UNIVERSIDAD TÉCNICA DE BABAHOYO

FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA

PROCESO DE TITULACIÓN
EXAMEN COMPLEXIVO DE GRADO O DE FIN DE CARRERA

PRUEBA PRÁCTICA
PREVIO A LA OBTENCIÓN DEL TÍTULO DE:
INGENIERO EN SISTEMA DE INFORMACIÓN

TEMA:
ESTUDIO DE LA INCIDENCIA DE LAS HERRAMIENTAS DE SEGURIDAD INFORMATICA NMAP Y BURP SUITE UTILIZADAS PARA REALIZAR PENTESTING EN APLICACIONES WEB PARA LA CASA DE LA CULTURA BABAHOYO - LOS RIOS

ESTUDIANTE:
VILLACRES MORANTE MILTON ANDRES

TUTOR:
ING. CARLOS GONZALO AGUIRRE RODRIGUEZ

OCTUBRE 2023 – MARZO 2024

ÍNDICE

RESUMEN

El presente caso de estudio se centra en investigar y analizar la incidencia de dos herramientas clave en el ámbito de la seguridad informática, a saber, Nmap y Burp Suite, cuando se aplican para llevar a cabo pruebas de penetración en aplicaciones web. Este estudio se centra en lo importante que son las pruebas de penetración como un paso crítico en la evaluación de la resiliencia de las aplicaciones web frente a posibles amenazas y vulnerabilidades. Es importante comparar herramientas como Nmap y Burp Suite para ver cuál es la mejor, la más rápida y la más eficiente para realizar pruebas URL. El hacking ético es una actividad legítima que ayuda a encontrar vulnerabilidades en sistemas informáticos, redes y aplicaciones, por lo que es importante utilizar estas herramientas correctamente. Este estudio tiene aspectos tanto técnicos como prácticos de las herramientas Nmap y Burp Suite, demostrando los beneficios y limitaciones en la seguridad de las aplicaciones web, la eficacia de cada herramienta para identificar y explotar vulnerabilidades potenciales y la capacidad de proporcionar soluciones y correcciones recomendadas. Se analizarán las tendencias y desafíos actuales en la seguridad de las aplicaciones web para proporcionar un marco contextual que permita realizar una evaluación de la efectividad de Nmap y Burp Suite.

Palabras claves: aplicaciones web, vulnerabilidad, seguridad, hacking ético

SUMMARY

This case study focuses on investigating and analyzing the impact of two key tools in the field of computer security, namely Nmap and Burp Suite, when applied to perform penetration testing of web applications. This study focuses on the importance of penetration testing as a critical step in assessing the resilience of web applications against potential threats and vulnerabilities. It is important to compare tools such as Nmap and Burp Suite to see which is the best, fastest and most efficient for performing URL testing. Ethical hacking is a legitimate activity that helps to find vulnerabilities in computer systems, networks and applications, so it is important to use these tools correctly. This study has both technical and practical aspects of the Nmap and Burp Suite tools, demonstrating the benefits and limitations in securing web applications, the effectiveness of each tool in identifying and exploiting potential vulnerabilities, and the ability to provide recommended solutions and fixes. Current trends and challenges in web application security will be analyzed to provide a contextual framework for an assessment of the effectiveness of Nmap and Burp Suite.

Key words: web applications, vulnerability, security, ethical hacking.

PLANTEAMIENTO DEL PROBLEMA

Hoy en día, cuando la transformación digital impulsa las operaciones de instituciones culturales como la Casa de Cultura Babahoyo-Los Ríos, la dependencia de las aplicaciones web para la gestión de servicios se ha vuelto crítica. Sin embargo, este entorno digital también ha creado amenazas cibernéticas cada vez más sofisticadas, lo que plantea importantes desafíos a la seguridad de la información almacenada en estas aplicaciones, que a menudo incluye datos personales y sensibles.

En este contexto, las pruebas de penetración se han convertido en el método principal para evaluar la efectividad de las herramientas de seguridad informática implementadas en aplicaciones web. A pesar de los esfuerzos, estas herramientas pueden contener vulnerabilidades que pueden ser aprovechadas por actores malintencionados. Esta situación resalta la necesidad urgente de una evaluación global y constante de la eficiencia de las medidas de seguridad actuales.

La Casa de la Cultura Babahoyo-Los Ríos, la importancia de este proceso en relación con su papel como unidad cultural y educativa es obvia. Omitir una evaluación integral puede poner en peligro a la agencia, afectar la calidad de sus servicios y socavar la confianza pública. Por tanto, un análisis exhaustivo es fundamental no sólo para solucionar los problemas de seguridad actuales, sino también para predecir y prevenir vulnerabilidades futuras.

El análisis de la superficie por sí solo no es suficiente. Se deben modelar escenarios de amenazas realistas, se deben considerar los posibles vectores de ataque y se debe evaluar la efectividad de las herramientas de seguridad para detectar y evitar las intrusiones. Ver la ciberseguridad como un proceso activo y variable es esencial para garantizar que las defensas se adapten a las amenazas mutables. Una vez que se descubre una vulnerabilidad, el desarrollo oportuno de correcciones y recomendaciones específicas es primordial para fortalecer la seguridad de su aplicación web.

Esto puede incluir implementar actualizaciones de software, agregar capas adicionales de seguridad, capacitar cada cierto tiempo a los empleados en prácticas de ciberseguridad y usar tecnologías más avanzadas como la inteligencia artificial o el aprendizaje automático para mejorar la detección de amenazas.

La Casa de la Cultura Babahoyo-Los Ríos debe adoptar un enfoque fuerte y continuo en materia de ciberseguridad. Las pruebas de penetración no solo deben considerarse una evaluación única, sino también parte de un enfoque estratégico para asegurar la protección continua de la información reservada y la confiabilidad de los servicios brindados al público. Sólo a través de estas acciones podremos lograr una ciberseguridad eficaz y flexible en la era digital.

JUSTIFICACIÓN

La relevancia de la seguridad informática en el entorno digital contemporáneo no puede ser subestimada, especialmente considerando el papel fundamental que las aplicaciones web desempeñan en la vida cotidiana de individuos, organizaciones e instituciones. Estas aplicaciones actúan como portales vitales para una amplia gama de actividades, desde transacciones financieras hasta comunicaciones personales y comerciales. Sin embargo, la creciente dependencia de estas plataformas también ha exacerbado la preocupación por las vulnerabilidades inherentes que los atacantes pueden explotar con fines maliciosos.

La elección de investigar en el ámbito de la seguridad de las aplicaciones web se justifica por la imperiosa necesidad de abordar estas vulnerabilidades y salvaguardar la integridad y confidencialidad de los datos sensibles que estas aplicaciones manejan. En particular, las instituciones culturales, como La Casa de la Cultura Babahoyo-Los Ríos, se encuentran en una posición crítica, ya que gestionan una amplia variedad de información personal y sensible a través de sus plataformas en línea. Desde datos de registro de usuarios hasta información financiera y cultural, estas entidades enfrentan desafíos significativos en la protección de los activos digitales y la mitigación de los riesgos asociados con posibles brechas de seguridad.

Como entidad dedicada a la promoción de la cultura y la educación, La Casa de la Cultura Babahoyo-Los Ríos reconoce la importancia de abordar proactivamente las amenazas cibernéticas para proteger tanto su reputación como la confianza de sus usuarios. La seguridad de sus aplicaciones web no solo es una cuestión de cumplimiento normativo, sino también un imperativo ético y moral para garantizar que la información confidencial

permanezca protegida y fuera del alcance de aquellos que buscan explotarla con fines ilícitos.

En este contexto, esta investigación no solo busca identificar y analizar las vulnerabilidades existentes en las aplicaciones web utilizadas por La Casa de la Cultura Babahoyo-Los Ríos, sino también proponer estrategias efectivas de mitigación y mejores prácticas de seguridad. Al hacerlo, no solo se fortalecerá la resiliencia de la institución frente a las amenazas cibernéticas, sino que también se reafirmará su compromiso con la protección de la información confidencial y el fomento de un entorno digital seguro y confiable para todos sus usuarios y colaboradores.

OBJETIVOS

Objetivo General

- Evaluar la incidencia de las herramientas de seguridad informática Nmap y Burp Suite utilizadas para realizar pentesting en aplicaciones web para la casa de la cultura Babahoyo-Los Ríos.

Objetivos Específicos

- Evaluar la efectividad de las herramientas Nmap y Burp Suite de seguridad en pentesting.
- Identificar ventajas y desventajas de Nmap y Burp Suite para identificar vulnerabilidades de páginas web.
- Proponer mejoras y recomendaciones específicas para fortalecer la seguridad de aplicaciones web.

LÍNEAS DE INVESTIGACIÓN

Este proyecto de investigación se enlaza con las áreas de "Sistemas de información y comunicación, emprendimiento e innovación" y "Redes y tecnologías inteligentes de software y hardware". Se llevará a cabo un análisis comparativo detallado de las principales herramientas de análisis de puertos en el sistema operativo Kali Linux, como lo son Nmap y Burp Suite. Se explorará las metodologías y enfoques de seguridad informática, con énfasis en el pentesting de aplicaciones web. Supervisa la inclinación y novedades actuales en la evaluación de la ciberseguridad.

Este proyecto investiga la efectividad de herramientas de pruebas de penetración como Nmap y Burp Suite en áreas específicas como La Casa de la Cultura y también analiza el rendimiento de estas herramientas y como se adaptan a las necesidades y circunstancias de su organización.

MARCO CONCEPTUAL

Páginas web

Según Enrique (2020), desde un punto de vista conceptual, una página web puede definirse como un documento digital que contiene información electrónica dispuesta de forma estructurada y accesible en Internet. Estos archivos se crean utilizando lenguajes de marcado como HTML y CSS y se mejoran con tecnologías interactivas como JavaScript, lo que proporciona un medio eficaz para presentar y distribuir contenido en línea.

Desde un punto de vista más formal, se puede pensar en una página web como un entorno digital formado por un conjunto de contenidos estructurados (textuales y no textuales). En esta definición, un conjunto de información se presenta de forma similar y organizada en una interfaz web que incluye tanto texto como elementos multimedia, gráficos, enlaces, etc.

Aunque los inicios de Internet se remontan a la década de 1960, su llegada no condujo a su uso mundial hasta la década de 1990. En apenas unos años, la web ha evolucionado enormemente, desde páginas simples con pocas imágenes y contenido estático hasta páginas complejas con contenido dinámico provenientes de bases de datos que permitieron la creación de "aplicaciones web". En pocas palabras, una aplicación web se puede definir como una aplicación en la que un usuario, utilizando un navegador, realiza solicitudes a una aplicación remota accesible a través de Internet y recibe respuestas que se muestran en el propio navegador.

La importancia de las aplicaciones web las ha convertido en la mejor opción para el crecimiento tecnológico, la migración y la sustitución de infraestructura y servicios que requiere la organización.

El trabajo en la red comenzó en marzo de 1999, cuando Tim Berner Lee, del Laboratorio Europeo de Física, propuso un proyecto para intercambiar información y transferir investigaciones e ideas en toda la organización. Actualmente, el laboratorio comparte proyectos

web con el MIT. Un error común es creer que Internet y la World Wide Web son lo mismo. No lo es, Internet es infraestructura: es el medio físico utilizado para transferir datos. Internet es un conjunto de protocolos y estándares para acceder a datos disponibles en internet.

Específicamente la Web es definida por tres estándares:

- URI (Uniform Resource Identifiers): un método para aclarar la localización de un recurso en internet.
- HTTP (Hyper Text Transfer Protocol): una normativa para transferir información fundada en hipertexto en la Internet.
- HTML (Hyper Text Markup Language): un lenguaje de intercambio para hipertexto en la Web. (Roselia, 2021)

Seguridad de páginas web

Haciendo énfasis a lo que dice Palacios (2020), no cabe duda de que la seguridad de los sistemas informáticos de cualquier organización se ha convertido en uno de los pilares más sensibles y vulnerables, siendo importante encontrar mecanismos para fortalecer la seguridad. Los planes de seguridad se convierten en una herramienta imprescindible para el procesamiento de la información, el desarrollo de recursos técnicos y el desarrollo de nuevas aplicaciones y tecnologías para la implantación de sistemas más avanzados.

La proliferación de aplicaciones, servidores remotos, nubes, el rápido desarrollo de los sistemas operativos y el consumo de cualquier tipo de software como servicio en dispositivos cada vez más vulnerables afecta al uso de las tecnologías de la información y a la sociedad de la comunicación. Abre un universo de estrategias altamente maliciosas que pueden destruir cualquier organización.

La falta de seguridad puede deberse a la falta de conocimiento de posibles amenazas o de medidas de seguridad para mitigarlas. Necesita saber qué proteger, qué prevenir y cómo

protegerse. Los elementos protegidos incluyen datos, software, hardware y consumibles. Una herramienta importante es el inventario. Debe recoger toda la información necesaria sobre los distintos activos de la organización. Estos activos son frágiles a varios tipos de ataques, como escuchas o interceptaciones, escuchas o monitoreo, falsificación de identidad y ataques de denegación de servicio.

La seguridad se puede dividir, a grandes rasgos, en seguridad física y seguridad lógica. La seguridad física hace referencia a la protección de la organización frente a accesos no autorizados y ataques físicos a los equipos e instalaciones. La seguridad lógica aplica mecanismos y barreras que protegen la información desde su propio medio. Algunos de los mecanismos más usados son:

La seguridad física consiste en proteger una organización contra el acceso no autorizado y los ataques físicos a sus equipos e instalaciones. La protección lógica utiliza métodos y barreras para proteger la información por sus propios méritos. Los mecanismos usados más utilizados son:

- Limitar el acceso a determinados programas o ficheros mediante el uso de cifrado o mediante claves.
- Otorgar los privilegios mínimos y necesarios a todos los usuarios del sistema, evitando dar permisos de más.
- Aplicar una gestión de la explotación del software eficiente por parte de los usuarios del sistema.
- Controlar que información entra y sale del sistema de información, y gestionar eficientemente la autorización de los usuarios para tales efectos.

Como señala Antonio (2020), los tres pilares de la seguridad de la información corresponden a los requisitos de confidencialidad, de integridad y de disponibilidad.

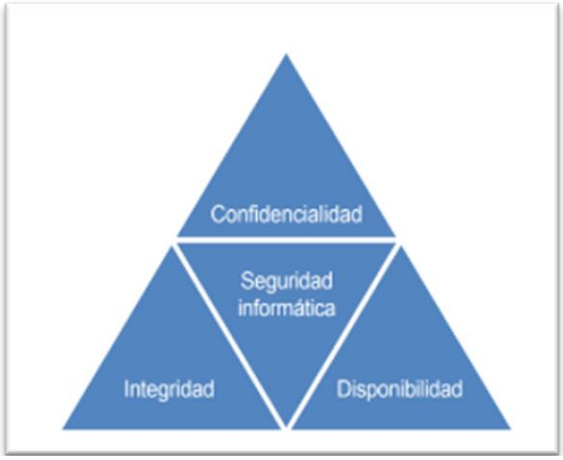


Figura 1: Pilares de la seguridad de información
Fuente: Paraninfo

Vulnerabilidades en páginas web

Para Lodeiro (2022), la seguridad de los sistemas informáticos de cualquier organización se ha convertido en uno de los pilares más sensibles y vulnerables, por lo que es importante buscar mecanismos para fortalecer la seguridad. Los planes de seguridad se convierten en una importante herramienta para procesar información, desarrollar recursos técnicos y desarrollar nuevas aplicaciones y tecnologías para implementar sistemas más avanzados.

La proliferación de aplicaciones, servidores remotos, nubes, el rápido desarrollo de los sistemas operativos y el uso de software como cualquier tipo de servicio en dispositivos cada vez más vulnerables afecta al uso de las tecnologías de la información y las comunicaciones en la sociedad. Esto abre una serie de tácticas altamente maliciosas que pueden destruir cualquier organización.

La falta de seguridad puede deberse a la falta de conocimiento de posibles amenazas o de medidas de seguridad para mitigarlas. Necesita saber qué proteger, qué prevenir y cómo protegerse. Los elementos protegidos incluyen datos, software, hardware y consumibles. Una

herramienta importante es el inventario. Debe recopilar toda la información necesaria sobre los distintos activos de la organización. Estos activos son vulnerables a varios tipos de ataques, como escuchas o interceptaciones, escuchas o monitoreo, suplantación de identidad o suplantación de identidad y ataques de denegación de servicio o denegación de servicio.

Estas son algunas de las vulnerabilidades más comunes que los desarrolladores y profesionales de seguridad deben tener en cuenta:

- **Inyección de código SQL**: se define como un ataque que se lleva a cabo en una aplicación web. El atacante ingresa código SQL en un cuadro de entrada (formulario web) para obtener acceso ilegal a la aplicación. (Cesar, 2023)

- **Ataques XXC**: La primordial preocupación de XSS es que las debilidades que permiten que tales ataques ocurran son frecuentes y se presentan siempre que una aplicación web utiliza información de un usuario dentro de la salida que genera sin validarla ni codificarla. Por lo tanto, un ciberdelincuente puede utilizar XSS para enviar un script malicioso a un usuario desprevenido. (Al-Haija, 2023)

- **Vulnerabilidades en autenticación:** contraseñas frágiles, falta de bloqueo de cuentas después de intentos inválidos, y manejo inseguro de sesiones pueden dar paso a compromisos de cuentas.

- **Inclusión de Archivos:** permite la inclusión de archivos locales o remotos, lo que puede dar lugar a la ejecución de código arbitrario o la exposición de información delicada.

- **Secuencias de Comandos del Lado del Servidor:** congiguraciones erróneas del servidor o la ejecución de scripts pueden abrir brechas para que los atacantes puedan ejecutar código en el servidor.

Escaneo de puertos

Desde el punto de vista de Andrés y Rico (2020), la mejor forma de prepararse ante posibles ataques es analizar la infraestructura de su empresa realizando pruebas de seguridad. Pasando el tema a un entorno más técnico y refiriéndonos a la configuración del dispositivo, podemos identificar brechas de seguridad mediante análisis periódicos de vulnerabilidad. Por lo tanto, las agencias y organizaciones deben implementar los siguientes controles para garantizar la confidencialidad, integridad y disponibilidad de su información.

La seguridad de la información es el factor más importante a considerar al implementar una red o sistema de datos. La información es el eje central sobre el que operan las instituciones y organizaciones, y un análisis adecuado permite a estas entidades comprender el comportamiento de sus empresas. Al realizar pruebas de laboratorio en un entorno controlado y utilizar técnicas de prueba de penetración, podemos realizar análisis de vulnerabilidad sin comprometer ningún sistema real.

Según Martínez (2023), el escaneo de puertos es un método de prueba que detecta qué servicios brinda la red o servidor analizando la conexión o intentando conectarse a otro puerto (TCP o UDP) de la víctima y espera solicitudes de ese puerto.

Al escuchar en un puerto específico, todo esto se hace mediante un método de ataque que consta de seis fases: reconocimiento, escaneo, inventario, explotación, mantenimiento del acceso y eliminación, organizadas de tal manera que garanticen el éxito de una sola fase. La mejor solución para la siguiente fase. Las herramientas, métodos y tiempo para completar cada tarea son muy importantes.

La fase de escaneo tiene cuatro objetivos principales que son detectar hosts activos, puertos abiertos, versiones de aplicaciones, sistemas operativos y otras vulnerabilidades de la red durante un ataque, por lo que se recomienda utilizar un sistema de agente móvil para

enriquecer el proceso de escaneo. Las puertas de enlace son principalmente sistemas heterogéneos que permiten crear, interpretar, ejecutar, reenviar y terminar agentes.

Hacking Ético

De acuerdo con Miguel (2023), el hacking ético es una rama de la seguridad técnica que tiene como objetivo prevenir, impedir, estabilizar y neutralizar vulnerabilidades en el software o hardware. Para ello es necesario tener conocimientos de redes, administración de servidores y sus respectivos servicios. La piratería ética se produce cuando una persona utiliza sus conocimientos informáticos para encontrar fallos, errores o vulnerabilidades.

En la actualidad hay aproximadamente 5.160 millones de usuarios de Internet, lo que representa el 64,4% de la población mundial. En este mundo digital, es importante proteger la información personal y garantizar la seguridad de la red. Los ejercicios de pruebas de penetración se han convertido en una práctica común en la industria de la seguridad cibernética a medida que las empresas se centran cada vez más en proteger sus sistemas y datos contra posibles ataques cibercriminales.

Para Eduardo (2020), a lo largo de los años, los llamados "hackers éticos" han tenido seguidores y detractores. Básicamente es una combinación de estas dos palabras: moral (que significa lo que es correcto y bueno) y hacker (que significa lo contrario). El descuido del hacking ético es uno de los principales contribuyentes a este problema.

Los piratas informáticos éticos irrumpen en los sistemas informáticos no para robar o cambiar información, sino para descubrir vulnerabilidades y vulnerabilidades. También se le llama prueba de penetración o prueba de penetración, es decir es "el arte de buscar vulnerabilidades de seguridad en una organización y luego publicar las vulnerabilidades de seguridad descubiertas y mitigarlas tanto como sea posible con un informe. Manténgalo lo más breve posible y evite filtraciones de datos y ataques informáticos".

Una persona que realiza pruebas de penetración o pruebas de pentesting se llama pentester. Este rol está relacionado con las necesidades y problemas de la organización. Por consiguiente, los exámenes de acceso son diferentes y el éxito depende de las habilidades y experiencia del candidato.

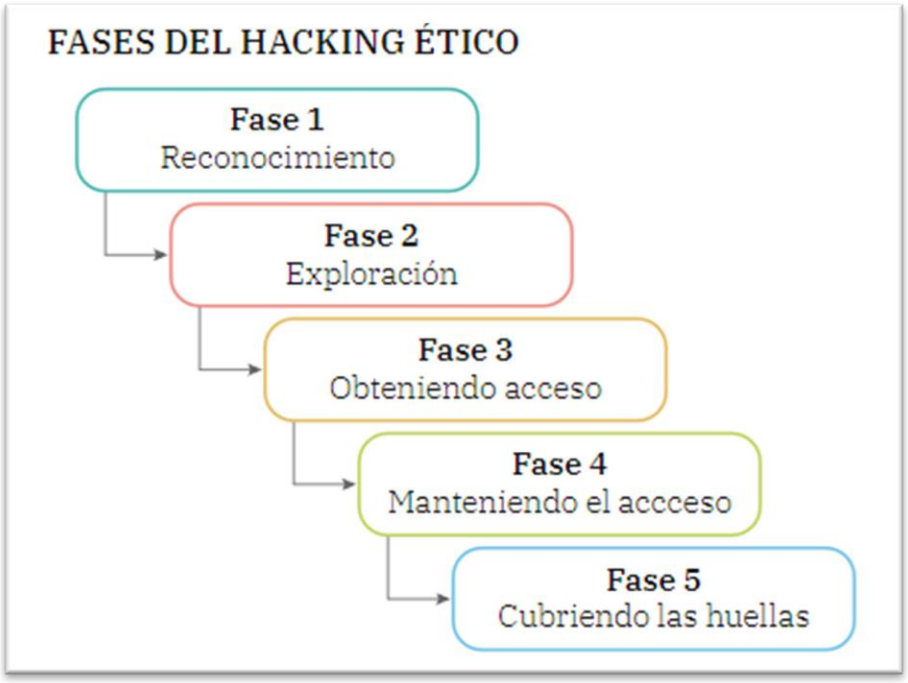


Figura 2: Fases del hacking ético
Fuente: Sena

De acuerdo con Roger (2022) estos son los tipos de hacking ético:

- Pruebas de penetración programadas: se analizan las debilidades del sistema.
- Pruebas de penetración no estructuradas: analiza todos los aspectos del sistema de información.
- Pruebas de penetración ciegas: abiertas y disponibles para cualquier organización.
- Pruebas de penetración informadas: De carácter confidencial y cuentan con derechos de acceso especiales otorgados por su institución.

- Pruebas de penetración externas: Realizado en la empresa con el objetivo de analizar la política y los mecanismos externos.
- Pruebas de penetración internas: Realizado en la empresa con el objetivo de analizar la política y los mecanismos externos.
-

Herramientas de escaneo de puertos

Nmap

Teniendo en cuenta a Gustavo y Yeiny (2022), NMAP detecta puertos y sistemas operativos a nivel de punto final, lo que permite que nuestras pruebas nos proporcionen análisis de vulnerabilidades. A través de este desarrollo podemos detectar e identificar vulnerabilidades en redes, sitios web y aplicaciones actualmente en uso. NMAP (Network Mapper) se ha convertido en una herramienta imprescindible para los profesionales de la seguridad informática y los administradores de sistemas porque proporciona capacidades avanzadas de escaneo de red a nivel de punto final.

Este software de código abierto detecta puertos y sistemas operativos abiertos en la red y otorga una vista minuciosa de la topología e infraestructura de la red de destino. Una de las primordiales ventajas de NMAP es su capacidad de realizar un escaneo completo, por lo que podemos ver no sólo los puertos abiertos, sino también los tipos de servicios en los puertos. Utiliza tecnologías avanzadas para comprender los sistemas operativos de los dispositivos de red. Este conocimiento integral proporciona a los profesionales de la seguridad una base sólida para realizar evaluaciones de vulnerabilidad.

El uso de NMAP en pruebas de seguridad nos brinda una comprensión completa de la superficie de ataque de la red. El escaneo de puertos nos ayuda a identificar servicios y aplicaciones en ejecución, mientras que la detección del sistema operativo proporciona

información valiosa sobre posibles vulnerabilidades de la plataforma. Este enfoque integral permite a los expertos abordar las vulnerabilidades de manera más efectiva. En sitios web y entornos de aplicaciones, NMAP también puede desempeñar un papel importante en el descubrimiento de puertos abiertos y la ejecución de servicios web. Esta propiedad es esencial para evaluar la seguridad de las aplicaciones web y garantizar que no haya puntos de acceso innecesarios o servicios mal configurados que puedan suponer un riesgo para la seguridad.

Otra característica importante de NMAP es su capacidad para realizar comprobaciones de vulnerabilidad independientes. Al acoplar este análisis con la información recopilada sobre puertos y sistemas operativos permite una evaluación precisa de las vulnerabilidades de la red. La identificación temprana de vulnerabilidades críticas permite a los equipos de seguridad tomar medidas correctivas antes de que actores malintencionados las puedan explotar.

Haciendo referencia a Martínez (2023), debido a que Nmap utiliza paquetes IP sin procesar, proporciona nuevas formas de determinar los hosts disponibles en la red o los servicios proporcionados por esos hosts, el sistema operativo y la versión del sistema operativo, el tipo de filtro de paquetes utilizado, etc., por esta razón es importante aclarar que es capaz de escanear redes grandes rápidamente y puede apuntar bien a hosts específicos.

Escaneo de una web nmap	www.google.com
Escaneo de un rango de IPs nmap	192.168.0.1-100
Escanear toda una subnet nmap	192.168.0.1/24
Escáner desde un fichero de texto nmap	-iL fichero.txt
Escanear un rango de puertos nmap	-p 201-300 192.168.0.1
Escanear los puertos más utilizados nmap	-F 192.168.0.1
Escanear los 65535 puertos	-p 192.168.0.1

Figura 3: Principales usos de Nmap
Fuente: Valencia 2023

Burp Suite

La herramienta Burp Suite Professional de seguridad web puede buscar las 10 vulnerabilidades principales de OWASP (Open Web Application Security Project). Es capaz de realizar análisis pasivos y activos Ofrece una perspectiva de análisis dual, esto debido a que puede llevar a cabo análisis tanto pasivos como activos.

El análisis pasivo significa observar y catalogar interacciones entre navegadores y aplicaciones web sin relación directa.

Por otro lado, el análisis proactivo implica solicitudes y acciones proactivas para evaluar la resistencia de la aplicación frente a posibles ataques. Esta capacidad de combinar escaneo pasivo y activo permite una evaluación un poco más completa de la seguridad de las aplicaciones web. Una de las características distintivas de Burp Suite Professional es su potente proxy/historial, que permite a los evaluadores de penetración modificar las comunicaciones HTTPS seguras a través de un navegador. Lo que es esencial para reonocer y dar remedio a vulnerabilidades en aplicaciones web que utilizan cifrado HTTPS.

La capacidad de manejar de forma segura estas comunicaciones facilita la identificación de vulnerabilidades potenciales y la evaluación de la fortaleza de una aplicación a las amenazas de seguridad. Aparte de las funciones de proxy, Burp Suite incluye otras herramientas y módulos especializados, como Security Scanner, que tecnifica el proceso de reconocimiento de vulnerabilidades, e Intruder, que concede ataques personalizados para evaluar la resistencia de la aplicación a diversos escenarios. Otra característica distinguida es la interfaz de usuario instintiva y fácil de usar otorgada por Burp Suite. Simplifica el proceso de prueba de penetración, facilitando a los profesionales de la seguridad explorar las distintas funciones y así poder dar un análisis a los resultados.

Según Saxena (2022), Burp Suite Professional es una herramienta imprescindible para

cualquier profesional de la ciberseguridad. Su capacidad para abordar vulnerabilidades clave de OWASP, realizar escaneos pasivos y activos y modificar comunicaciones seguras utilizando su poderoso proxy/historial lo convierte en un recurso confiable para proteger aplicaciones web en un entorno cada vez más comprometido.

Como señalan Albahar & Alansari (2022), capacidad de automatizar total o parcialmente el escaneo. Tiene menos vulnerabilidades de falsos positivos y mayores capacidades de detección de verdaderos positivos.

MARCO METODOLÓGICO

Se utilizará una combinación de métodos de investigación exploratorios y descriptivos para realizar un análisis técnico comparativo de las herramientas de escaneo de puertos en la web. Esta decisión metodológica se basó en la necesidad urgente de realizar una revisión exhaustiva de una amplia gama de fuentes de información relevantes para este campo en particular. Este proceso de revisión detallado incluirá el estudio de trabajos de investigación anteriores, revisión de libros de texto para obtener una base teórica sólida, revisión crítica de artículos de revistas académicas relevantes para mantenerse al día con los últimos desarrollos y análisis detallado para proporcionar un estudio de caso práctico y contextual de una perspectiva cultural.

La elección de un método de investigación proporcionará información acerca de la cantidad de información existente, lo que permitirá un análisis más detallado y completo del entorno de seguridad de red actual para aplicaciones web que usan herramientas de escaneo de puertos como Nmap y Burp Suite.

Además, la implementación de un enfoque descriptivo va a otorgar una estructura sólida para la recopilación y posterior presentación de datos detallados sobre los factores técnicos, el rendimiento y la aplicación práctica de estas herramientas.

La integración conjunta de estas perspectivas se propone llegar a una visión integral y rigurosa para el análisis comparativo de las herramientas de escaneo portuario, que aborde no sólo su funcionalidad básica, sino que también logre evaluar su efectividad en diferentes contextos y escenas.

RESULTADOS

Nmap se destaca por realizar escaneos de puertos completos y brindar información de servicio detallada. Sin embargo, se debe considerar el tráfico de red que genera y la posibilidad de detección por parte de sistemas de prevención de intrusiones. Nmap es conocido por la capacidad que tiene para descubrir sistemas remotos, aunque su precisión se puede ver afectada por configuraciones de seguridad avanzadas. Al contrario, Burp Suite se enfoca en la seguridad de las aplicaciones web, centrándose en descubrir y explotar vulnerabilidades de ese entorno. Sus herramientas son capaces de interceptar y modificar el tráfico entre navegadores y aplicaciones web, lo que facilita una evaluación de seguridad exhaustiva en estas situaciones. A pesar de que su enfoque específico puede limitar su utilidad para un análisis de red más amplio, la interfaz gráfica intuitiva de Burp Suite facilita la navegación y el análisis de los resultados, esto la convierte en una herramienta más fácil de usar para usuarios menos capacitados en cuestión de las interfaces de línea de comandos.

Nmap se destaca por realizar escaneos de puertos completos y brindar información de servicio detallada. Sin embargo, se debe considerar el tráfico de red que genera y la posibilidad de detección por parte de sistemas de prevención de intrusiones.

Sus herramientas son capaces de interceptar y modificar el tráfico entre navegadores y aplicaciones web, lo que facilita una evaluación de seguridad exhaustiva en estas situaciones. A pesar de que su enfoque específico puede limitar su utilidad para un análisis de red más amplio, la interfaz gráfica intuitiva de Burp Suite facilita la navegación y el análisis de los resultados, esto la convierte en una herramienta más fácil de usar para usuarios menos capacitados en cuestión de las interfaces de línea de comandos.

Tabla 1: Ventajas y Desventajas de Nmap y Burp Suite

Herramienta	**Nmap**	**Burp Suite**
Función principal	Escaneo de puertos y descubrimiento de redes	Suite de pruebas de penetración web
Ventajas	▪ Rápido y eficiente ▪ Una amplia gama de tipos de escaneo ▪ Detecta vulnerabilidades comunes ▪ De código abierto	• Interfaz de grafico de usuario intuitiva • Una amplia gama de herramientas para realizar pentesting • Soporte para diferentes tipos de aplicativos webs • Versiones gratuitas y de pago
Desventajas	▪ Puede resultar difícil para un principiante usar su interfaz de línea de comandos ▪ No es tan completo como Burp para realizar pentesting	• En ocasiones puede tornarse lento para escanear redes grandes • Se requiere de más conocimiento técnico en comparación con Nmap
Recomendación	Usarlo para realizar escaneo de redes y descubrimiento de hosts	Es mejor usarlo para pruebas de penetración web
Costo	Gratuito	Gratuito en su versión limitada y de pago en su versión completa

La naturaleza de código abierto de Nmap permite una mayor flexibilidad a este respecto al considerar la integración con otras herramientas y scripts. Burp Suite, por otro lado, sobresale en sus capacidades de integración, pero su orientación más específica a aplicaciones web puede limitar su eficacia en escenarios web más amplios. La elección entre estas herramientas

dependerá de los objetivos específicos del estudio, el alcance del análisis y las preferencias de los usuarios. En muchos casos, la combinación de Nmap y Burp Suite puede proporcionar un enfoque integral que aprovecha las fortalezas respectivas de cada herramienta para lograr resultados de pruebas de penetración más completos y precisos. Es importante considerar la versatilidad de estas herramientas, ya que Nmap puede adaptarse a diferentes entornos y escenarios de red, mientras que Burp Suite está diseñado específicamente para abordar vulnerabilidades relacionadas con aplicaciones web, lo que demuestra su experiencia en esta área en particular.

DISCUSIÓN DE RESULTADOS

La evaluación comparativa detallada de herramientas de escaneo de puertos como Nmap y Burp Suite se caracteriza por la capacidad de proporcionar resultados precisos y comprensibles que se alinean efectivamente con los conceptos previamente descritos en el marco conceptual. El examen de los resultados obtenidos reveló diversos conceptos, superposiciones y diferencias significativas que permiten una comprensión más profunda de la efectividad y aplicabilidad de estas herramientas en el contexto de las pruebas de penetración de aplicaciones web de La Casa de la Cultura Babahoyo-Los Ríos.

Uno de los hallazgos notables de esta evaluación fue la confirmación de la importancia crítica de la velocidad de escaneo al evaluar estas herramientas de seguridad de red. Tal y como está previsto en el marco conceptual, este aspecto crítico se identifica como un punto clave para la detección inmediata de potenciales vulnerabilidades. La capacidad de escanear de forma rápida y eficiente se considera un componente importante para garantizar una respuesta ágil y eficaz ante cualquier signo sospechoso. De esta manera, la investigación asume la hipótesis subyacente de que la velocidad de escaneo juega un papel muy importante en la identificación temprana de amenazas y la seguridad dinámica de la red. Estos resultados no sólo fortalecen las bases teóricas de la arquitectura conceptual, sino que también brindan una dimensión práctica y aplicada para comprender la utilidad de las herramientas analizadas en el campo específico de la Casa de la Cultura Babahoyo-Los Ríos.

En cuanto a la precisión del descubrimiento de servicios, los resultados obtenidos al comparar Nmap y Burp Suite son totalmente consistentes con las expectativas descritas en la arquitectura conceptual. Este hallazgo en particular vuelve a enfatizar la notable efectividad de Nmap, ya que muestra una tasa de detección más alta en comparación con Burp Suite.

La ubicación precisa de Nmap es lo primordial para identificar de forma precisa y completa los servicios en su red. La importancia de esta eficacia en el descubrimiento de

servicios, se refleja en la necesidad de identificar los componentes de la red con precisión y detalle. Esto en particular es importante para las pruebas de penetración, donde la detección precisa se transforma en la base para una detección eficaz de vulnerabilidades. Nmap logra esta tarea de una forma eficiente e integral, otorgando una base sólida para una mayor evaluación y reducción de riesgos, dando facilidad a la toma de decisiones informadas para mejorar la ciberseguridad.

A pesar de los resultados positivos en términos de eficacia y precisión, persisten incertidumbres en relación con el aspecto de facilidad de uso y la diversidad de funcionalidades, una dimensión que fue destacada en el marco conceptual. Aunque Nmap sobresale en términos de funcionalidades avanzadas y capacidades analíticas, los hallazgos revelan una tendencia hacia la complejidad, especialmente para usuarios con poca experiencia en el campo de la seguridad informática.

Como se enfatiza en el marco conceptual, la facilidad de uso y la accesibilidad son factores clave ya que afectan directamente el uso y la eficacia de las herramientas analíticas. Nmap ofrece muchas funciones, pero la curva de aprendizaje puede ser alta para quienes no tienen experiencia en seguridad de redes.

Explorar soluciones que equilibren las capacidades analíticas y la accesibilidad es fundamental para garantizar un uso más amplio y eficaz de la herramienta, especialmente en entornos donde la formación y el conocimiento en ciberseguridad pueden variar ampliamente entre los usuarios. Este aspecto muestra que, si bien Nmap puede ser una herramienta poderosa, su utilidad real puede depender de la experiencia y las habilidades técnicas de la persona que la implementa.

CONCLUSIONES

La evaluación muestra que Nmap destaca por su precisión en el descubrimiento de servicios y cumple con las expectativas definidas en el marco conceptual. Sin embargo, las preocupaciones sobre la facilidad de uso y la complejidad asociada, especialmente para usuarios con experiencia limitada, requieren una consideración cuidadosa de la efectividad de la herramienta en contextos donde la accesibilidad es crítica. Burp Suite es una herramienta diseñada específicamente para la seguridad de aplicaciones web, destacando su eficacia a la hora de identificar vulnerabilidades en contextos específicos. Su intuitiva interfaz gráfica facilita la navegación y el análisis de los resultados, haciéndolo más accesible para aquellos menos familiarizados con la seguridad informática.

Utilizando Nmap, se descubrieron varias vulnerabilidades en la aplicación web de La Casa da Cultura Babahoyo-Los Ríos, lo que confirma la precisión de las pruebas de penetración en la identificación de áreas de vulnerabilidad potencial. La combinación de estas dos herramientas proporciona una descripción general completa de las amenazas y vulnerabilidades y proporciona una base sólida para los pasos posteriores del proceso. Se recomienda considerar solicitudes híbridas basadas en recomendaciones y sugerencias de mejora. Esta es una estrategia que utiliza las capacidades respectivas de Nmap y Burp Suite.

Aprovecha las capacidades de Nmap en análisis de redes a gran escala y la experiencia de Burp Suite en seguridad de aplicaciones web para proporcionar un enfoque integral y equilibrado. También destaca la importancia de proporcionar al personal formación específica para utilizar eficazmente estas herramientas y superar obstáculos difíciles.

RECOMENDACIONES

Si necesita un análisis extenso y preciso para la evaluación de la red, se recomienda Nmap. Gracias a su excelente precisión en la detección de servicios, Nmap se posiciona como la herramienta preferida para mapear la infraestructura de red y descubrir vulnerabilidades potenciales. Para proporcionar un análisis de vulnerabilidad más completo y específico de aplicaciones web específicas, se recomienda incluir Burp Suite en el proceso de prueba de penetración. Centrándose en la seguridad de las aplicaciones web, Burp Suite destaca por su eficacia a la hora de identificar posibles debilidades y vulnerabilidades en este ámbito concreto. La interfaz gráfica intuitiva permite una fácil navegación y análisis de resultados incluso para personas con pocos conocimientos técnicos.

Se destacó la importancia de establecer sistemas para el seguimiento continuo de los resultados de esta estrategia. Los comentarios de los empleados y los procesos de revisión periódica le ayudarán a realizar los ajustes necesarios y garantizarán su adaptación a nuevas amenazas y problemas de seguridad a medida que surjan en su entorno.

Se enfatizó que es muy importante brindar capacitación especializada a los responsables de realizar pruebas de penetración. Esto incluirá sesiones detalladas sobre el uso adecuado de Nmap y Burp Suite, asegurando así que el personal esté en condiciones de conocimiento necesario para utilizar plenamente las virtudes de estas herramientas sin interrupciones y sea capaz de superar posibles obstáculos de complejidad.

REFERENCIAS

Albahar, M., Alansari, D., & Jurcut, A. (2022). *Comparación empírica de herramientas de prueba de penetración para detectar vulnerabilidades de aplicaciones web.* Obtenido de https://www.mdpi.com/2079-9292/11/19/2991

Al-Haija, A. (Septiembre de 2023). *ScienceDirect.* Obtenido de https://www.sciencedirect.com/science/article/pii/S2590123023003936

Andres, O. J., & Rico, B. D. (20 de Mayo de 2020). *Risti (Revista Iberica de Tecnologias e Informacion).* Obtenido de https://www.researchgate.net/profile/Dewar-Rico-Bautista/publication/340618632_A_practical_guide_to_analyzing_vulnerabilities_in_a_GNULinux_client-server_environment_using_a_pentesting_methodology/links/5e9529b3299bf13079979529/A-practical-guide-to-analyz

Antonio, P. P. (31 de Marzo de 2020). *Seguridad Informatica.* Obtenido de https://books.google.es/books?hl=es&lr=&id=UCjnDwAAQBAJ&oi=fnd&pg=PR5&dq=Seguridad+de+paginas+web+2020&ots=-IU1hq8Yh8&sig=FP9LCibf6Y-6d3llotpsIkNJ-fw#v=onepage&q&f=false

Cesar, A. (Julio de 2023). *Uso de Técnicas de Minería de Datos para la Detección de Ataques de Inyección de SQL en Sistemas de Bases de Datos.* Obtenido de http://scielo.senescyt.gob.ec/scielo.php?script=sci_arttext&pid=S1390-01292023000200019

Eduardo, R. L. (12 de Enero de 2020). *Herramientas fundamentales para el hacking etico.* Obtenido de https://www.medigraphic.com/pdfs/revcubinfmed/cim-2020/cim201j.pdf

Enrique, F. P. (Octubre de 2020). *Diseño y construccion de paginas web.* Obtenido de https://books.google.es/books?hl=es&lr=&id=AdC4EAAAQBAJ&oi=fnd&pg=PT65&dq=paginas+web+2020&ots=fiZ0r9rdZu&sig=lCXA-

gzwDJhZSsF36qX4g7ptgjk#v=onepage&q&f=false

Lodeiro, E. G. (21 de Junio de 2022). *ANÁLISIS DE VULNERABILIDADES DE PAGINAS WEB.* Obtenido de https://upcommons.upc.edu/bitstream/handle/2117/373338/171264.pdf?sequence=1&isAllowed=y

M, A., & N, S. (22 de Junio de 2022). *Evaluación de escáneres de seguridad de aplicaciones web Black-Box para detectar vulnerabilidades de inyección.* Obtenido de https://www.mdpi.com/2079-9292/11/13/2049

Martinez, G. V. (Octubre de 2023). *Análisis técnico comparativo de herramientas de escaneo de puertos de redes de telecomunicaciones.* Obtenido de http://dspace.utb.edu.ec/bitstream/handle/49000/15074/E-UTB-FAFI-SIST.INF-000201.pdf?sequence=1&isAllowed=y

Miguel, M. J. (13 de Junio de 2023). *Estudio y análisis del anonimato en la red.* Obtenido de https://openaccess.uoc.edu/bitstream/10609/148149/1/amantillaTFG0623memoria.pdf

Quezada, S., Alban, C., & Lopez, P. (Febrero de 2023). *Factores de riesgo, amenazas, vulnerabilidades y defensa en aplicaciones web turisticas.* Obtenido de https://www.proquest.com/openview/0d6c5600ad7df199b04e448d071cd4be/1?pq-origsite=gscholar&cbl=1006393

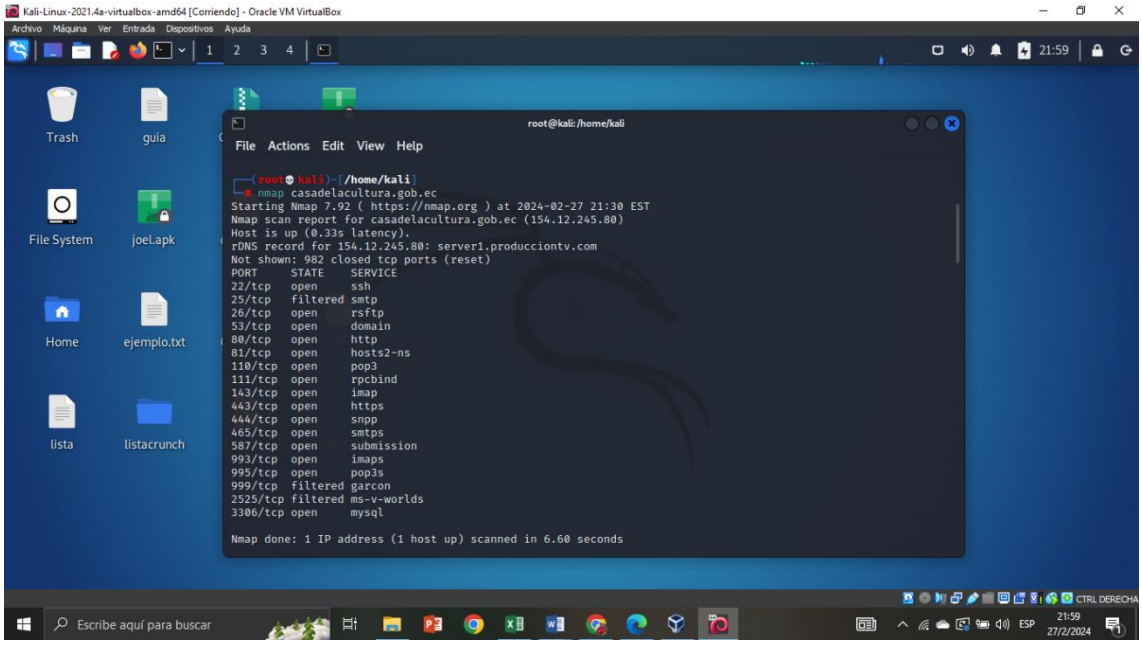
Roger, P. H. (2022). *TÉCNICAS DE HACKING ÉTICO.* Obtenido de https://repositorio.uss.edu.pe/bitstream/handle/20.500.12802/9377/Pi%c3%b1ashca%20Huerta%20Roger%20Jhoel.pdf?sequence=1&isAllowed=y

Roselia, P. L. (31 de Mayo de 2021). *Revista Brasileira de Ergonomia.* Obtenido de https://www.revistaacaoergonomica.org/article/627d7dbba9539512dd3e22e4/pdf/abergo-2-2-3.pdf

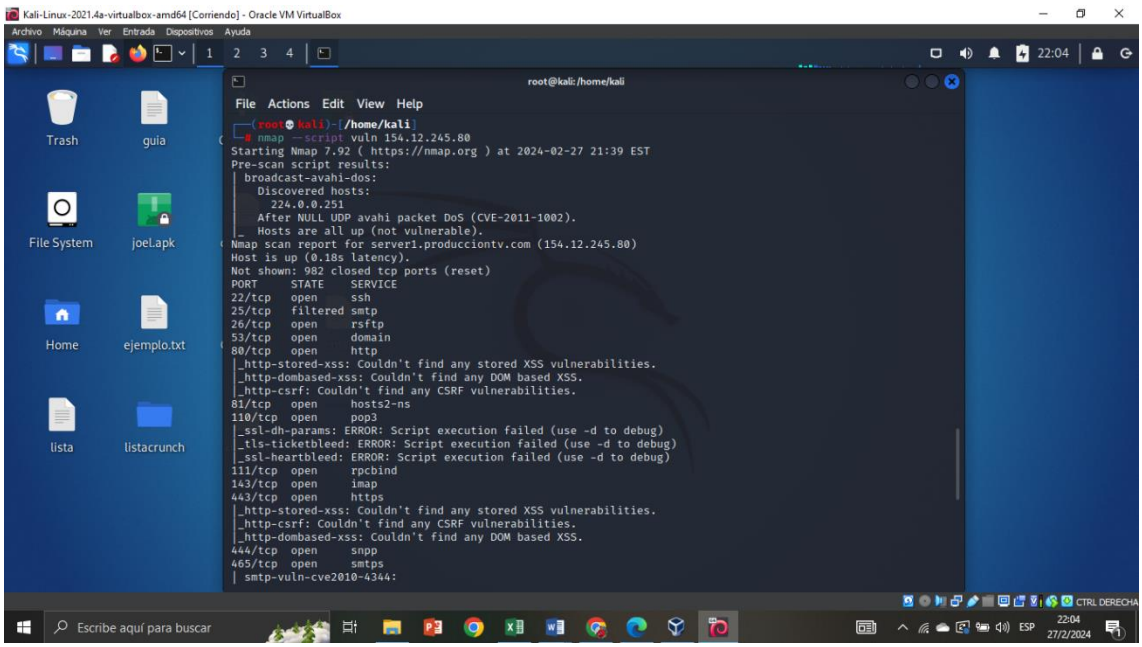
Yeiny, H. R., Judith, P. M., & Gustavo, T. L. (23 de Noviembre de 2022). *La importancia del*

computo forense en la actualidad. Obtenido de https://terc.mx/index.php/terc/article/view/298/256

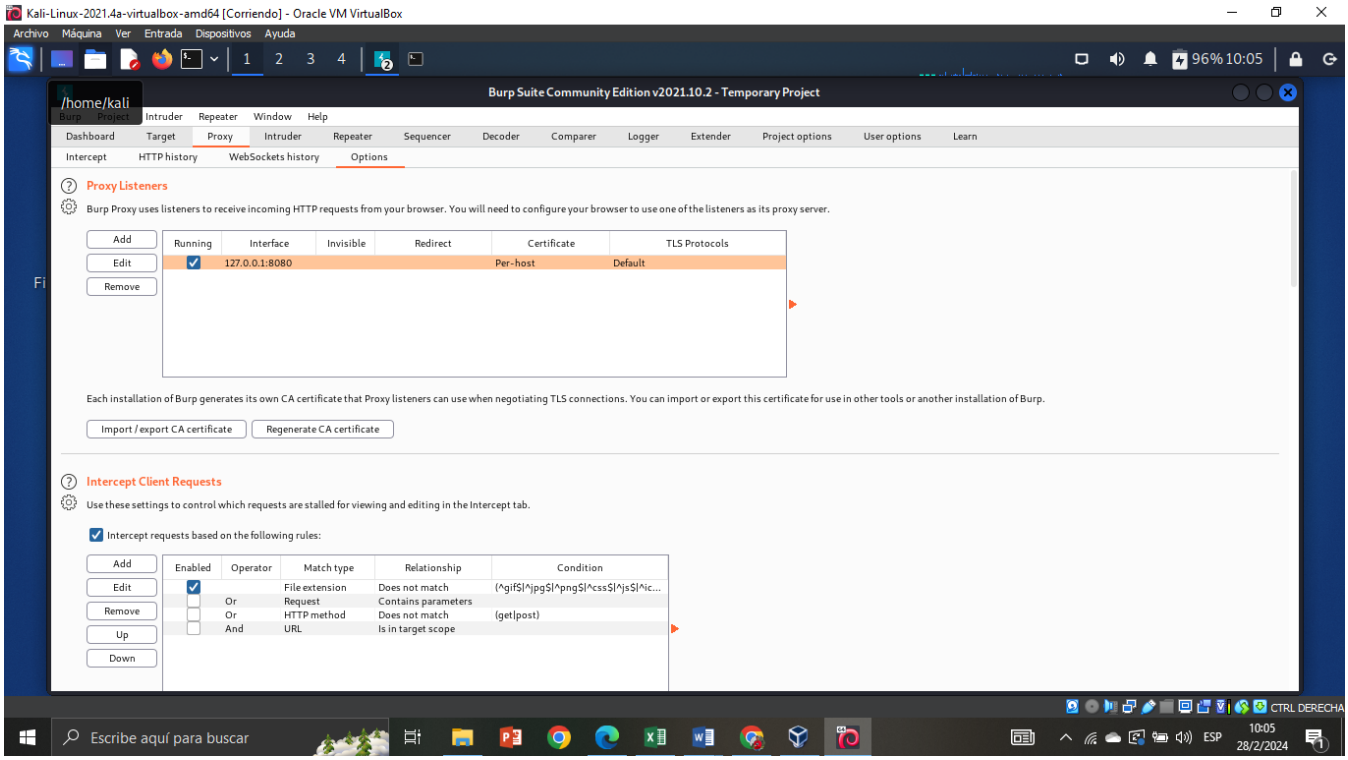
ANEXOS



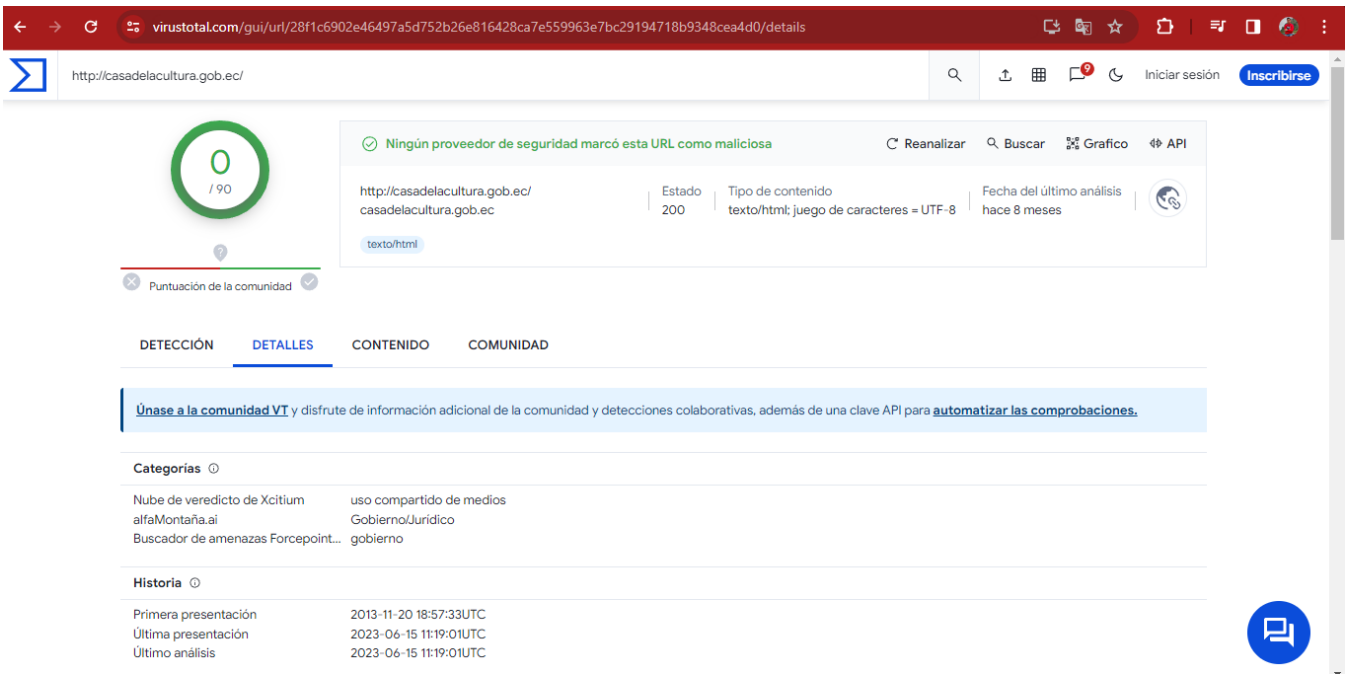
Anexo 1: Escaneo de puertos de página de La Casa de la Cultura
Fuente: Elaboración propia



Anexo 2: Escaneo de vulnerabilidades de la página de La Casa de la Cultura
Fuente: Elaboración propia



Anexo 3: Interfaz de Burp Suite y sus herramientas
Fuente: Elaboración propia



Anexo 4: Identificación de dirección IP de la Pagina de La Casa de la Cultura mediante virustotal.com

Fuente: Elaboración propia

UNIVERSIDAD TÉCNICA DE BABAHOYO
FACULTAD ADMINISTRACION FINANZAS E INFÓRMATICA
DECANATO

Babahoyo, 16 de febrero de 2024
D-FAFI-UTB-0177-2024

Sr.
Henry Layana Franco
REPRESENTANTE LEGAL DE LA EMPRESA CASA DE LA CULTURA ECUATORIANA "BENJAMIN CARRION" NUCLEO DE LOS RIOS.
Ciudad. -

De mis consideraciones:

Reciba un cordial saludo por parte de la Facultad de Administración, Finanzas e Informática de la Universidad Técnica de Babahoyo, donde formamos profesionales altamente capacitados en los campos de Tecnologías de la Información y de Administración, competentes, con principios y valores cuya practica contribuye al desarrollo integral de la sociedad, es por ello que buscamos prestigiosas Empresas e Instituciones Públicas y Privadas en las cuales nuestros futuros profesionales tengan la oportunidad de afianzar sus conocimientos.

El señor **MILTON ANDRES VILLACRES MORANTE,** con cédula de identidad No. **125048422-5** estudiante de la Carrera de Ingeniería en Sistemas de Información, matriculado en el proceso de titulación en el periodo NOVIEMBRE 2023 – ABRIL 2024, trabajo de titulación modalidad examen de carácter complexivo, previo a la obtención del grado académico profesional universitario de tercer nivel como INGENIERO EN SISTEMAS DE INFORMACIÓN, solicita por intermedio del Decanato de esta Facultad el debido permiso para realizar su Estudio de Caso con su tema: **" ESTUDIO DE LA INCIDENCIA DE LAS HERRAMIENTAS DE SEGURIDAD INFORMÁTICA NMAP Y BURP SUITE UTILIZADAS PARA REALIZAR PENTESTING EN APLICACIONES WEB PARA LA CASA DE LA CULTURA BABAHOYO-LOS RIOS".**

Atentamente,

Lcdo. Eduardo Galeas Guijarro, MAE.
DECANO

c.c: Archivo

CASA - DE LA CULTURA ECUATORIANA "BENJAMIN CARRION" NUCLEO DE LOS RIOS
RECIBIDO
22 FEB 2024 HORA 11:32
Firma Autorizada

Av. Universitaria Km 2 ½ vía Montalvo. Teléfono (05) 2572024 e-mail: decanatofafi@utb.edu.ec	Elaborado por: Ing. Marilyn Coloma Aguilar	Revisado por: Lcdo. Eduardo Galeas Guijarro, MAE

Anexo 5: Carta de pedido de permiso a La Casa de la Cultura para realizar la investigación

Casa de la Cultura Ecuatoriana "Benjamín Carrión" Núcleo de Los Ríos

Babahoyo, 22 de febrero del 2024
OFICIO N°007-DP4-CCE-NLR-2024

Señor.
Lcdo. Eduardo Gáleas Guijarro, MAE.
DECANO DE LA FALCULTAD DE ADMINISTRACION, FINANZAS E INFORMATICA.

De mis consideraciones:

Reciba un fraterno y solidario saludo de quienes conformamos la **CASA DE LA CULTURA ECUATORIANA "BENJAMÍN CARRIÓN" NÚCLEO DE LOS RÍOS**.

Yo, **HENRY LAYANA FRANCO**, me dirijo a usted como **REPRESENTANTE** de la institución **CASA DE LA CULTURA ECUATORIANA "BENJAMÍN CARRIÓN" NÚCLEO DE LOS RÍOS**, ubicada en las calles **AV. GENERAL BARONA #1507 Y 9 DE NOVIEMBRE**, para hacerle conocer que hemos **ACEPTADO** al estudiante **VILLACRES MORANTE MILTON ANDRES** con CI. **125048422-5** de la **UNIVERSIDAD TECNICA DE BABAHOYO en la FACULTAD DE ADMINISTRACION, FINANZAS E INFORMATICA de la carrera SISTEMAS DE INFORMACION (REDISEÑADA) OCTAVO SEMESTRE ''A'' MATUTINO**, realizar en nuestra empresa su proyecto de estudio de caso denominado **'ESTUDIO DE LA INCIDENCIA DE LAS HERRAMIENTAS DE SEGURIDAD INFORMATICA NMAP Y BURP SUITE UTILIZADAS PARA REALIZAR PENTESTING EN APLICACIONES WEB PARA LA CASA DE LA CULTURA BABAHOYO-LOS RIOS'** el cual es requisito indispensable para que se pueda titular.

Seguros de contar con una favorable acogida a la presente, le anticipo mis agradecimientos personales e institucionales.

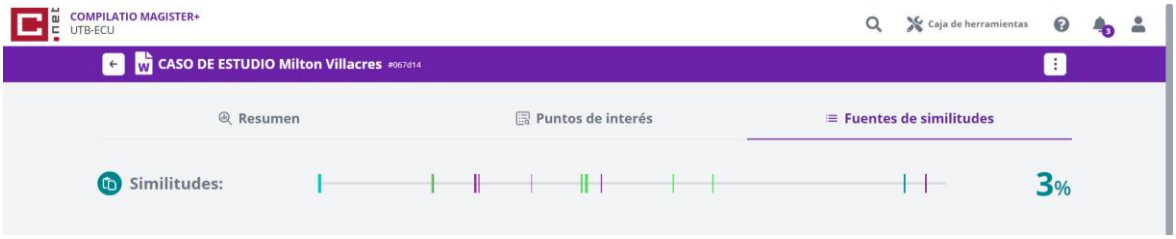
Atentamente,

Henry Vicente Oswaldo Layana Franco
DIRECTOR PROVINCIAL DE LA
CASA DE LA CULTURA ECUATORIANA
"BENJAMÍN CARRIÓN" NÚCLEO DE LOS RÍOS

CCE BENJAMÍN CARRIÓN NÚCLEO LOS RÍOS

General Barona 1507 y 9 de Noviembre – Telf: 052020364
Email: henry.layana@casadelacultura.gob.ec

Anexo 6: Carta de autorización de La Casa de la Cultura



Anexo 7. Certificado de Análisis de Detección de Plagio