de Transportes.

2.3.2 Técnica de Recolección de Información

En primera instancia, en la recolección de información de forma general se utilizará la entrevista, la cual estará dirigida al encargo del Departamento de Tecnologías de la Información de la Cooperativas de Transporte y que a su vez se coordinará las actividades a realizar dentro del departamento.

Para el desarrollo del proyecto nos enfocaremos en técnicas de seguridad informática ofreciendo una mejor viabilidad al desarrollo del proyecto. La técnica de caja blanca

recopilará información, comenzando por determinar el objetivo y luego obtener información específica utilizando métodos no intrusivos. Entre los datos más importantes a obtener en el uso de esta técnica tenemos:

- Equipos activos
- Procesos en ejecución
- Nombre de dominicos
- Puertos abiertos
- Direcciones ip
- Mapeo de redes
- Información de contactos

Las técnicas de sondeo de puertos servirán para la verificación y disponibilidad de los puertos en servidores.

La ingeniería social será otra técnica para recolección de información a usar, esta se desarrollará en base a la búsqueda de información personal de los miembros del departamento de TI. Mediante publicaciones de empleo por parte de la Cooperativa al área de TI obtendremos información sobre softwares y bases de datos que usan.

En el desarrollo exitoso del proyecto los beneficiarios directos serán las personas que trabajan en el departamento de Tecnologías de la Información y los beneficiarios indirectos los empleados, directores y usuarios.

2.4 Metodología de Desarrollo del Proyecto

Open Source Security Testing Methodology (OSSTMM)

OSSTMM 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 [30]. Las fases de desarrollo de la metodología son las siguientes:

Figura 3. Fases OSSTMM [30].

Ethical Hacking

Ethical hacking que significa la ética hacker es aplicada en las comunidades virtuales o de la ciber comunicación. La certificación de este brinda un amplio conocimiento sobre las más actuales herramientas que nos permiten proteger un sistema de ataques y diversos entornos en el área de la seguridad informática [31]. Las fases del Ethical Hacking son:

Figura 4. Fases de Ethical Hacking [31].

Para el desarrollo del proyecto se utilizará una metodología hibrida compuesta de la combinación de fases de la metodología OSSTMM (Open Source Security Testing Methodology) y las fases de Ethical Hacking.

Las fases a utilizar son las siguientes:

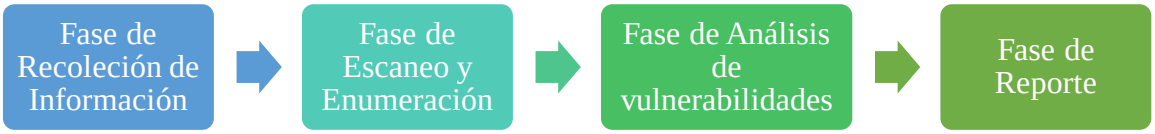


Figura 5. Fases de desarrollo.

Fase de Recolección de Información: El propósito de esta fase es la recolección de datos, tales como: cultura organizacional, reglas, normas y políticas, además permite establecer las limitaciones de la auditoría, esta fase de la metodología OSSTMM se la aplica conjuntamente con la etapa de recolección de información del hacking ético [32].

Fase de Escaneo y Enumeración: Esta fase es el núcleo de las pruebas de seguridad informática, en donde se determina el alcance de las interacciones de los activos de información y posibles brechas de seguridad, en esta fase se verifica los accesos a aplicaciones y sistemas y los controles establecidos para los mismos [32].

Fase de Análisis de vulnerabilidades: En esta etapa se realizan diferentes actividades, tales como la verificación de procesos y exposiciones que puedan provocar algún tipo de interacción, además se analiza la información que se descubre; es decir, se ponen a la luz los activos de información que se encuentran mal situados o mal administrados. Además, se buscó información disponible de manera abierta en buscadores utilizando técnicas de Google hacking, teniendo como objetivo la verificación de información relevante que estuviera sin ningún tipo de restricción en la red [32].

Fase de Reporte: Esta fase perteneciente al test de intrusión utilizará canales encubiertos para la ex filtración de evidencias tal y como los nuevos atacantes están realizando actualmente. Por último, debe proceder a documentar el análisis realizado, incluyendo las evidencias tomadas como resultado del test. Este punto se detalla en mayor profundidad en el Plan de pruebas [33].

CAPÍTULO III

Desarrollo de la propuesta

3.1 REQUERIMIENTOS

RQ-01	Se hace uso de la máquina virtual Kali Linux, para ello, se debe tener los siguientes requerimientos computacionales: - Disco de 80 Gb - Memora RAM de 3 Gb - Adaptador Puente
RQ-02	El sistema de Kali Linux debe estar actualizado con la última versión, en este caso la versión 2021.2
RQ-03	Elegir las herramientas apropiadas a través de un análisis eficaz, se evalúa las características, uso y ejecución.
RQ-04	En el desarrollo de las fases del proyecto se debe utilizar herramientas Open Source analizadas anteriormente. Aunque también se hace uso de una herramienta de pago en su versión gratuita para la comparación de resultados.
RQ-05	Para la recolección de información se hace uso de la entrevista al encargado del departamento de TI, además de una investigación diagnostica.
RQ-06	Aplicación de la técnica de caja blanca como método principal para el desarrollo del proyecto.
RQ-07	Utilizar el usuario Root del sistema para la ejecución de herramientas.
RQ-08	Ejecución de la herramienta Nmap con los argumentos necesarios para obtener puertos abiertos.
RQ-09	Para la obtención de las vulnerabilidades se debe tener la base de datos del sistema encendido y corriendo.
RQ-010	Ejecución de la herramienta Metasploit para la obtención de vulnerabilidades, se debe hacer uso de los scripts de db_nmap y los respectivos argumentos.

RQ-011	Evidenciar todo el proceso a través de capturas de pantalla y la definición de pasos a seguir.
RQ-012	Hacer uso de páginas oficiales para el análisis de vulnerabilidades y la clasificación de las mismas.
RQ-013	Usar cuadros comparativos en la clasificación del nivel de riesgo en cada resultado.
RQ-014	Presentar resumen estadístico del proceso y resultados obtenidos en las fases anteriores.
RQ-015	Proponer soluciones para resolver las vulnerabilidades encontradas en cada servidor.

Tabla 1. Requerimientos del Proyecto

3.2 Fase 1: Fase de Recolección de Información.- En esta fase se procede a identificar y comparar las herramientas que serán seleccionadas para efectuar el análisis de vulnerabilidades de los servidores.

Herramienta/ Parámetro	Nmap	Dmitry	Nexpose	Nslookup	Vega	Metasploit	Owasp Zap	Nikto
Requerimiento Computacionales	Bajo	Bajo	Bajo	Bajo	Medio	Medio	Bajo	Bajo
Complejidad de uso	Bajo	Bajo	Bajo	Bajo	Medio	Medio	Bajo	Bajo
Interfaz	Línea de comando	Línea de comando	Interfaz	Línea de comando	Interfaz	Línea de comando	Interfaz	Línea de comando
Objetivos	Sitios web, red y host	Sitios web y host	Red y host	Sitios web	Sitios web	Sitios web, red y host	Sitios web y host	Sitios web y host
Tiempo de repuesta (rendimiento)	Media	Medio	Medio	Medio	Media	Media	Alto	Medio
Resultados	Escaneo de puerto y obtención de información	Recopilación de información	Obtención y análisis de vulnerabilidades	Recopilación de información	Obtención de Información y análisis de vulnerabilidades	Obtención de Información y análisis de vulnerabilidades	Obtención de Información y análisis de vulnerabilidades	Obtención de Información y análisis de vulnerabilidades
Herramienta a utilizar	✖		✖			✖		

Tabla 2. Cuadro comparativo para la selección de herramientas

Nombre	Concepto/Uso	Ventajas	Desventajas	Tipo
Kali Linux	Es una distribución en Linux usada para la auditoria y seguridad informática en general.	• Admite la recopilación del núcleo, permitiendo agregar drivers, parches o nuevas funcionalidades. • Permite la personalización del paquete source mediante Debian Tools.	• Los servicios de red están deshabilitados. • Es difícil de instalar si es una maquina física.	Open Source
Nmap	Programa de código abierto que sirve para efectuar escaneo y rastreo de puertos	• Consta de varias opciones para realizar escaneos difícilmente detectables para la víctima. • Puede escanear cualquier rango de puertos y ver el estado de estos.	• El proceso de escaneo puede ser largo y lleva su tiempo. • El uso de la herramienta dependerá de la maquina y red.	Open Source
Nexpose	Es una herramienta que permite hacer un análisis exhaustivo de las vulnerabilidades de ambientes y redes. Puede ser útil para auditorias completas dirigidas a pequeñas y grandes empresas que manejan infraestructura tecnológica.	• Al realizar el escaneo se puede descargar en un archivo rar los resultados. • Disponible para Windows y Linux.	• Es una herramienta de pago. • Está disponible solo en inglés.	Open Source y de pago
Metasploit	Es un proyecto de código abierto para la seguridad informática, que	• Mayo fragilidad en la búsqueda de vulnerabilidades.	• Solo se actualiza esporádicamente.	Open Source

	proporciona información acerca de vulnerabilidades de seguridad y ayuda en tests de penetración "Pentesting" y el desarrollo de firmas para sistemas de detección de intrusos.	• Uso de exploits.	• El msfweb solo se debe usar en redes de confianza.	

Tabla 3. Herramientas para el desarrollo del proyecto

Las herramientas Nmap, Metasploit y Nexpose fueron las escogidas entre varias ya que presentan las mejores características en cuanto a requerimientos computacionales y eficacia en su ejecución, son herramientas Open Source permitiendo el libre uso para este caso de estudio, además se ejecutan a través de líneas de comandos y se adaptan de la mejor manera para el desarrollo del trabajo, por ello, se procederá con la respectiva instalación y ejecución.

3.2.1 Identificación de servidores

Servidor	Memoria	Disco duro	Sistema Operativo	Marca/versión	Utilidad
SERVIDOR ABC	32 GB	2 discos 1 Tb 1 Tb	Windows Server 2012 R2	Hp ProLiant DL160 Gen 9	Utilizado para la contabilidad
SERVIDOR DEF	32 GB	2 discos 2 Tb 2 Tb	Windows Server 2016	ProLiant ML350 Gen10	Contabilidad y facturación a nivel nacional.
SERVIDOR GHI	4 GB	1 Tb	Windows 7	HP Pc	Manejo de la gasolinera

Tabla 4. Servidores del Departamento de TI

La institución cuenta con tres servidores activos y uno inactivo los cuales se encuentran dentro del departamento de TI, las características más importantes y su uso fueron dadas por el personal encargado y a su vez verificadas personalmente en el sistema de cada servidor, el uso de estos equipos está distribuidos tanto para el servicio de transporte y encomiendas como para el manejo de la gasolinera, esto incluye la facturación e información de los clientes.

3.2.2 Diagrama de Red

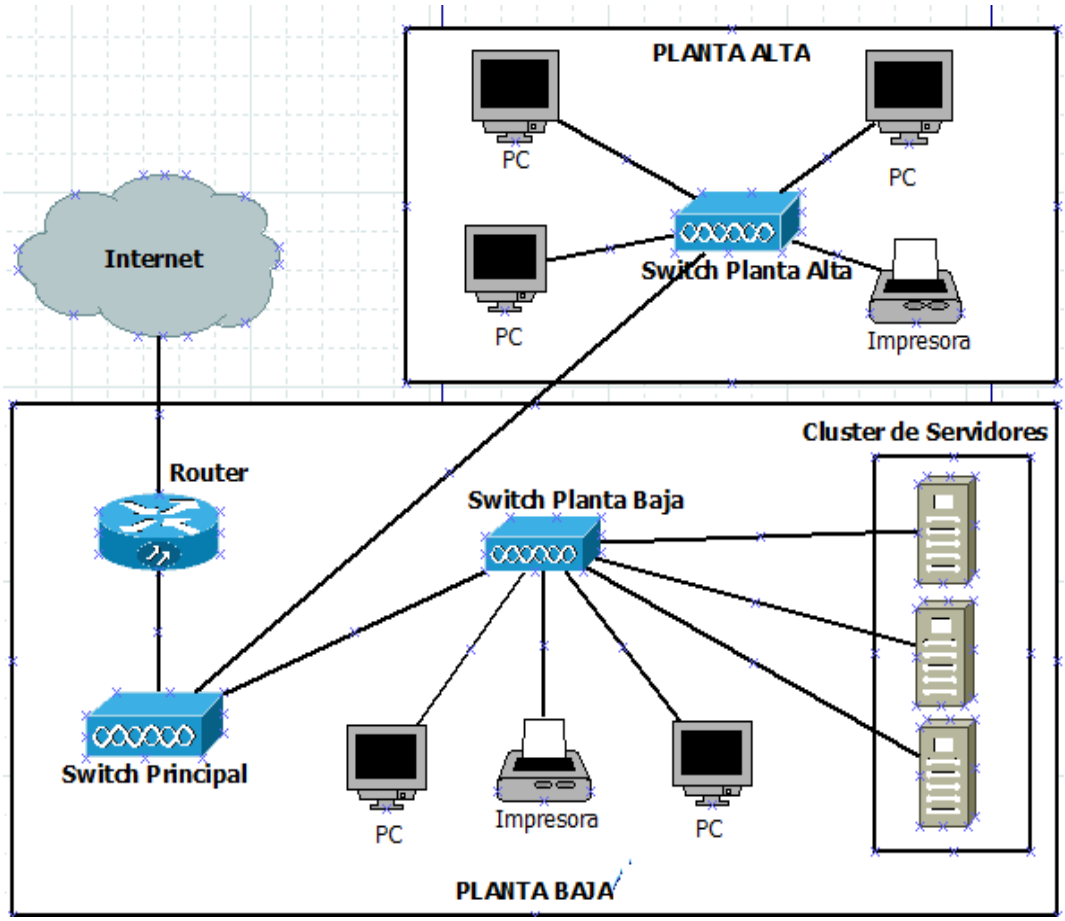


Figura 6. Diagrama de red de la Institución

Este diagrama de red representa de forma general toda la infraestructura tecnológica de la cooperativa de trasporte y evidentemente la conexión de los servidores con los demás equipos, sin embargo, hay que recalcar que los servidores se encuentran en diferentes sitios dentro del departamento.

3.3 Fase 2: Fase de Escaneo y Enumeración.- Se procede a ejecutar las herramientas Open Source para la obtención de las vulnerabilidades en cada equipo y posteriormente su enumeración.

3.3.1 Configuración del escenario

En esta fase utilizaremos la máquina virtual de Kali Linux para la cual realizamos los siguientes pasos:

1. Una vez ya instalada correctamente la máquina virtual procedemos a realizar cambio en el ajuste de red, colocando el conector en adaptar puente para una mejor conexión a la red de servidores.

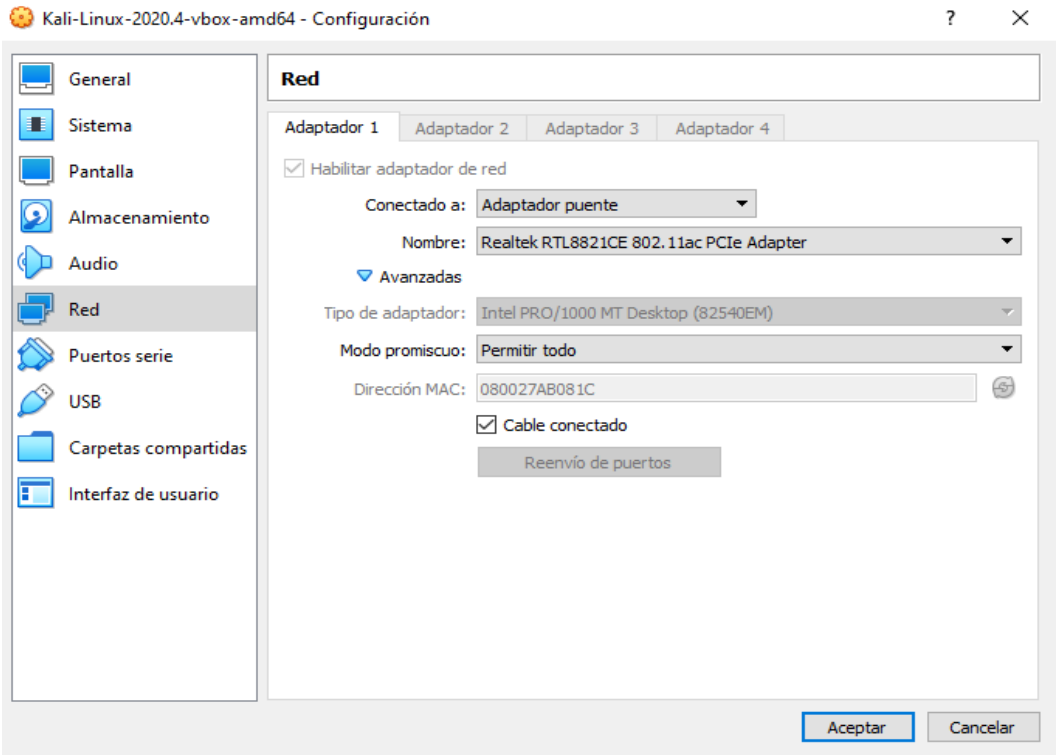


Figura 7. Configuración del adaptador de red

2. Iniciamos Kali Linux, abrimos la consola e ingresamos como usuario root.

Figura 8. Usuario root en Kali Lnux

Cabe recalcar que para tener acceso a los servidores del departamento de TI se asignó un puerto de red a través del switch principal y un cable de red, por ello, es posible la conexión directa desde la máquina virtual Kali Linux hacia la infraestructura de servidores y para comprobar se realizó uso del comando “ping” hacia cada dirección IP obteniendo respuesta inmediata.

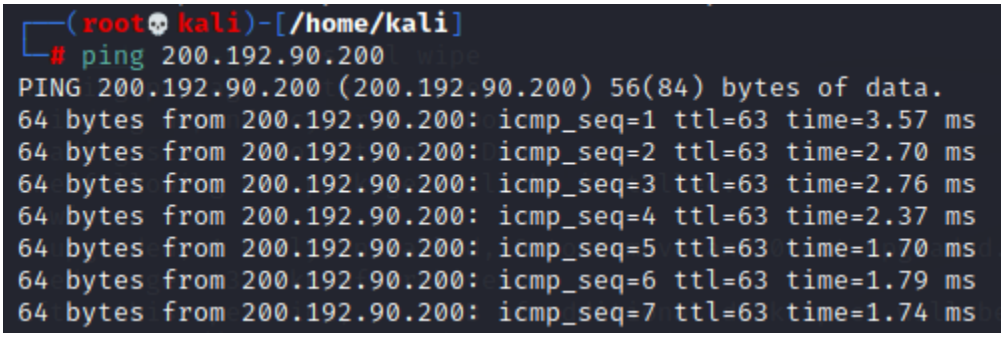


Figura 9. Ping a las IP de los servidores

3.3.2 Escaneo de puertos

Herramienta Nmap

En esta parte se intenta encontrar los tipos de puertos de cada equipo y así encontrar posibles riegos a los que están sujetos los servicios ya que los puertos abiertos son usados por usuarios mal intencionados para la denegación de servicios o afectar directamente a los equipos. Ya sabiendo las direcciones IP procedemos a utilizar la herramienta Nmap de la siguiente manera.

Ejecutamos el comando de Nmap en la línea de comando más la dirección IP.

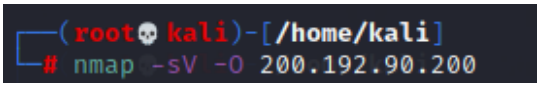


Figura 10. Escaneo de puerto con nmap

Donde:

- -sV: analiza el conjunto de puertos abiertos detectados para descubrir servicios y versiones.
- -O: envía paquetes TCP y UDP al objetivo y analizar el tipo de implementación de la pila TCP/IP.

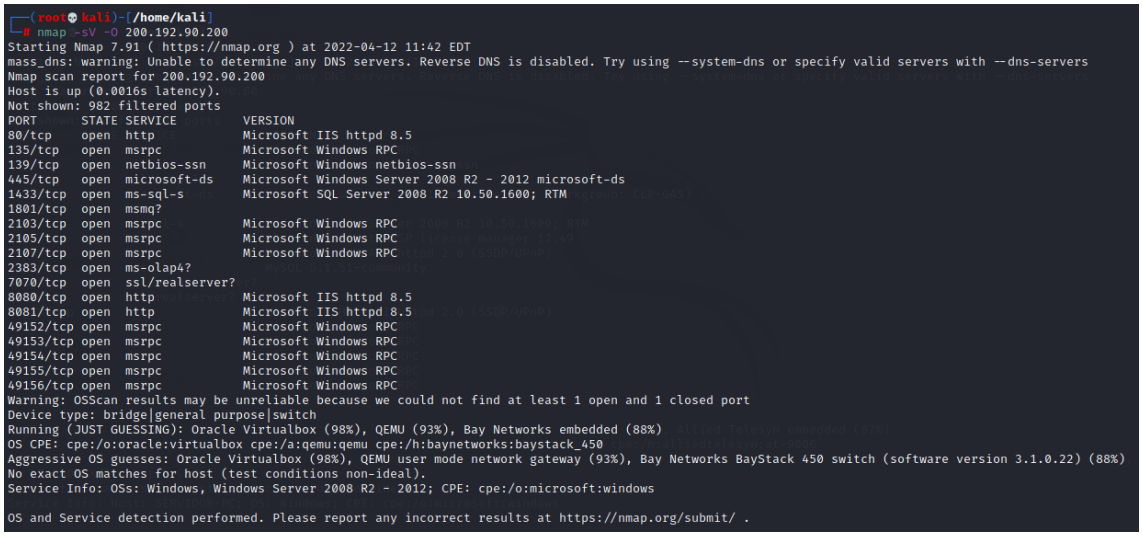


Figura 11. Resultado de la escaneada de puertos

A continuación, se mostrarán los resultados obtenidos en la ejecución del comando expuesto anteriormente de los servidores de la institución, verificando los puertos abiertos, servicios y versiones empleadas en los mismos, además del sistema operativo instalado.

SERVIDOR ABC **IP: 200.192.90.200**			
Puerto	**Estado**	**Servicio**	**Versión**
80/tcp	Abierto	http	Microsoft IIS httpd 8.5
135/tcp	Abierto	Msrpc	Microsoft Windows RPC
139/tcp	Abierto	netbios-ssn	Microsoft Windows netbios- ssn
455/tcp	Abierto	microsoft-ds	Microsoft Windows Server 2008 R2
1433/tcp	Abierto	ms-sql-s	Microsoft SQL Server 2008 R2
2103/tcp	Abierto	Msrpc	Microsoft Windows RPC
2105/tcp	Abierto	Msrpc	Microsoft Windows RPC
2107/tcp	Abierto	Msrpc	Microsoft Windows RPC
8080/tcp	Abierto	http-proxy	Microsoft IIS httpd 8.
8081/tcp	Abierto	http	Microsoft IIS httpd 8.5

49152/tcp	Abierto	Msrpc	Microsoft Windows RPC
49153/tcp	Abierto	Msrpc	Microsoft Windows RPC
49154/tcp	Abierto	Msrpc	Microsoft Windows RPC
49155/tcp	Abierto	Msrpc	Microsoft Windows RPC
49156/tcp	Abierto	Msrpc	Microsoft Windows RPC

Tabla 5. Puertos abiertos del SERVIDOR ABC

SERVIDOR DEF **IP: 200.192.90.202**			
Puerto	**Estado**	**Servicio**	**Versión**
80/tcp	Abierto	http	Microsoft IIS httpd 10.0
135/tcp	Abierto	msrpc	Microsoft Windows RPC
139/tcp	Abierto	netbios-ssn	Microsoft Windows NetBIOS- ssn
455/tcp	Abierto	microsoft-ds	Microsoft Windows Server 2008 R2
1433/tcp	Abierto	ms-sql-s	Microsoft SQL Server 2016 13.00.1742
1443/tcp	Abierto	ms-wbt-server	Microsoft Terminal Services
2103/tcp	Abierto	msrpc	Microsoft Windows RPC
2105/tcp	Abierto	msrpc	Microsoft Windows RPC
2107/tcp	Abierto	msrpc	Microsoft Windows RPC
5405/tcp	Abierto	netsupport	NetSupport PC remote Control
8080/tcp	Abierto	http-proxy	Microsoft IIS httpd 10.0

Tabla 6. Puertos abiertos del SERVIDOR DEF

SERVIDOR GHI **IP: 200.192.90.80**			
Puerto	**Estado**	**Servicio**	**Versión**
135/tcp	Abierto	Msrpc	Microsoft Windows RPC
139/tcp	Abierto	netbios-ssn	Microsoft Windows netbios- ssn

455/tcp	Abierto	microsoft-ds	Microsoft Windows 7-10 microsoft-ds (workgroup: CLP-GAS)
1433/tcp	Abierto	ms-sql-s	Microsoft SQL Server 2008 R2 10.50.1600; RTM
1947/tcp	Abierto	http	Aladdin/SafeNet HASP license manager 12.49
2869/tcp	Abierto	http	Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
3306/tcp	Abierto	Mysql	MySQL 5.1.51-Community
3389/tcp	Abierto	ssl/ms-wbt-server	
7070/tcp	Abierto	ssl/Realserver	
10243/tcp	Abierto	http	Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
49152/tcp	Abierto	Msrpc	Microsoft Windows RPC
49153/tcp	Abierto	Msrpc	Microsoft Windows RPC
49154/tcp	Abierto	Msrpc	Microsoft Windows RPC
49155/tcp	Abierto	Msrpc	Microsoft Windows RPC
49158/tcp	Abierto	Msrpc	Microsoft Windows RPC

Tabla 7. Puertos abiertos del SERVIDOR GHI

En las tablas se exponen los puertos abiertos de cada servidor, los cuales, se convierte en una especie de puerta de entrada a la información permitiendo un posible ataque a los servicios que están detrás de estos puertos. Los puertos abiertos se pueden considerar el principio de una vulnerabilidad permitiendo a los delincuentes informáticos realizar diferentes tipos de ataques como una denegación de servicio, ataque de fuerza fruta o realizar una escala de privilegios y tener el control del servidor.

Para la obtención de vulnerabilidades en los servidores se utilizarán dos herramientas para la comparación de los resultados. La primera herramienta es una Open Source, siendo Metasploit en su última versión que vine instalado en el sistema operativo de Kali Linux y la segunda herramienta es Nexpose que es una herramienta de pago, pero para su

ejecución en este caso se utilizó una licencia gratuita por treinta días, además a diferencia de la primera, esta herramienta se la utilizo en el sistema operativo de Windows 10 Home.

Herramienta Metasploit

Para la obtención de las vulnerabilidades en Metasploit se procede a configurar el escenario de la siguiente manera:

1. Arrancamos Kali Linux e ingresamos a la consola como usuario root.

Figura 12. Ingreso como usuario root

2. Iniciamos el servicio de PostgreSQL con el comando **/etc/init.d/postgresql start**

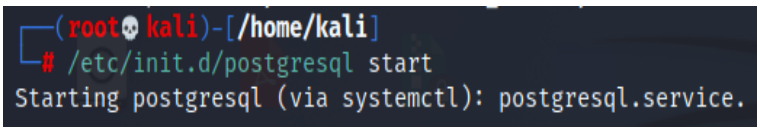


Figura 13. Inicio del servicio PostgreSql

3. Verificamos que el servicio este activado con el comando **/etc/init.d/postgresql status.**

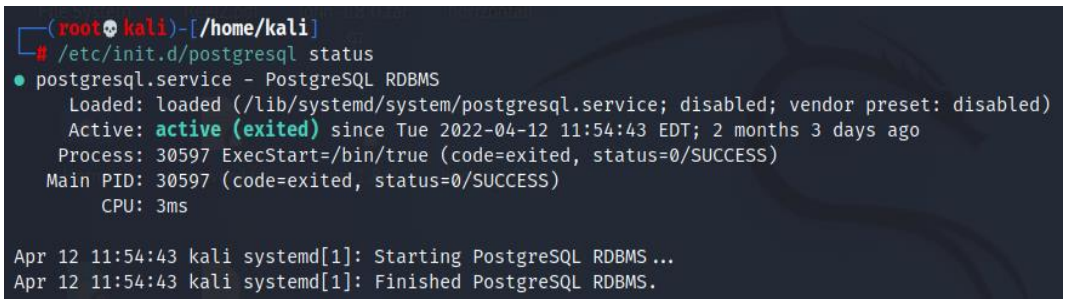


Figura 14. Verificación del servicio

4. Iniciamos la herramienta de Metasploit a través del comando **msfconsole**

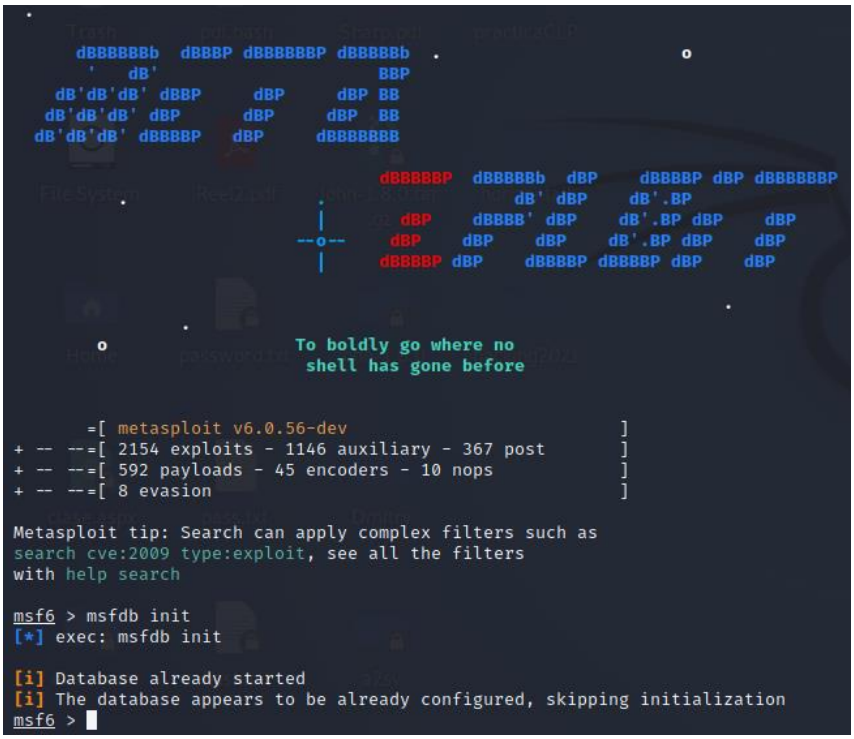


Figura 15. Herramienta Metasploit

5. En esta parte utilizaremos Nmap de metasploit y a su vez los scripts vuln NSE (Nmap Scripting Engine) que son suficientemente potentes para obtener y detectar vulnerabilidades en los servidores. Ejecutamos el script de Nmap a través del siguiente comando:

```
msf6 > db_nmap -sV -Pn --script vuln 200.192.90.202
```

Figura 16. Comando ejecutado en metasploit

En donde:

- -sV: interroga al conjunto de puertos abiertos detectados para tratar de descubrir servicios y versiones.

- -Pn: determina las maquinas activas para un escaneo más pesado y medir la velocidad de la red.
- --script: ejecuta un análisis utilizando una lista que en este caso son las vulnerabilidades.
- vuln: verifica las vulnerabilidades especificas e informan los resultados si se los encuentran.

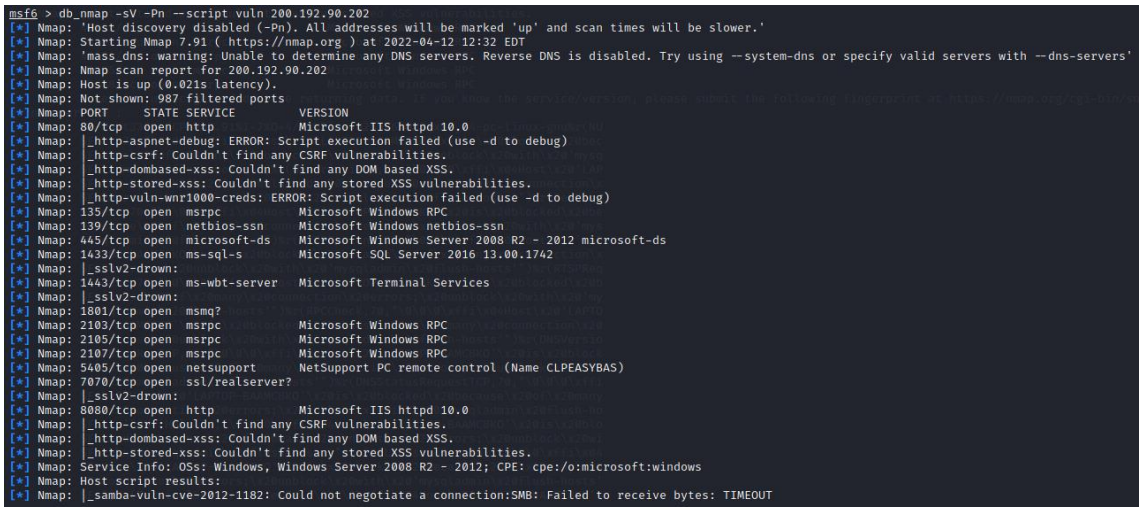


Figura 17. Vulnerabilidades encontradas con Metasploit

Finalmente terminado el proceso se procede a la respectiva enumeración. A continuación, se reflejan las vulnerabilidades encontradas en los servidores.

Resumen de vulnerabilidades				
Servidor	**Vulnerabilidad**	**Tipo**	**Explotable**	**Nivel de riesgo**
SERVIDOR ABC	CVE2014-3704	Inyección SQL	Si	Alto
	CVE2012-1182	Errores Numéricos	Si	Alto
	CVE2009-3103	Error en la gestión de recursos	Si	Alto
SERVIDOR DEF	CVE2014-3704	Inyección SQL	Si	Alto
	CVE2012-1182	Errores Numéricos	Si	Alto

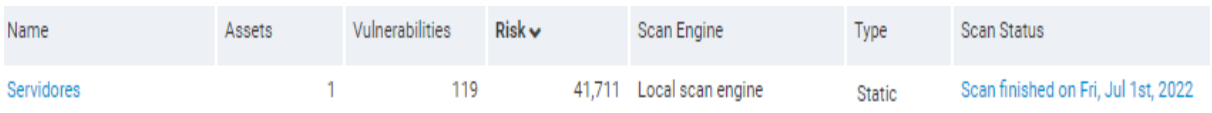
	CVE2012-1675	Permiso privilegio y/o control de acceso	Si	Alto
	CVE2009-3103	Error en la gestión de recursos	Si	Alto
SERVIDOR GHI	CVE2014-3704	Inyección SQL	Si	Alto
	CVE2014-3566	Errores criptográficos	Si	Medio
	CVE2012-2122	Autentificación Incorrecta	Si	Medio

Tabla 8. Vulnerabilidades con Metasploit

Para la determinación del nivel de riesgo y tipo de vulnerabilidades encontradas se hizo uso de la página oficial del instituto nacional de ciberseguridad de España quienes tienen un desglose completo y actualizado de las vulnerabilidades conocidas hasta la actualidad. El nivel de riesgo es determinado mediante el impacto al que está sometido la víctima, eso quiere decir que debe cumplir con ciertos valores y aspectos para saber si tienen un nivel alto, medio o bajo [34].

Herramienta Nexpose

A diferencia de la anterior, esta herramienta se maneja por medio de una interfaz, por lo tanto, una vez configurado todo el escenario para la ejecución de la herramienta Nexpose (ver anexo 2) procedemos con la obtención de vulnerabilidades, en este caso para comparar resultados se la ejecutó para el SERVIDOR GHI. Los resultados obtenidos con esta herramienta son alarmantes, en total fueron encontradas 119 vulnerabilidades como lo muestra la siguiente imagen.



Name	Assets	Vulnerabilities	Risk	Scan Engine	Type	Scan Status
Servidores	1	119	41,711	Local scan engine	Static	Scan finished on Fri, Jul 1st, 2022

Figura 18. Resultado de la herramienta Nexpose

A continuación, se muestran un resumen de las vulnerabilidades más destacadas y su nivel de severidad:

Titulo	Fecha de Publicación	Nivel de severidad
Versión obsoleta de Microsoft SQL Server	01/07/1999	Crítico
Versión obsoleta de MySQL	25/07/2007	Crítico
Firma SMB deshabilitada	01/11/2004	Muy fuerte
No se requiere firma SMBv2	01/11/2004	Muy fuerte
No se requiere firma SMB	01/11/2004	Muy fuerte
Vulnerabilidad de Oracle MySQL (CVE-2012-3163)	16/10/2012	Crítico
Vulnerabilidad de Oracle MySQL (CVE-2013-0385)	16/01/2013	Muy fuerte
Se permiten inicios de sesión CIFS no válidos	25/01/2005	Crítico
Vulnerabilidad de Oracle MySQL (CVE-2012-3158)	16/10/2012	Crítico
Vulnerabilidad de Oracle MySQL (CVE-2012-0882)	21/12/2012	Crítico
Vulnerabilidad de Oracle MySQL (CVE-2013-1492)	25/03/2013	Crítico
Vulnerabilidad de Oracle MySQL (CVE-2012-0553)	28/03/2013	Crítico
CIFS Share grabable by Guest	01/01/1999	Muy fuerte
Certificado X.509 del servidor TLS/SSL que no es de confianza	01/01/1995	Muy fuerte
El servidor TLS/SSL admite algoritmos de cifrado de exportación	01/01/1996	Muy fuerte
Vulnerabilidad de Oracle MySQL (CVE-2012-2122)	26/06/2012	Muy fuerte
Vulnerabilidad de Oracle MySQL (CVE-2012-5611)	03/12/2012	Muy fuerte
Clave criptográfica débil	01/01/2005	Moderado
El servidor TLS/SSL es compatible con deS e IDEA Cipher Suites	01/02/2009	Muy fuerte
Vulnerabilidad de Oracle MySQL (CVE-2013-1521)	16/04/2013	Muy fuerte
Vulnerabilidad de Oracle MySQL (CVE-2013-2378)	16/04/2013	Muy fuerte
Vulnerabilidad de Oracle MySQL (CVE-2013-2375)	16/04/2013	Muy fuerte

Tabla 9. Vulnerabilidades con Nexpose

3.4 Fase 3: Fase de Análisis de vulnerabilidades.- En esta fase se realiza el respectivo análisis de vulnerabilidades encontradas con la herramienta Metasploit y su organización por nivel de riesgo.

3.4.1 Análisis de vulnerabilidades

Vulnerabilidades de nivel Alto (Herramienta Metasploit)

Vulnerabilidad	CVE-2014-3704
Fecha de publicación	15/10/2014
Tipo	Inyección SQL

Impacto	Afecta parcialmente a la integridad, confidencialidad y disponibilidad del sistema.
Descripción	La función expandArguments en la API de la base de datos de abstracción para Drupal core 7.x anterior a 7.32 genera declaraciones falsas, lo que permite a atacantes remotos realizar ataques de inyección SQL a través de un conjunto de claves criptográficas de diseño especial.
Host afectado	SERVIDOR ABC, SERVIDOR DEF, SERVIDOR GHI
Recomendación	• Actualice o instale la última versión de Drupal, en este caso la última versión es la 7.32 • Asignar mínimos privilegios a usuarios comunes a la base de datos. • Usar copias de seguridad en determinados tiempos. • Si se tiene problemas con la actualización, es posible aplicar un parche temporal para solucionar la vulnerabilidad.

Tabla 10.Vulnerabilidad CVE-2014-3704

Vulnerabilidad	CVE-2012-1182
Fecha de publicación	10/04/2012
Tipo	Errores Numéricos (Generador de código RPC de Samba)
Impacto	Compromiso total de la integridad, confidencialidad y disponibilidad del sistema.
Descripción	El generador de código RPC de Samba 3.x anteriores a 3.4.16, 3.5.x anteriores a 3.5.14, y 3.6.x anteriores a 3.6.4 no implementó la validación de la longitud de la matriz de manera coherente con la validación de la matriz de asignación de memoria, lo que permitió que un atacante remoto para ejecutar una instrucción Programación aleatoria a través de una llamada RPC especialmente diseñada.
Host afectado	SERVIDOR ABC y SERVIDOR DEF
Recomendación	• Parchear o actualizar la versión de Samba. • Seleccionar la versión adecuada al sistema operativo. • Se recomienda la versión 3.6.4

Tabla 11. Vulnerabilidad CVE-2012-1182

Vulnerabilidad	CVE-2009-3103
Fecha de publicación	08/09/2009
Tipo	Error en la gestión de recursos
Impacto	Compromiso total de la integridad, confidencialidad y disponibilidad del sistema.
Descripción	Error de índice de matriz en la implementación del protocolo SMBv2 en srv2.sys en Windows Vista versión Gold, SP1 y

	SP2, Windows Server 2008 versión Gold y SP2, y Windows 7 RC, de Microsoft, permite a los atacantes remotos ejecutar código arbitrario o causar una denegación de servicio (bloqueo de sistema).
Host afectado	SERVIDOR ABC y SERVIDOR DEF
Recomendación	• Tener el sistema operativo actualizado en su última versión. En este caso del Windows Server 2012 R2. • Deshabilitar SMB v2 y asi el host se comunicará mediante SMB 1.0. • Bloquear los puertos TCP 139 Y 445 en el firewall. Tener en cuenta que al realizar esto, los servicios y aplicaciones que usen estos puertos no funcionaran. • Bloquear toda comunicación entrante no solicitada de Internet ayudando a impedir ataques por medio de los puertos.

Tabla 12. Vulnerabilidad CVE-2009-3103

Vulnerabilidad	CVE-2012-1675
Fecha de publicación	08/05/2012
Tipo	Permisos, privilegios y/o control de acceso
Impacto	Afecta parcialmente a la integridad, confidencialidad y disponibilidad del sistema.
Descripción	TNS Listener, tal como es usado en Oracle Database 11g 11.1.0.7, 11.2.0.2, y 11.2.0.3, y 10g 10.2.0.3, 10.2.0.4, y 10.2.0.5, y en Oracle Fusion Middleware, Enterprise Manager, E-Business Suite, y posiblemente otros productos, permite a atacantes remotos ejecutar comandos de base de datos arbitrarios realizando un registro remoto de una instancia o nombre de servicio de base de datos que ya existe y, a continuación, realizando un ataque de man-in-the-middle (MITM) para secuestrar conexiones de bases de datos.
Host afectado	SERVIDOR DEF
Recomendación	• Usar clases de transporte seguro en Oracle para restringir el registro de instancias. • Permitir que solo las instancias locales puedan registrarse, • Si se tiene Oracle RAC también se recomienda usar clase de transporte seguro para restringir el registro de instancias, • Usar “SECURE_REGISTER_listener_name=” para restringir el registro de instancias con el nodo local y los agentes de escuchan SCAN en un entorno RAC 11.2.

Tabla 13. Vulnerabilidad CVE-2012-1675

Vulnerabilidades de nivel Medio (Herramienta Metasploit)

Vulnerabilidad	CVE-2014-3566
Fecha de publicación	14/10/2014
Tipo	Errores Criptográficos (Protocolo SSL)
Impacto	No hay impacto en la integridad, confidencialidad y disponibilidad del sistema.
Descripción	El protocolo SSL 3.0, utilizado en OpenSSL hasta 1.0.1i y otros productos, utiliza relleno (padding) CBC no determinístico, lo que facilita a atacantes man-in-the-middle obtener datos en texto plano a través de un ataque de relleno (padding) Oracle, también conocido como el problema 'POODLE'.
Host afectado	SERVIDOR GHI
Recomendación	• Desactive el protocolo SSL 3.0 para todo aquel servicio afectado. • Tener en cuenta que puede ver error en el inicio de sección inicial. • Usar McAfee en su última versión ya que corrige automáticamente el riesgo.

Tabla 14. Vulnerabilidad CVE-2014-3566

Vulnerabilidad	CVE-2012-2122
Fecha de publicación	26/06/2012
Tipo	Autenticación incorrecta (Oracle MySQL)
Impacto	Afecta parcialmente a la integridad, confidencialidad y disponibilidad del sistema.
Descripción	Cuando se ejecuta en determinados entornos con determinadas implementaciones de la función memcmp, permite que atacantes remotos eviten la autenticación utilizando repetidamente la misma contraseña incorrecta, lo que eventualmente provoca una comparación de token con resultado de éxito en una variable de retorno no validada
Host afectado	SERVIDOR GHI
Recomendación	• Evitar exponer la base de datos a la red. • Configurar el acceso al dominio de la base de datos solo para localhost. • Restringir el acceso al sistema local modificando el archivo my.cnf. • Actualizar o parchear la base datos.

Tabla 15. Vulnerabilidad CVE-2012-2122

Vulnerabilidades de nivel Crítico (Herramienta Nexpose)

Vulnerabilidad	mssql-obsoleto-version
Fecha de publicación	01/07/1999
Tipo	Versión Obsoleta de Microsoft SQL Server
Impacto	Afecta directamente a la integridad, confidencialidad y disponibilidad del sistema.
Descripción	Se está ejecutando una versión obsoleta del servidor de base de datos Microsoft SQL. Como ya se termina el período de soporte técnico, ya no se tiene parches de seguridad estando expuestos a ataques.
Host afectado	SERVIDOR GHI
Recomendación	• Actualizar a la versión más reciente de Microsoft SQL Server • Utilizar la documentación técnica de Microsoft para ayudar a empezar, administrar, desarrollar y trabajar con SQL Server.

Tabla 16. Vulnerabilidad mmql-obsoleto-version

Vulnerabilidad	mysql-obsoleto-version
Fecha de publicación	01/07/1999
Tipo	Versión Obsoleta de Microsoft SQL Server
Impacto	Afecta directamente a la integridad, confidencialidad y disponibilidad del sistema.
Descripción	Se está ejecutando una versión obsoleta de MySQL. Ya no existe un periodo de soporte para esta versión por consiguiente no cuenta con parches de seguridad estando expuestos a ataques.
Host afectado	SERVIDOR GHI
Recomendación	• Actualizar a la versión más reciente de Oracle MySQL. • Utilizar la documentación técnica de Microsoft para ayudar a empezar, administrar, desarrollar y trabajar con SQL Server.

Tabla 17. Vulnerabilidad mysql-obsoleto-version

Vulnerabilidad	Windows7-obsoleto
Fecha de publicación	14/01/2020
Tipo	Versión Obsoleta de Microsoft Windows 7
Impacto	Afecta directamente a la integridad, confidencialidad y disponibilidad del sistema.
Descripción	El soporte extendido para todas las versiones de Windows 7 finalizó a inicios del año 2020, por lo tanto, las versiones no

	compatibles de Windows pueden contener fallos de seguridad.
Host afectado	SERVIDOR GHI
Recomendación	• Actualizar a la versión más reciente de Microsoft Windows. • Instalar un Windows adecuado a los requisitos computacionales de la máquina.

Tabla 18. Vulnerabilidad Windows7-obsoleto

Vulnerabilidad	CVE-2012-3163, CVE-2012-3158
Fecha de publicación	16/10/2012
Tipo	Versión incorrecta (Oracle MySQL)
Impacto	Afecta directamente a la integridad, confidencialidad y disponibilidad del sistema.
Descripción	Estas versiones obsoletas permiten a los usuarios autenticados remotos afectar la confidencialidad, la integridad y la disponibilidad a través de vectores desconocidos relacionados con el esquema de información.
Host afectado	SERVIDOR GHI
Recomendación	• Consultar con el sitio web de Oracle para obtener información obre parches y actualizaciones. • Aplicar la actualización apropiada para el sistema.

Tabla 19. Vulnerabilidad CVE-2012-3163 CVE-2012-3158

Vulnerabilidad	cifs-invalid-logins-allowed
Fecha de publicación	25/01/2005
Tipo	Se permiten inicios de sesión CIFS no válidos
Impacto	Afecta directamente a la integridad, confidencialidad y disponibilidad del sistema.
Descripción	Todas las variantes conocidas de Windows desde Windows XP incluyen un modo de funcionamiento "ForceGuest" mediante el cual el servicio CIFS permite a los usuarios no autenticados conectarse al servicio con acceso limitado.
Host afectado	SERVIDOR GHI
Recomendación	Dentro de la configuración de seguridad local en el panel de control de Windows server, modifique la siguiente configuración. • Establezca la opción “Directivas locales -> Asignación de derechos de usuario -> Acceso de silencio a este equipo desde la red” y así incluir la cuenta de invitado.

	• Establezca la opción “Políticas locales -> Opciones de seguridad -> Cuentas: estado de la cuenta de invitado” en deshabilitado.

Tabla 20. Vulnerabilidad cifs-invalid-logins-allowed

Vulnerabilidad	CVE-2012-0882
Fecha de publicación	21/12/2012
Tipo	Versión incorrecta (Oracle MySQL)
Impacto	Afecta directamente a la integridad, confidencialidad y disponibilidad del sistema.
Descripción	Permite a los atacantes remotos ejecutar código arbitrario a través de vectores no especificados ya que existe un desbordamiento de búfer en SSL.
Host afectado	SERVIDOR GHI
Recomendación	• Descargar y aplicar la actualización de Oracle MySQL a la versión 5.5.22 • Corregir parches acumulativos, pero tener en cuenta que el sistema operativo puede proporcionar sus propios medios para la respectiva actualización.

Tabla 21. Vulnerabilidad CVE-2012-0882

Vulnerabilidad	CVE-2013-1492, CVE-2012-0553
Fecha de publicación	28/03/2013
Tipo	Versión incorrecta (Oracle MySQL)
Impacto	Afecta directamente a la integridad, confidencialidad y disponibilidad del sistema.
Descripción	Esta versión de MySQL tiene vectores de impacto y ataque no especificados.
Host afectado	SERVIDOR GHI
Recomendación	• Descargar y aplicar la actualización de Oracle MySQL a la versión 5.5.22 • Corregir parches acumulativos, pero tener en cuenta que el sistema operativo puede proporcionar sus propios medios para la respectiva actualización.

Tabla 22. Vulnerabilidad CVE-2013-1492, CVE-2012-0553

3.5 Fase 4: Fase de Reporte.- En esta fase se presenta un resumen técnico de todo el proceso ejecutado en las fases anteriores, así como información relevante sobre los resultados obtenidos.

3.5.1 Reporte estadístico de Vulnerabilidades

Vulnerabilidades con Metasploit

Con la ejecución de esta herramienta se encontraron diez vulnerabilidades en su totalidad descripta a continuación:

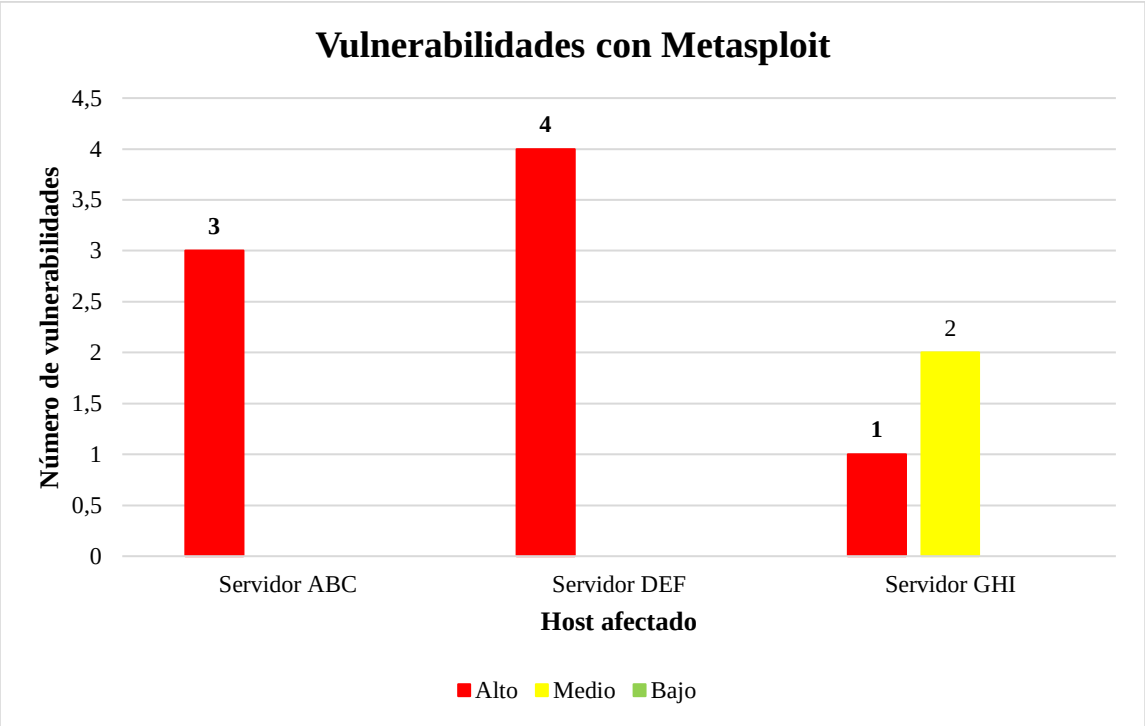


Figura 19. Cantidad de vulnerabilidades con Metasploit

Las vulnerabilidades encontradas en los servidores muestran el peligroso en los que se encuentras estos además de los servicios que prestan hacia la institución. Su impacto y su respectivo análisis se da por medio del nivel de riesgo por lo que clasifican de la siguiente manera:

	Vulnerabilidades		
Servidores	**Alto**	**Medio**	**Bajo**
SERVIDOR ABC	CVE-2014-3704 CVE-2012-1182 CVE-2009-3103		
SERVIDOR DEF	CVE-2014-3704 CVE-2012-1182 CVE2012-1675 CVE-2009-3103		

SERVIDOR GHI	CVE-2014-3704	CVE-2014-3566 CVE-2012-2122	
TOTAL	**8**	**2**	**0**

Tabla 23. Nivel de riesgo de las vulnerabilidades

La clasificación del nivel de riesgo se da a través una investigación realizada por el Instituto Nacional de Ciberseguridad de España [35] quienes clasifican el nivel de seguridad de la siguiente manera:

Nivel alto

- Permite a un atacante remoto violar la protección de seguridad de un sistema.
- Permite un ataque local para tomar el control completo del sistema.

Nivel medio

- Se encuentra a la mitad del riesgo por lo que el sistema puede funcionar con normalidad.

Nivel bajo

- La vulnerabilidad no permite el robo de información o la toma del control de un sistema.
- El riesgo de la vulnerabilidad resulta inocua para la mayoría de las empresas u organizaciones.

Vulnerabilidades con Nexpose

Con Nexpose se analizó las vulnerabilidades en uno de los servidores, cuyos resultados evidencian la robustes de la herramienta ya que, a diferencia de la anterior, se detectaron gran cantidad de vulnerabilidades resumidas en el siguiente gráfico estadístico:

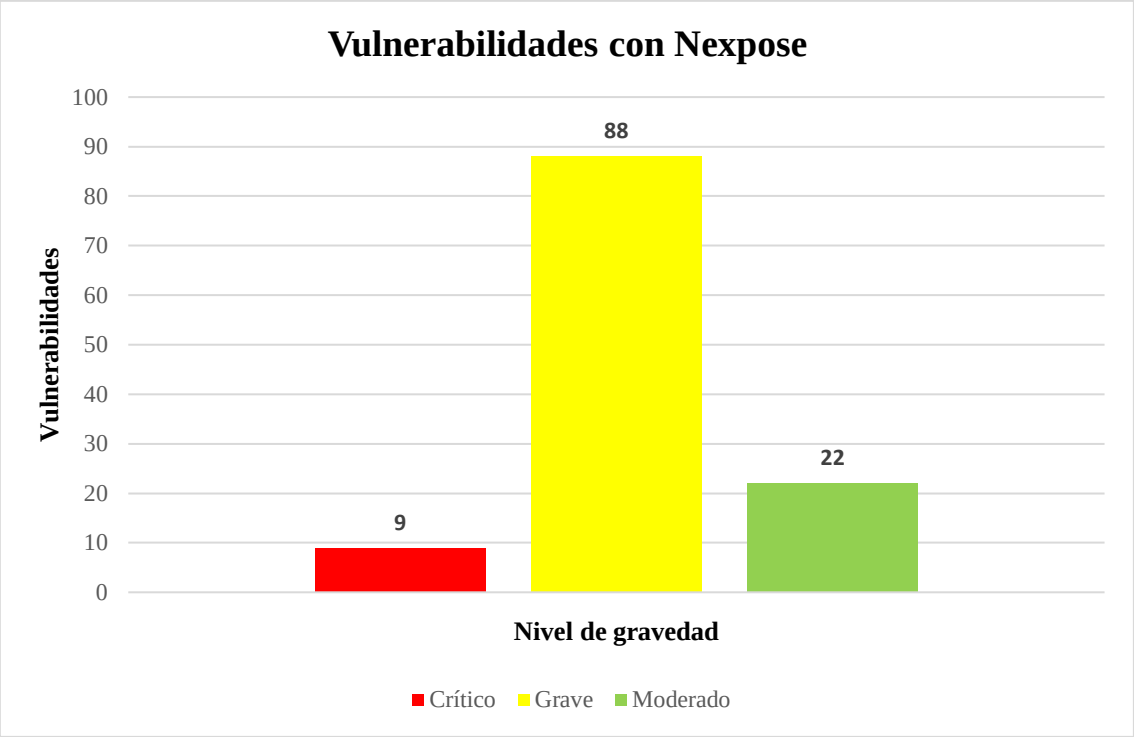


Figura 20. Nivel de gravedad con Nexpose

Se encontraron un total de 119 vulnerabilidades durante el análisis, de estos, nueve eran vulnerabilidades criticas requiriendo de la solución lo más antes posible ya que son relativamente fáciles de explotar para cualquier usuario mal intencionados pudiendo obtener el control total de los sistemas y servicios; 88 vulnerabilidades son graves siendo más difíciles de explotar y es posible que no se puedan acceder a los sistemas usando estas vulnerabilidades; 22 son moderadas siendo el nivel más bajo también pueden proporcionar información a los atacantes pero se pueden solucionar de manera más oportuna.

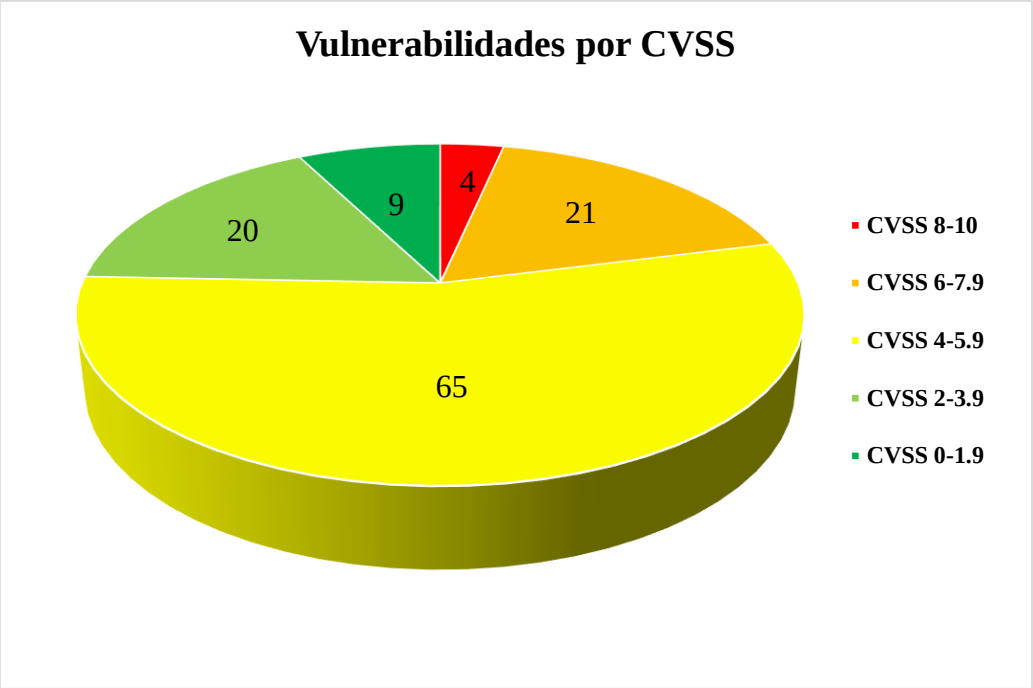


Figura 21. Vulnerabilidades por nivel de CVSS

La herramienta también analiza las vulnerabilidades por el nivel de CVSS que básicamente utiliza tres métricas, grupo de métricas base quienes representan la característica fundamental de la vulnerabilidad y que no varía con el tiempo ni el ambiente; el grupo de métricas temporal que representa las características que cambian con el tiempo; por último el grupo de métrica ambiental que representa las características de las vulnerabilidades que solo son relevantes para un entorno especifico [36]. Por ello este nivel se clasifica de la siguiente manera:

Puntuación	Severidad por CVSS
0 – 1.9	Nula
2 – 3.9	Baja
4 – 5.9	Media
6 – 7.9	Alta
8 – 10	Critica

Tabla 24. Evaluación de Severidad

3.5.2 Documentación de soluciones a vulnerabilidades más críticas encontradas

A continuación, se documentan de forma general las vulnerabilidades encontradas en los servidores incluyendo las soluciones prácticas que se deberían ejecutar para proteger y asegurar la correcta funcionalidad de los sistemas y servicios de la cooperativa de transporte de la provincia de Santa Elena.

CVE-2014-3704

- Actualice o instale la última versión de Drupal, en este caso la última versión es la 7.32
- Asignar mínimos privilegios a usuarios comunes a la base de datos.
- Usar copias de seguridad en determinados tiempos.
- Si se tiene problemas con la actualización, es posible aplicar un parche temporal para solucionar la vulnerabilidad.

CVE-2012-1182

- Parchear o actualizar la versión de Samba.
- Seleccionar la versión adecuada al sistema operativo.
- Se recomienda instalar la versión 3.6.4

CVE-2009-3103

- Tener el sistema operativo actualizado en su última versión. En este caso del Windows Server 2012 R2.
- Deshabilitar SMB v2 y asi el host se comunicará mediante SMB 1.0.
- Bloquear los puertos TCP 139 Y 445 en el firewall. Tener en cuenta que al realizar esto, los servicios y aplicaciones que usen estos puertos no funcionaran.
- Bloquear toda comunicación entrante no solicitada de Internet ayudando a impedir ataques por medio de los puertos.

CVE-2012-1675

- Usar clases de transporte seguro en Oracle para restringir el registro de instancias.
- Permitir que solo las instancias locales puedan registrarse,
- Si se tiene Oracle RAC también se recomienda usar clase de transporte seguro para restringir el registro de instancias,

CVE-2014-3566

- Desactive el protocolo SSL 3.0 para todo aquel servicio afectado.
- Tener en cuenta que puede ver error en el inicio de sección inicial.
- Usar McAfee en su última versión ya que corrige automáticamente el riesgo.

CVE-2012-2122

- Evitar exponer la base de datos a la red.
- Configurar el acceso al dominio de la base de datos solo para localhost.
- Restringir el acceso al sistema local modificando el archivo my.cnf.
- Actualizar o parchear la base datos.

MSSQL-OBSOLETE-VERSION

- Actualizar a la versión más reciente de Microsoft SQL Server
- Utilizar la documentación técnica de Microsoft para ayudar a empezar, administrar, desarrollar y trabajar con SQL Server.

CVE-2012-3163, CVE-2012-3158

- Consultar con el sitio web de Oracle para obtener información obre parches y actualizaciones.
- Aplicar la actualización apropiada para el sistema.

Se permiten inicios de sesión CIFS no válidos

Dentro de la configuración de seguridad local en el panel de control de Windows server, modifique la siguiente configuración.

- Establezca la opción “Directivas locales -> Asignación de derechos de usuario -> Acceso de silencio a este equipo desde la red” y así incluir la cuenta de invitado.
- Establezca la opción “Políticas locales -> Opciones de seguridad -> Cuentas: estado de la cuenta de invitado” en deshabilitado.

CVE-2013-0384, CVE-2012-5611

- Actualizar MySQL Server a la versión 5.1.67, 5.5.29 o posterior.

CVE-2012-0882, CVE-2013-1492, CVE-2012-0553

- Descargar y aplicar la actualización de Oracle MySQL a la versión 5.5.22
- Corregir parches acumulativos, pero tener en cuenta que el sistema operativo puede proporcionar sus propios medios para la respectiva actualización.

Firma SMB deshabilitada

- Configure Samba para habilitar la firma SMB según corresponda, abra smb.conf y coloque *server signing = auto*.
- Para requerir la firma coloque *server signing = mandatory* en smb.conf

CIFS Share grabbable by Guest

- Ajustar los permisos de uso compartido para que solo los miembros de la organización tengan acceso.
- Evitar dar acceso de lectura o escritura a un recurso compartido.

CVE-2014-0224

- Actualizar a última versión de Open SSL, se recomienda la versión 3.0.5

Servidor TLS/SSL admite algoritmos de cifrado de exportación

- Configure el servidor para deshabilitar la compatibilidad con cifrados de exportación.
- Consulte la documentación del proveedor del servidor para la aplicación de la configuración de cifrado.

Acceso abierto a la base de datos

- Configure los servidores de base de datos para que solo permita el acceso a sistemas de confianza.
- Colocar la base de datos en una zona de red interna.

Firma basada en MD5 en el certificado TLS/SSL Server X.509

- Dejar de usar algoritmos de firma en MD5 y en su lugar use SHA-2.

Servidor TLS/SSL es compatible con SSLv3

- Configurar el servidor para que requiera a los clientes TLS versión 1.2 mediante cifrados compatibles con cifrado autenticado con datos asociados.

Seguridad Lógica de Servidores

Política de seguridad de equipos

- El departamento de Tecnologías de la Información de la cooperativa debe proporcionar soluciones de seguridad que integre herramientas como antivirus, antispyware, firewall y políticas para la prevención de intrusos.
- Los servidores deben tener instalado un antivirus lo suficientemente eficaz y con la respectiva licencia de ser el caso.
- Se debe realizar un análisis periódico en la seguridad informática en los servidores y tener actualizado todos os sistemas posibles.

Política para Sistemas y Software desactualizados

- Actualizar el sistema y softwares de los servidores de acuerdo a las nuevas actualizaciones o parches de seguridad.
- Se recomienda la depuración de Log en cada mantenimiento periódico a lo que están sujetos los equipos.
- El sistema instalado debe garantizar la seguridad y estabilidad de los servicios y del equipo físico.
- Los softwares instalados deben provenir de sitios o fuentes seguras para evitar problemas de funcionamiento y seguridad.
- Asignar responsabilidades a los miembros del departamento para que estén vigilantes a problemas y vulnerabilidades.

Políticas ante configuraciones por defecto

- Evitar las configuraciones por defecto en los servicios a los cuales tengan acceso usuarios.
- Administrar los privilegios de la cuenta de administrador mediante la asignación de roles de usuario.
- Reducir el número de usuarios con acceso a la cuenta de Administrador en mínimo posible.

Políticas ante ataques a los servidores

- Tener un manual o procedimiento anti intrusos y capacitar con los miembros del departamento.
- Al detectar algún ataque se debe implementar un Sistema de Detección de Intrusos que se podrá encargar de monitorizar los eventos que ocurren en los sistemas de los servidores.
- Configurar IDS para evitar poner en riesgo la confidencialidad, disponibilidad e integridad en la infraestructura de servidores.

CONCLUSIONES

- ✓ La cooperativa de transporte de la provincia de Santa Elena no ha realizado ningún estudio en relación a la seguridad informática a los servidores del departamento de TI, además no cuentan con un manual de seguridad informática para estos activos de información y tampoco hacen uso de herramientas que ayuden al análisis de vulnerabilidades, por ello, esta propuesta tecnológica es de gran ayuda para la cooperativa.

- ✓ El análisis de vulnerabilidades aplicado en este proyecto se ejecutó a través de una investigación diagnostica y a través de los estudios realizados por el Instituto Nacional de Ciberseguridad de España.

- ✓ Para la obtención de vulnerabilidades se utilizó tanto una herramienta gratuita ejecutada en línea de comandos y una herramienta de pago a través de una interfaz gráfica evidenciando la eficacia y disponibilidad en los resultados y así concluir que es mejor utilizar herramientas de pago para una mejor visualización de resultados.

RECOMENDACIONES

- ✓ El encargado del departamento de TI de la cooperativa de transporte de la provincia de Santa Elena debe realizar un estudio periódico a la seguridad informática en los servidores para reducir vulnerabilidades y riesgos que pongan en peligro los servicios de la institución.

- ✓ Se debe aplicar herramientas de análisis y detención de vulnerabilidades de acuerdo con los servicios de cada servidor.

- ✓ Para un mejor análisis se recomienda usar mas de una herramienta de escaneo de vulnerabilidades y si es posible una de pago para la respectiva comparación de resultados.

- ✓ El administrador de los servidores debe actualizar en su última versión los servicios que se ejecutan en ellos además de los sistemas operativos ya que la mayoría de vulnerabilidades encontrados se solucionan con la aplicación de parches de seguridad que vienen incluida en la respectiva actualización, además se debe implementar una técnica de hardening para la protección de puertos abiertos.

Anexos

Anexo 1. Entrevista

Tema: Estudio de la seguridad informática a los servidores de una cooperativa de transporte de la provincia de Santa Elena.

Fecha: 10/10/2021

Entrevista dirigida a: Director o encargado del departamento de TI,

Objetivo: Obtener información de forma oral y personalizada sobre la seguridad informática en los servidores de la Cooperativa de Transporte.

Preguntas

1. **¿Quiénes conforman el departamento de TI en la Cooperativa de Transporte?**

2. **¿Cuáles son los tipos de servidores con los que cuenta la institución?**

3. **¿Cómo está estructurada la infraestructura de TI?**

4. **¿Quiénes son los encargados de la seguridad de la información en el departamento de TI?**

5. **¿Cuál es el tipo de amenazada que se detecta con mayor frecuencia en los servidores de la Cooperativa de Transporte?**

6. **¿Cuáles son las acciones que ha tomado para mitigar estos ataques?**

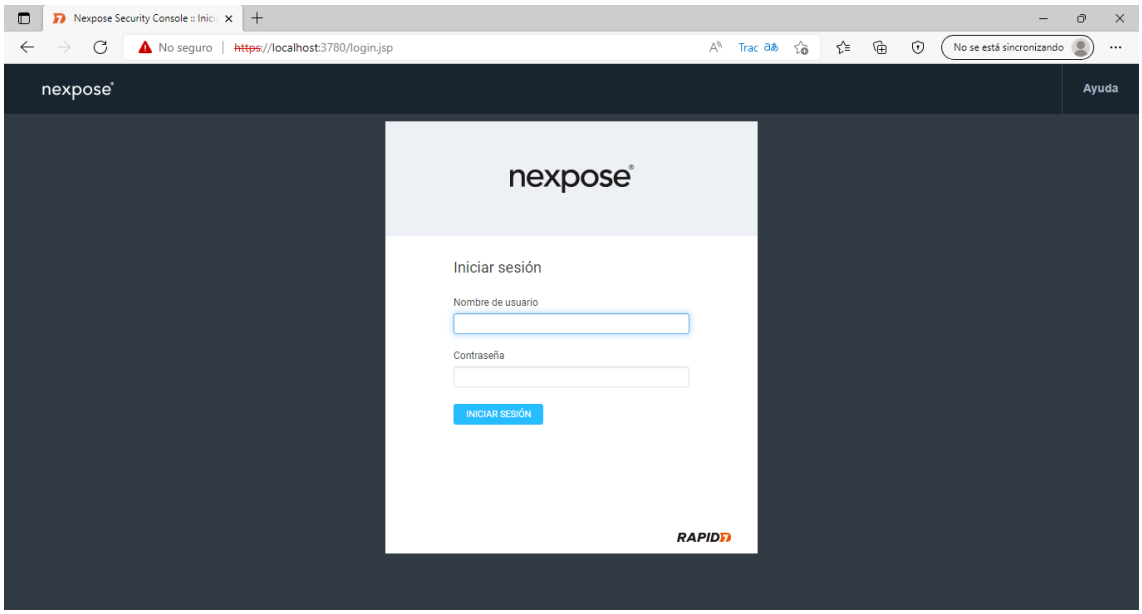
7. **¿Se han realizado estudios a la seguridad informática en la Institución?**

8. **¿Cuenta con reportes mensuales?**

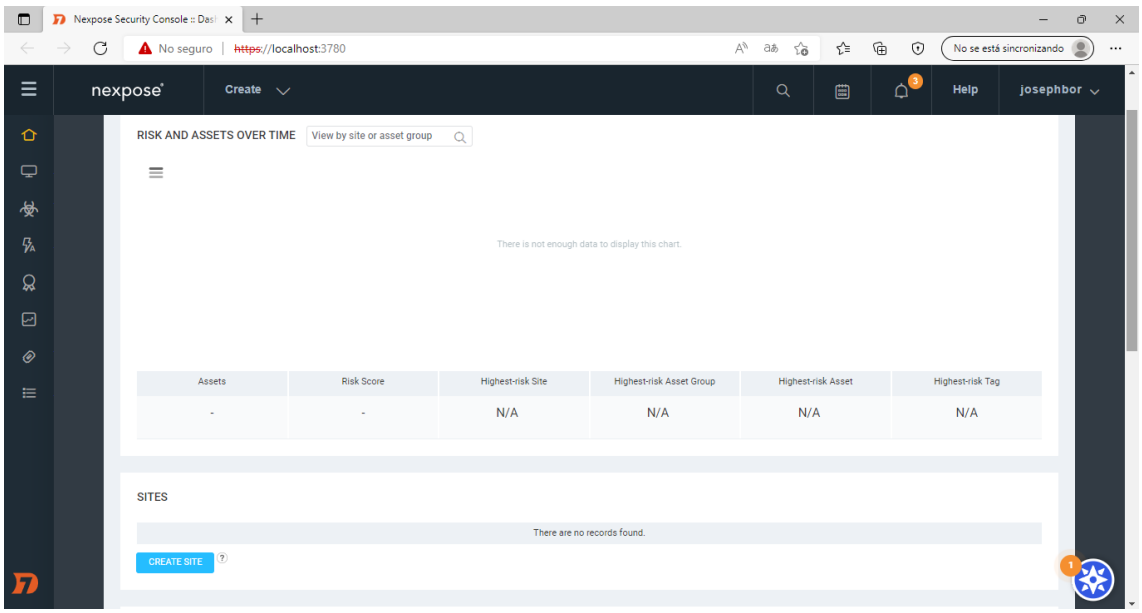
Anexo 2. Herramienta Nexpose

Configuración del escenario

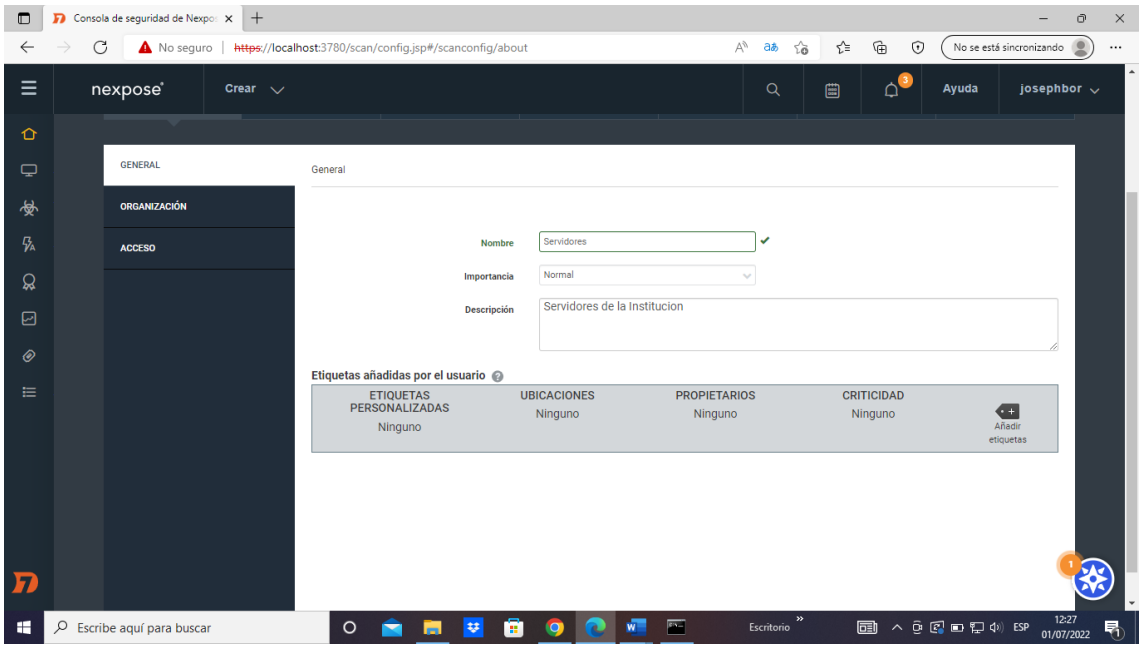
1. Una vez descargado e instalado la herramienta Nexpose para Windows y la obtención de la licencia gratuita por treinta días, se procede al ingreso del usuario y contraseña como lo requiere el Login del software.



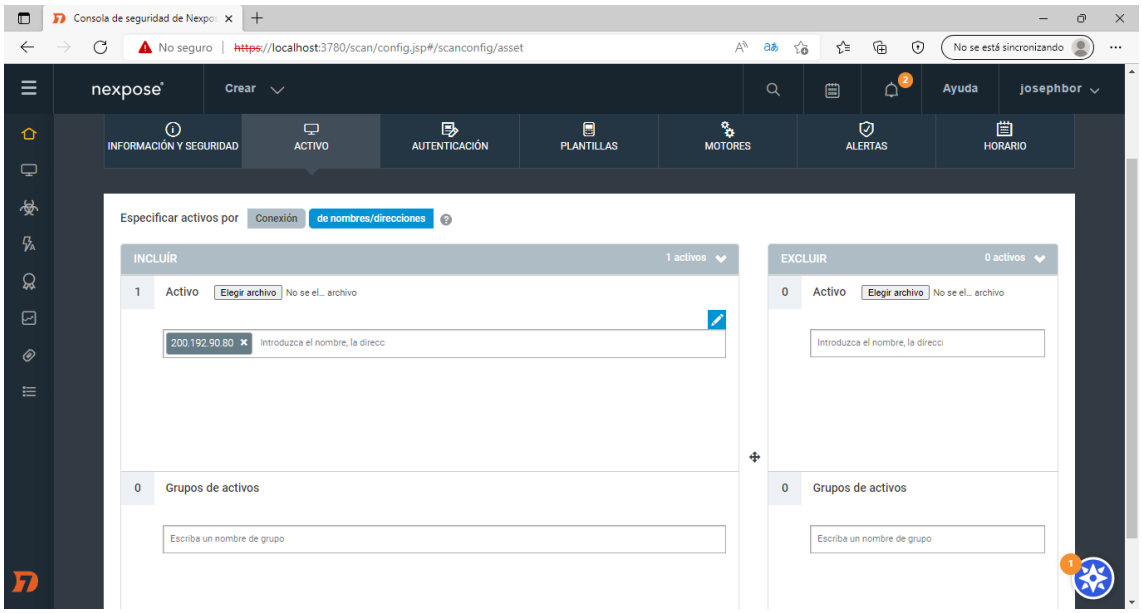
2. Al ingresar vemos la interfaz sin datos y prácticamente todos sus campos en blanco, por ello damos clic en “crear sitio”.



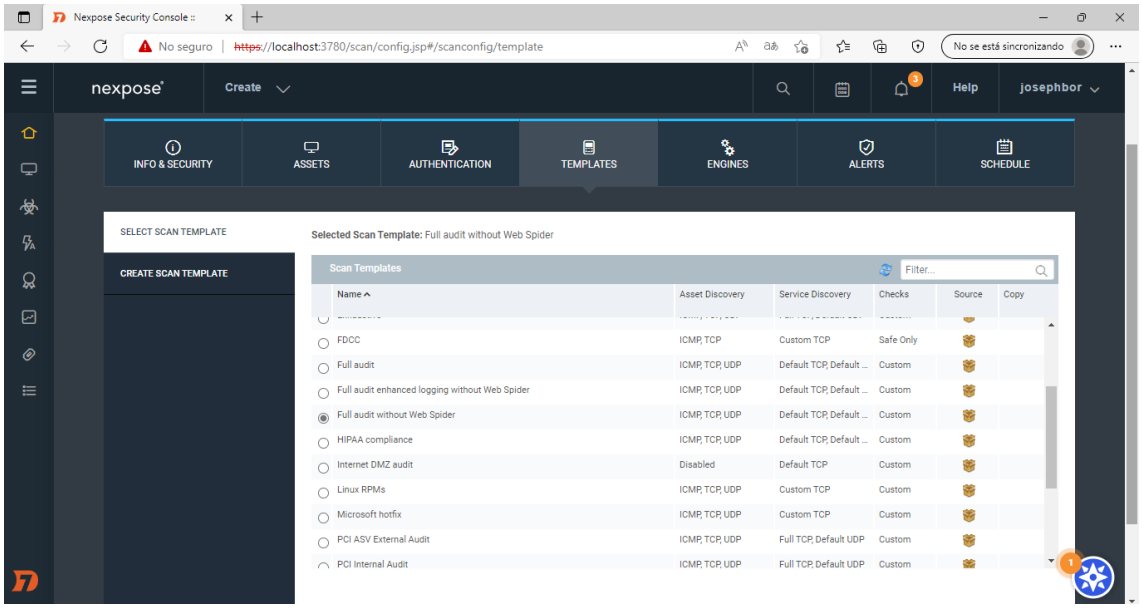
3. Colocamos un nombre al caso, el nivel de importancia y una breve descripción, también podemos colocar información sobre la institución y el acceso al objetivo, pero eso dependerá de la empresa o el profesional.



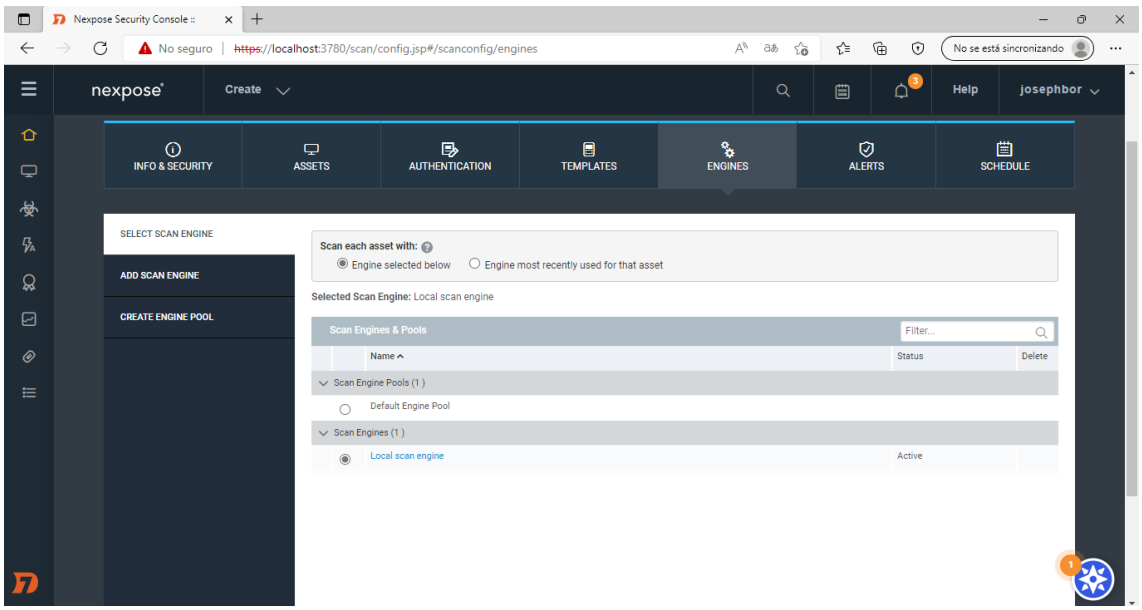
4. Para colocar al activo se puede hacer uso de la dirección IP, rango de IP o el nombre del host, en este caso se colocó la IP del SERVIDOR GHI.



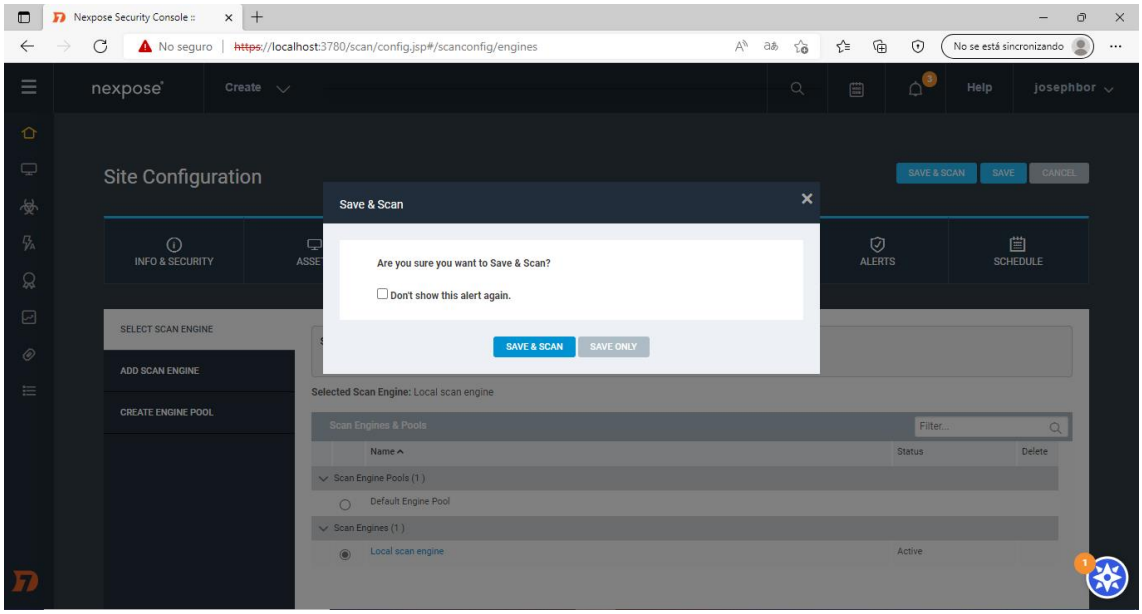
5. El siguiente es la autentificación, pero se la deja como esta, en la sección de plantillas se elige “Auditoria Completa sin Web Spider”.



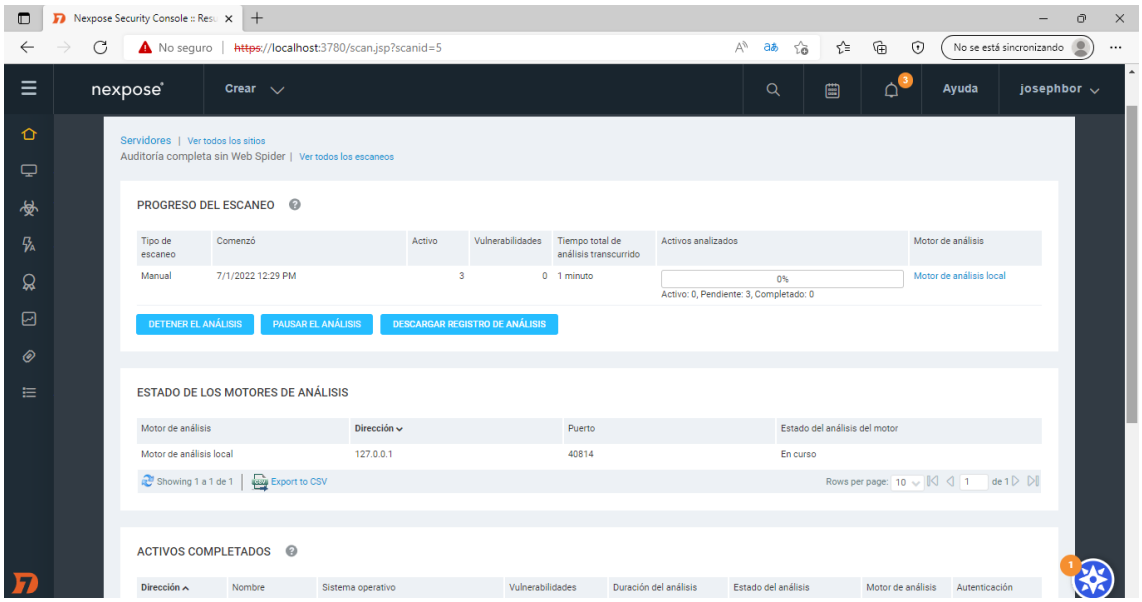
6. Como Nexpose usa motores de búsqueda de vulnerabilidades, utilizamos “Local scan Engine” que vine por defecto.



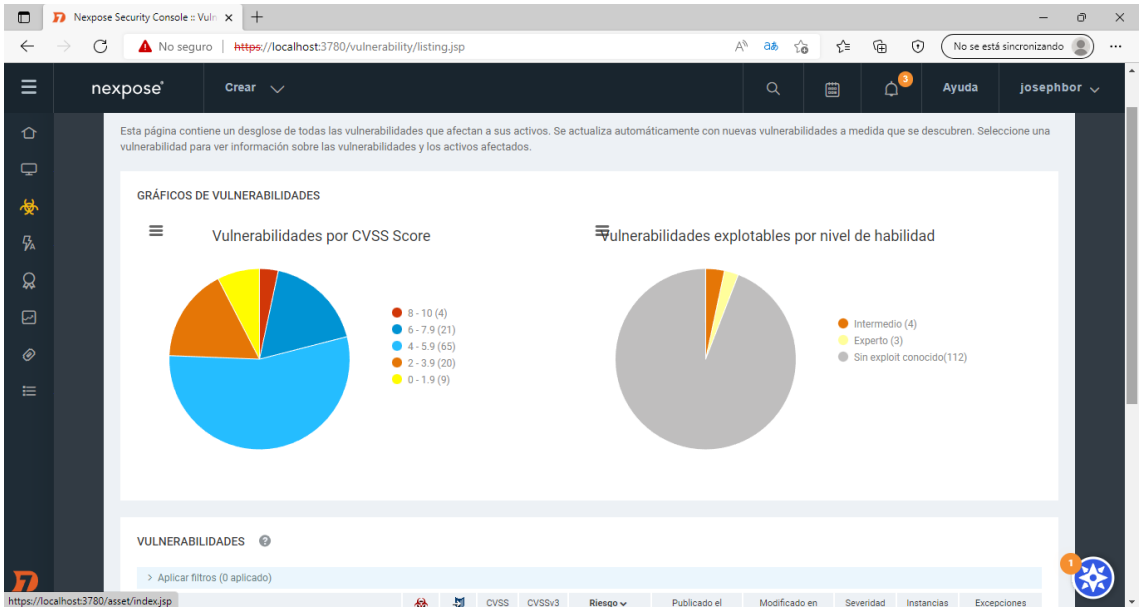
7. Nos dirigimos a “Guardar y escanear”, aceptamos y se procede con la obtención de vulnerabilidades.



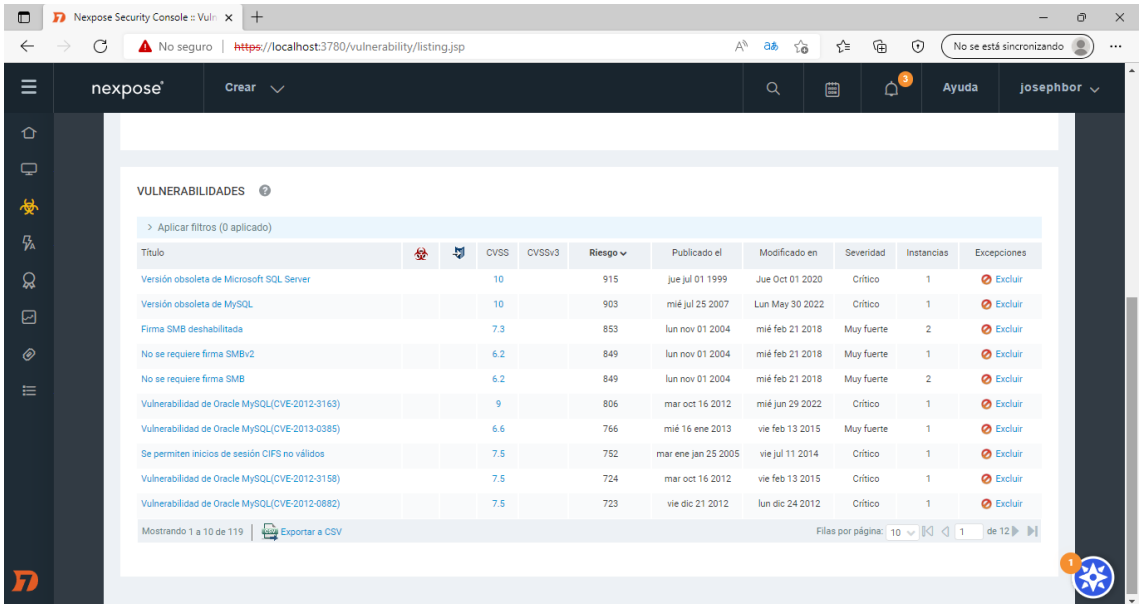
8. Luego solo nos toca esperar a que termine el proceso y obtener los resultados más precisos.



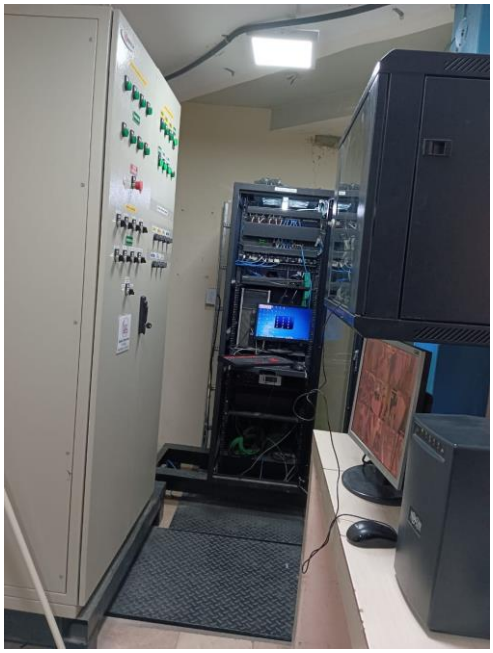
9. Cuando termine el proceso, Nexpose tiene la capacidad de mostrar en forma de estadísticas las vulnerabilidades encontradas por esta herramienta.



10. Finalmente se presentan todas las vulnerabilidades clasificándolas por nivel se severidad.



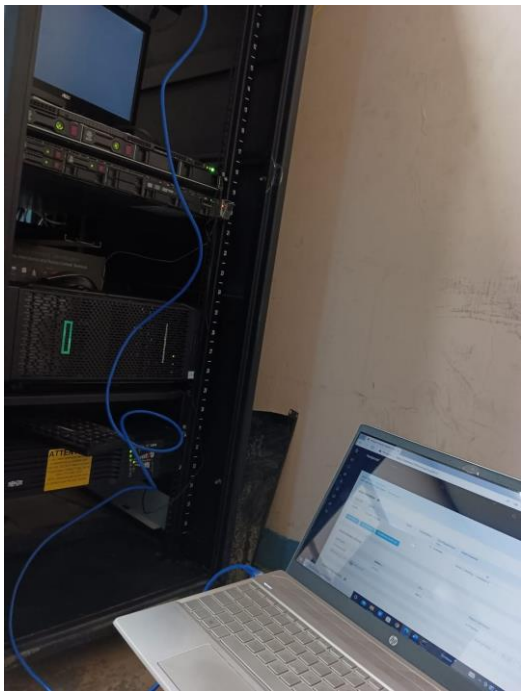
Anexo 3. Acceso al departamento de TI



Ingreso al departamento de TI

Servidor ABC Y Servidor DEF

Servidor GHI



Ejecución de herramientas

Acceso al Clúster de Servidores

COOPERATIVA
LIBERTAD PENINSULAR

CERTIFICO

Que el señor **Joseph Andres Borbor Toala**, portador de la Cédula de Ciudadanía No.2400036204, estudiante de la **Universidad Estatal Península de Santa Elena, Facultad de Sistema y Telecomunicaciones, carrera de Tecnologías de la Información**, realizó el respectivo desarrollo de una propuesta tecnológica en esta institución con el tema "ESTUDIO DE LA SEGURIDAD INFORMÁTICA EN LOS SERVIDORES DE LA COOPERATIVA DE TRANSPORTE LIBERTAD PENINSULAR", actividad que ha desempeñado a total cabalidad, cumpliendo con las políticas y reglamentos de la empresa.

El peticionario podrá hacer uso del presente documento como constancia, para anexar a la respectiva propuesta tecnológica.

Atentamente

DANNY DANIEL RIVERA GONZALEZ

Ing. Danny Rivera González
Responsable de Informática y Tecnología
Cooperativa Libertad Peninsular

COOPERATIVA DE TRANSPORTE • Fundada Jun. 28/76 •

La Libertad, 10 de Septiembre de 2021

CERTIFICADO ANTIPLAGIO

En calidad de tutora del trabajo de titulación denominado **"ESTUDIO DE LA SEGURIDAD INFORMÁTICA A LOS SERVIDORES DE UNA COOPERATIVA DE TRANSPORTE DE LA PROVINCIA DE SANTA ELENA"**, elaborado por la estudiante,**Borbor Toala Joseph Andres**, egresado de la **Carrera de Tecnologías de la Información**, de la **Facultad de Sistemas y Telecomunicaciones** de la Universidad Estatal Península de Santa Elena, previo a la obtención del título de Ingeniero en Tecnologías de la Información, me permito declarar que una vez analizado en el sistema anti plagio URKUND, luego de haber cumplido los requerimientos exigidos de valoración, elpresente proyecto ejecutado, se encuentra con 4% de la valoración permitida, por consiguiente se procede a emitir el presente informe.

Adjunto reporte de similitud.

Atentamente,

Ing. Lídice Haz López, Msi.

DOCENTE TUTORA

Reporte URKUND

Ouriginal

Document Information

Analyzed document	Documento Final - BORBOR JOSEPH-1.docx (D142636594)
Submitted	8/3/2022 7:19:00 PM
Submitted by	
Submitter email	joseph.borbor1cala@upse.edu.ec
Similarity	4%
Analysis address	lhaz.upse@analysis.urkund.com

Sources included in the report

SA	**METODOLOGÍA DE HACKING ÉTICO FARA MEJORAR LA SEGURIDAD INFORMÁTICA DE LA INFRAESTRUCTURA TECNOLÓGICA EN EL G AD PROVINCIAL DE NAPO_Chavez Victor.docx** Document METODOLOGÍA DE HACKING ÉTICO FARA MEJORAR LA SEGURIDAD INFORMÁTICA DE LA INFRAESTRUCTURA TECNOLÓGICA EN EL G AD PROVINCIAL DE NAPO_Chavez Victor.docx (D110903186)	3
SA	**Tesis Gabriel Cuadros - VFinal.pdf** Document Tesis Gabriel Cuadros - VFinal.pdf (D140322438)	1
SA	**PérezGonzálezCristian.pdf** Document PérezGonzálezCristian.pdf (D53240839)	1
SA	**Tesis_RemigioChagmana_2022.pdf** Document Tesis_RemigioChagmana_2022.pdf (D135442912)	2
SA	**TESIS MAYRA_MIRLA para urkund.docx** Document TESIS MAYRA_MIRLA para urkund.docx (D50331343)	1

BIBLIOGRAFÍA

[1] G. Baca, Introducción a la Seguridad Informática, Mexico: Grupo Editorial Patria, 2016.

[2] S. Moya, «ISA InTech,» 26 Febrero 2018. [En línea]. Available: https://www.isamex.org/intechmx/index.php/2018/02/26/los-estandares-seguridad-informatica-aplica-a-la-industria-actual/. [Último acceso: 9 Junio 2021].

[3] ESET, «Security Report,» ESET, 2021.

[4] Kaspersky, «Ciberamenaza Mapa en tiempo real,» Kaspersky, 7 Julio 2021. [En línea]. Available: https://cybermap.kaspersky.com/es. [Último acceso: 7 Julio 2021].

[5] Cooperativa Libertad Peninsular, «Cooperativa Libertad Peninsular,» 06 Octubre 2021. [En línea]. Available: https://clp.com.ec/. [Último acceso: 10 Junio 2021].

[6] J. Izquierdo y T. Tafur, «MECANISMOS DE SEGURIDAD PARA CONTRARRESTAR ATAQUES INFORMATICOS EN SERVIDORES WEB Y BASE DE DATOS,» Pimentel, 2017.

[7] A. Rosa y F. Castro, «ANÁLISIS Y DETECCIÓN DE VULNERABILIDADES EN LOS SERVIDORES PÚBLICOS DEL CENTRO DE CÓMPUTO DE LA EMPRESA INTERMEDIARIA DE VENTAS UTILIZANDO LA METODOLOGÍA INTERNACIONAL OSSTMM,» Universidad de Guayaquil Facultad de Ciencias Matemáticas y Físicas Carrera de Ingeniería en Networking y Telecomunicaciones, Guayaquil, 2015.

[8] D. Quirumbay y R. Catuto, «Análisis de amenazas y vulnerabilidades informáticas basado en la Norma ISO 27002, en el proceso de citas del servidor web de una Institución,» La Libertad: Universidad Estatal Península de Santa Elena, 2021, La Libertad, 2021.

[9] Kali, «Kali,» Kali, 16 Junio 2020. [En línea]. Available: https://www.kali.org/. [Último acceso: 16 Junio 2021].

[10] Nmpa, «Nmap.org,» Nmap, 16 Junio 2021. [En línea]. Available: https://nmap.org/. [Último acceso: 16 Junio 2021].

[11] S. Behera, «Hacking Exposed,» de *Hacking Exposed: Know the secrets of Network Security*, India, Copyright BPB Publications, 2005, p. 191.

[12] H. Rizaldos, OpenWebinars, 18 Octubre 2018. [En línea]. Available: https://openwebinars.net/blog/que-es-metasploit/. [Último acceso: 16 Junio 2022].

[13] S. Daza, «Behackerpro,» 21 Agosto 2021. [En línea]. Available: https://behacker.pro/. [Último acceso: 26 Junio 2022].

[14] Facsistel, «Facultad de Sistemas y Telecomunicaciones,» Facsistel, 29 Septiembre 2021. [En línea]. Available: http://facsistel.upse.edu.ec/index.php?option=com_content&view=article&id=58&Itemid=463. [Último acceso: 29 Junio 2022].

[15] C. Peñaherrera, «Esquema gubernamental de seguridad de la informacón EGSI,» Quito, 2013.

[16] Plan de Creación de Oportunidades, «Observatorio Regional de Planificación para el Desarrollo,» 2021. [En línea]. Available: https://observatorioplanificacion.cepal.org/sites/default/files/plan/files/Plan-de-Creaci%C3%B3n-de-Oportunidades-2021-2025-Aprobado_compressed.pdf. [Último acceso: 8 Mayo 2022].

[17] Universidad internacional de Valencia, «Viu,» Universidad internacional de Valencia, 9 Septiembre 2016. [En línea]. Available: https://www.universidadviu.com/ec/actualidad/nuestros-expertos/que-es-la-seguridad-informatica-y-como-puede-ayudarme. [Último acceso: 13 Junio 2022].

[18] M. Romero y G. Figueroa, Introducción a la seguridad informatica y el análisis de culnerabilidades, Editorial Área de Innovación y Desarrollo, S.L, 2018.

[19] Nmap Org, «Nmap.Org,» [En línea]. Available: https://nmap.org/. [Último acceso: 22 Mayo 2022].

[20] Kali, «Kali Org,» 10 Febrero 2022. [En línea]. Available: https://www.kali.org/tools/dmitry/. [Último acceso: 22 Mayo 2022].

[21] Kali, «Kali Org,» 30 Marzo 2022. [En línea]. Available: https://www.kali.org/docs/introduction/what-is-kali-linux/. [Último acceso: 23 Mayo 2022].

[22] Metasploit, «Rapid7 metasploit,» [En línea]. Available: https://www.metasploit.com/. [Último acceso: 23 Mayo 2022].

[23] D. Cunha, «Welivesecurity,» 20 Junio 2020. [En línea]. Available: https://www.welivesecurity.com/la-es/2020/06/03/nexpose-herramienta-analisis-vulnerabilidad/#:~:text=Explicamos%20qu%C3%A9%20es%20Nexpose%2C%20una,vulnerabilidades%20de%20ambientes%20y%20redes.&text=2020%20%2D%2001%3A00PM-,Explicamos%20qu%C3%A9%20es%20Nex. [Último acceso: 5 Julio 2022].

[24] W. Jiménez, «Seguridad Informática o de la Indormación en Pymes,» *Universidad Piloto de Colombia,* vol. I, pp. 3-5, 2022.

[25] G. Valenzo, «Idric,» 24 Marzo 2022. [En línea]. Available: https://www.idric.com.mx/blog-post/conoce-la-importancia-del-analisis-de-vulnerabilidad-para-una-empresa. [Último acceso: 23 Mayo 2022].

[26] Facultad de Escuela de Negocios, «Tech School Business,» 29 Septiembre 2021. [En línea]. Available: https://www.techtitute.com/ec/escuela-de-negocios/blog/hacking-etico. [Último acceso: 13 Junio 2022].

[27] Ambit Team, «Bulding Solutions Together,» 10 Noviembre 2020. [En línea]. Available: https://www.ambit-bst.com/blog/tipos-de-vulnerabilidades-y-amenazas-inform%C3%A1ticas. [Último acceso: 24 Mayo 2022].

[28] S. De la O, Promocion Social, Mexico: Escuela Nacional de trabajo Sosial, UMAM, 2000.

[29] F. L. Sánchez, Proceso de decisión del consumidor Aplicación a los planes de pensiones individuales, Madrid: ESIC EDITORIAL, 2007.

[30] L. Blanco, «Metodologías Ethical Hacking,» Universidad Mayor de San Andrés, La Paz, 2013.

[31] R. Lima, «Qué Comprende Ethical Hacking,» Universidad Mayor de San Andrés, La Paz, 2010.

[32] D. Gordon y R. Villamar, «Análisis de estrategias de gestión de seguridad informática con base en la metodología Open Source Security Testing Methodology Manual (OSSTMM) para la intranet de una Institución de Educación Superior,» *Universidad de Guadalajara,* vol. VII, nº 1, p. 2, 2018.

[33] D. Ariza, «Ethical Hacking: Una estrategia de defensa proactiva,» *Universidad Piloto de Colombia,* vol. I, nº 1, p. 11.

[34] Incibe Instituto nacional de ciberseguridad, «incibe-cert_,» NextGenerationEU, [En línea]. Available: https://www.incibe-cert.es/alerta-temprana/vulnerabilidades. [Último acceso: 25 Junio 2022].

[35] Instituto Nacional de Ciberseguridad de España, «Incibet-cert,» [En línea]. Available: https://www.incibe-cert.es/alerta-temprana/vulnerabilidades/ayuda-buscador-vulnerabilidades. [Último acceso: 6 Julio 2022].

[36] D. Franco, J. Perea y L. Tovar, «Herramientas para la Detención de vulnerabilidades basdas en la identificación de servicios,» *Scielo,* vol. XXIV, nº 5, pp. 1-16, 2013.