Universidad Continental

FACULTAD DE INGENIERÍA

Escuela Académico Profesional de Ingeniería
de Sistemas e Informática

Trabajo de Investigación

Aplicación de Pentesting en el análisis de vulnerabilidades del sistema web de gestión administrativa de la Empresa DEVHUAYRA SAC Huancayo

Margaret Lesly Palacios Gallardo

Para optar el Grado Académico de
Bachiller en Ingeniería de Sistemas e Informática

Huancayo, 2021

AGRADECIMIENTO

Un agradecimiento a mis padres, quienes me brindaron todo su apoyo y enseñanzas en cada una de las etapas de mi vida. Así mismo agradezco a mis maestros en la universidad quienes aportaron en mi formación académica y profesional.

DEDICATORIA

A mi Padre y a mi Madre por brindarme una excelente formación, amor y apoyarme en el cumplimiento de mis metas académicas, profesionales y personales.

ÍNDICE

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

RESUMEN

El presente informe de investigación trata la Aplicación de Pentesting en el análisis de vulnerabilidades del sistema web de Gestión Administrativa de la empresa Devhuayra SAC Huancayo. Se delimitó la aplicación del Pentesting solo al sistema web de Gestión Administrativa, con la autorización del Gerente de Devhuayra SAC. Quien se comprometió a la aplicación del Pentesting como parte del plan inicial de lineamiento y estrategia de seguridad de la información para su empresa.

Para realizar la aplicación del Pentesting primero se definió una metodología de trabajo basada en las metodologías OSSTMM, NIST SP-800-115 y OWASP Top Ten para la etapa de identificación de vulnerabilidades. Se utilizó como herramienta de software el sistema operativo Kali Linux 2020 v4 orientado a la seguridad informática. Se ejecutaron las 4 etapas del Pentesting con las herramientas y comandos de Kali Linux: Reconocimiento o Recolección de Información, Escaneo o Análisis de Vulnerabilidades, Explotación de Vulnerabilidades y Post Explotación. Luego se realizó el análisis de las vulnerabilidades encontradas asociándolas a las amenazas que podrían aprovecharse de las mismas para luego obtener una matriz de riesgos, la cual representó el estado inicial del Sistema Web respecto a la seguridad de la información. Posteriormente se recomendó los controles de seguridad apropiados por cada vulnerabilidad a fin de cerrarlas. Finalmente se obtuvo una matriz con el riesgo residual vs la matriz inicial.

Se concluyó que la aplicación de Pentesting permitió identificar y clasificar las vulnerabilidades de acuerdo a su nivel de gravedad así mismo se recomendaron los controles de seguridad para reducir el impacto negativo de las vulnerabilidades.

Palabras Clave: Pentesting, seguridad de la información, seguridad web, riesgos informáticos, vulnerabilidades

ABSTRACT

This research report is about Pentesting Application to contribute to information security of Administrative Management web system in Devhuayra SAC Huancayo. The Pentesting application was delimited only to the Administrative Management web system, with the authorization of the Devhuayra SAC Manager, who committed to the application of Pentesting as part of the initial guideline plan and information security strategy for the company.

To apply Pentesting application, a work methodology was first defined based on the OSSTMM, NIST SP-800-115 and OWASP Top Ten methodologies for the vulnerability identification stage. The Kali Linux 2020 v4 operating system oriented to computer security was used as a software tool. The 4 stages of Pentesting were applied with tools and Kali Linux commands: Recognition or Collection of Information, Scanning or Analysis of Vulnerabilities, Exploitation of Vulnerabilities and Post Exploitation. Then, the analysis of the vulnerabilities found was carried out, associating them with the threats that could take advantage of them and then obtaining a risk matrix, which represented the initial state of the Web System with respect to information security. Subsequently, the appropriate security controls were recommended for each vulnerability in order to close them. Finally, a matrix was obtained with residual risk vs initial matrix.

In conclusion, Pentesting application will identify and classify the vulnerabilities according to their level of severity, as well as the security controls to reduce the negative impact of the vulnerabilities.

Keywords: Pentesting, information security, web security, computer risks, vulnerabilities

INTRODUCCIÓN

Actualmente el mundo crece digitalmente, las empresas han trasladado toda su información y procesos a la nube. Así como se han producido mejoras e incrementos en el uso de las tecnologías de la información, cloud computing, internet, aplicaciones web, móviles, también se han incrementado el número de ciberdelincuentes que buscan obtener información, dinero, u otro activo que sea de valor de para la empresa, sus ataques son cada vez más sofisticados y la frecuencia con las que se realizan también han incrementado. Se valen de fallos o vulnerabilidades en los sistemas o red para ganar acceso y hacer daño, pero no solo los sistemas informáticos se ven comprometidos, las personas muchas veces resultan el eslabón más débil.

En el Perú las políticas de seguridad de la información no son obligatorias para todos los sectores. Las empresas medianas a pequeñas en su mayoría no toman estrategia de valor la seguridad de la información, la cual garantiza los principios de la seguridad: disponibilidad, integridad y confidencialidad ante sus activos.

El Pentesting es una de las herramientas aliadas para contribuir a la seguridad de la información dentro de una empresa. Por ello el presente informe de investigación con título "Aplicación de Pentesting en el análisis de vulnerabilidades del sistema web de Gestión Administrativa de la empresa Devhuayra SAC Huancayo" tiene el propósito la identificación de vulnerabilidades presentes en el sistema web de la empresa utilizando las herramientas orientadas a seguridad informática tales como el sistema operativo Kali Linux y sus respectivos comandos y herramientas integradas, para luego recomendar los controles de seguridad más adecuados a fin de contribuir a que el sistema sea más seguro.

El presente informe consta de 4 capítulos.

CAPÍTULO I. Se presenta el planteamiento del problema de estudio exponiendo el nivel de concientización y aplicación de estrategias de seguridad en nuestro país, así mismo se identifica el problema general y específico del caso de estudio. Se presentan los objetivos relacionados al problema, la justificación, las hipótesis y finaliza con las variables.

CAPÍTULO II. En el marco teórico se presenta toda la bibliografía encontrada a fin de establecer las bases teóricas necesarias para el estudio. Los antecedentes son presentados a nivel internacional y nacional. El capítulo finaliza con la definición de términos para facilitar la compresión del lector.

CAPÍTULO III. Se presenta el marco metodológico del estudio: método, diseño, nivel y tipo de investigación. Luego se muestran las técnicas de recolección de información y análisis de las mismas.

CAPÍTULO IV. Los resultados obtenidos a partir de la aplicación del Pentesting y la discusión a partir de ella se detallan en este capítulo. Finalmente se brindan las conclusiones y recomendaciones para futuros proyectos relacionados al Pentesting.

CAPÍTULO I

PLANTEAMIENTO DEL ESTUDIO

1.1 PLANTEAMIENTO Y FORMULACIÓN DEL PROBLEMA

De acuerdo a (1) informa que del año 2016 al 2020 la confianza de los usuarios en los servicios de comercio electrónico ha incrementado en un punto, dentro de una escala del 1 al 5, teniendo en cuenta que el 2016 se registraba 2 puntos y al 2020 3 puntos. Esta situación refleja un incremento en la inclinación al uso de servicios web y una gran cantidad de usuarios que los utilizan, así mismo la mira de los ciberdelincuentes se ha incrementado en el mundo digital. En Perú, de acuerdo a (1), la sensibilización en el marco de formación y capacitación cibernética no ha tenido ningún incremento. Las empresas pequeñas e incluso medianas no invierten en controles y políticas de seguridad. Respecto a entidades del gobierno aún no se cuenta con una estrategia nacional de ciberseguridad. Teniendo en cuenta el panorama general ante el incremento de la actividad digital también se ha reportado un incremento en los ciberataques.

Según (2) se reporta un incremento en ciberataques en Latinoamérica y el Perú, siendo las amenazas más comunes: ransomware, phishing, criptominería y el uso de exploits. El número de ciberataques aumento en un 15% en el Perú en el 2020, siendo el sector financiero, salud e e-commerce los más afectados. Esta problemática resulta cada vez más creciente. Por ello tengamos presente que los ciberataques no dejaran de suceder, no se pueden evitar.

Los ataques cibernéticos se aprovechan de las vulnerabilidades. El objetivo es conseguir acceso al sistema o red. Con el aumento de los sitios web y el rápido desarrollo de otras aplicaciones en la web, cada vez aumenta más la posibilidad de sufrir ataques. A la par, los atacantes toman de su tiempo, esfuerzo y conocimientos para crear nuevas herramientas y técnicas más efectivas y rápidas para robar información, destruir datos, robar dinero, desprestigiar una compañía, exponer datos, interrumpir la operación y el funcionamiento de los sistemas.

Los cibercriminales utilizan diferentes métodos para atacar ataque de inyección por comandos, el ataque de inyección SQL, phishing, Cross-Site scripting (XSS), ataques de fuerza bruta, envenenamiento CEO, entre muchísimos otros más, adaptándolos o usándolos de forma combinada para llevar a cabo elaborados ciberataques, estos dependerán de sus motivos. Uno de los ataques más conocidos según (3) es el ataque distribuido de denegación del servicio (DDoS), en el que se utilizan bots infectados para congestionar un sitio web o una aplicación web debido a la cantidad de peticiones que se realizan simultáneamente, el objetivo es que los usuarios legítimos no pueden acceder a él, algo que cuesta a las empresas millones de dólares en ingresos, pérdida de productividad, interrupción de sus servicios web y daños en la reputación.

De acuerdo a (4) en la sección vulnerabilidades destacables respecto al primer trimestre del 2020 concluye que los ataques relacionados a Cross Site Scripting son los que ocupan

el primer lugar, seguido de configuraciones inseguras en la gestión de permisos de usuarios, así mismo vulnerabilidades en la protección de datos sensibles y deficientes controles en la validación de ingreso de datos.

Por ello el presente estudio se centra en desarrollar la aplicación de Pentesting para identificar las vulnerabilidades en el sistema web de Gestión Administrativa siguiendo una metodología basada en OSSTMM, NIST SP-800-115 y OWASP Top Ten. Para luego brindar las recomendaciones apropiadas en el cierre de las vulnerabilidades existentes. A fin de reducir el impacto que pueda causar un ciberataque.

1.2 FORMULACIÓN DEL PROBLEMA

1.2.1 PROBLEMA GENERAL

¿Influenciará la aplicación de Pentesting en al análisis de vulnerabilidades del sistema web de Gestión Administrativa de la empresa Devhuayra SAC Huancayo?

1.2.2 PROBLEMAS ESPECÍFICOS

¿Es posible clasificar las vulnerabilidades encontradas de acuerdo al nivel de gravedad?

¿Es posible reducir las vulnerabilidades encontradas mediante la recomendación de controles de seguridad apropiados?

1.3 OBJETIVOS

1.3.1 OBJETIVO GENERAL

Aplicar el Pentesting para el análisis de vulnerabilidades web de Gestión Administrativa de la empresa Devhuayra SAC Huancayo.

1.3.2 OBJETIVOS ESPECÍFICOS

Clasificar las vulnerabilidades encontradas de acuerdo al nivel de gravedad.

Reducir las vulnerabilidades encontradas mediante la recomendación de controles de seguridad apropiados.

1.4 JUSTIFICACIÓN

1.4.1 JUSTIFICACIÓN TECNOLÓGICA

Ante el incremento de ciberataques a sistemas web y teniendo en cuenta que esta situación no se puede evitar, es de vital importancia tomar las medidas de acción necesaria para proteger a todo aquello que sea de valor para las empresas. Debemos tener en cuenta que el impacto que se genera del aprovechamiento de las vulnerabilidades puede ocasionar un impacto no solo económico sino de reputación.

Actualmente las empresas dependen de sitios web y aplicaciones para darse a conocer, ofrecer sus productos y/o servicios o para manejar sus procesos internos, por ello se hace creciente la necesidad de proteger los datos que navegan a través de Internet los cuales contienen datos personales, números de tarjetas, cuentas bancarias u otro tipo de información sensible. Los ciberataques, que ya no se limitan a objetivos de alto nivel, pueden afectar a cualquier empresa que dependa de aplicaciones, dispositivos y sistemas en red. Por ello se deben tomar los controles y medidas apropiados para identificar vulnerabilidades y riesgos dentro de la empresa Devhuayra tales como el Pentesting como parte de un plan de Seguridad de la información, que debe ser aceptado y liderado por la gerencia.

1.4.2 JUSTIFICACIÓN SOCIAL

El objetivo de aplicar Pentesting a la empresa Devhuayra es identificar tempranamente las vulnerabilidades a fin de cerrarlas, y reducir el impacto ante un posible ciberataque, que puede causar no solo pérdida de información o dinero, también genera un impacto negativo en la reputación de la empresa. Los clientes ya no confían en los servicios que se prestan. Inclusive los colaboradores de la empresa podrían no confiar en los sistemas informáticos de la empresa y la información que esta procesa.

1.4.3 JUSTIFICACIÓN TEÓRICA

La aplicación del Pentesting se ejecuta bajo las guías metodologías OSSTMM, NIST SP-800-115 y OWASP Top Ten, las cuales han sido probadas y ejecutadas por miles de empresas y profesionales en seguridad de la información.

1.5 HIPÓTESIS Y DESCRIPCIÓN DE VARIABLES

1.5.1 HIPÓTESIS GENERAL

La aplicación del Pentesting al sistema web de Gestión Administrativa de la empresa Devhuayra SAC Huancayo influye en el análisis de vulnerabilidades.

1.5.2 HIPÓTESIS ESPECÍFICA

La aplicación del Pentesting permite clasificar las vulnerabilidades sistema web de Gestión Administrativa.

La aplicación del Pentesting reduce las vulnerabilidades del sistema web de Gestión Administrativa.

1.6 VARIABLES

1.6.1 VARIABLE INDEPENDIENTE

Aplicación de Pentesting.

- Alcance de la aplicación.
- Metodologías de aplicación.
- Herramientas de Pentesting.

1.6.2 VARIABLE DEPENDIENTE

Análisis de vulnerabilidades del sistema web de gestión administrativa de la empresa Devhuayra SAC Huancayo.

- Cantidad de vulnerabilidades encontradas y clasificadas
- Numero de vulnerabilidades reducidas – solucionadas.

1.6.3 DEFINICIÓN DE VARIABLES

a) Aplicación de Pentesting

Acceso legal y autorizado a sistemas de información, con el objetivo de hacerlos más seguros a través de herramientas para la identificación y explotación de vulnerabilidades.

b) Análisis de vulnerabilidades del Sistema Web de Gestión Administrativa de la empresa Devhuayra SAC Huancayo.

Es el proceso de identificar y categorizar una vulnerabilidad presente en el sistema, para luego analizarla en un posible escenario de riesgos que puede causar un impacto negativo, posteriormente se recomiendas las implementaciones más adecuadas para reducir dicha vulnerabilidad.

1.6.4 OPERACIONALIZACIÓN DE LAS VARIABLES

Variable	Definición	Indicadores	Instrumentos
Aplicación de Pentesting	Acceso legal y autorizado a sistemas de información, con el objetivo de hacerlos más seguros a través de herramientas para la identificación y explotación de vulnerabilidades.	Ejecución de 4 fases del Pentesting tomando como guía las metodologías OSSTMM, NIST SP-800-115 y OWASP.	Conjunto de Procedimientos
Análisis de vulnerabilidades del sistema web de gestión administrativa de la empresa Devhuayra SAC Huancayo	Es el proceso de identificar y categorizar una vulnerabilidad presente en el sistema, para luego analizarla en un posible escenario de riesgos que puede causar un impacto negativo, posteriormente se recomiendas las implementaciones más adecuadas para reducir dicha vulnerabilidad.	▪ Cantidad de vulnerabilidades encontradas y clasificadas ▪ Numero de vulnerabilidades reducidas – solucionadas.	▪ Checklist ▪ Resultados de Pentesting

CAPÍTULO II

MARCO TEÓRICO

2.1. ANTECEDENTES DEL PROBLEMA

2.1.1 ANTECEDENTES INTERNACIONALES

- En (5) se tuvo el objetivo de trazar las fases del Pentesting profesional y algunas de las herramientas y técnicas más conocidas para la ejecución de cada fase desde una perspectiva profesional y que se enfoca en una situación real. En conclusión, “hay muchísimas formas de acceder a un equipo y de obtener información relevante sobre una empresa”. Las causas de ocurrencia son debido a la negligencia de los administradores de los sistemas, como la no actualización de las aplicaciones, la ausencia de políticas de seguridad en el cambio y establecimiento de contraseñas, o muchas veces el uso de la misma contraseña para más de un equipo. Sin embargo, aun haciendo correctamente lo anterior no estamos seguros. Ningún sistema de seguridad

es completamente seguro, no existe, por otro lado, las personas resultan el blanco más fácil y atrayente para los ciberdelincuentes. La solución más acertada es crear conciencia en seguridad de la información y realizar auditorías periódicas. Este estudio hace énfasis en buscar vulnerabilidades caudas por el error humano en las configuraciones de servidores, aplicaciones, base de datos u otros, por la misma razón especial atención a la verificación del cumplimiento de políticas de seguridad al realizar dichas configuraciones.

- (6) mencionó respecto al uso de herramientas de Pentesting que el tiempo de respuesta se refiere a la cantidad de tiempo necesario para que una herramienta complete una tarea específica, mientras que por otro lado la cobertura indica el número de elementos detectados por las respectivas herramientas, dichas herramientas sirven de apoyo para la identificación de vulnerabilidades. Basado en ello se concluye que "las pruebas de penetración son esencialmente importantes para que las organizaciones fortalezcan la seguridad de sus sistemas. con un enfoque apropiado junto con si esos defectos posiblemente peligrosos son amenazas reales para el sistema, para ello se deben seleccionar las herramientas más adecuadas". Por ello se deben escoger las herramientas de Pentesting que contribuyan directamente al hallazgo de vulnerabilidades considerar si es un entorno web o local, sistema o red, pruebas de caja negra o blanca, así mismo no alerta a los sistemas de detección de tráfico anormal como IPS, IDS, firewall, por ejemplo utilizar nmap null.

- (7), tuvo el objetivo de evaluar la seguridad de un sistema en etapas. Se menciona que "durante las pruebas iniciales, se identifican las vulnerabilidades presentes en el sistema y se explotan tal como haría un atacante con fines maliciosos. Esto permite al pentester realizar una

evaluación de riesgos en la actividad comercial del cliente basándose en los resultados de la prueba y sugerir un plan de medidas correctivas" concluyendo que "a pesar de las diferencias evidenciadas todas siguen una estructura general que consiste en entender el contexto en el que se va a realizar las pruebas de penetración e intrusión, hacer un acercamiento al objetivos interactuando y conociendo el sistema en busca de vulnerabilidades, la explotación de esas vulnerabilidades y finaliza con la elaboración y presentación de un informe donde se muestra el procesos realizado, hasta dónde se puede llegar si se explotan las vulnerabilidades y lo más importante las recomendaciones para cerrar esas brechas de seguridad que ponen en riesgo a la organización". Teniendo en cuenta este estudio se realizará una etapa previa de reconocimiento al sistema, a fin de tener claro el objetivo y las tecnologías que lo componen, para luego utilizar las herramientas de software y efectuar un reconocimiento más exhaustivo. Se debe tener en consideración que desde la primera fase de Pentesting se pueden ir encontrando vulnerabilidades incluso sin el uso de ninguna herramienta. Pero lo más importante es brindar y aplicar las recomendaciones para cerrar dichas brechas de seguridad.

2.1.2 ANTECEDENTES NACIONALES

- (8) tuvo por objetivo determinar la contribución al realizar una auditoría de tipo Penetration Testing para la seguridad de la información. Expone que se debe identificar el nivel de intrusión, determinar el nivel de impacto ante un posible ciberataque en el marco de la integridad, disponibilidad y confidencialidad. Finalmente propone los lineamientos necesarios para los controles de seguridad. Luego de la ejecución del Pentesting se lograron encontrar 05 vulnerabilidades de clasificación ALTA por causas de puertos abiertos y 02 vulnerabilidades por ataques DOS. Así mismos se logró

identificar que “el impacto de un fallo de seguridad, que perjudicaría directamente a la Integridad de la información en un 40% del daño ocurrido, así como un 26% a la Integridad de la Información y un 34% a la disponibilidad de la información”. Finalmente “se brindaron los lineamientos adecuados para fortalecer los controles de seguridad”. De acuerdo a este estudio se clasificaran las vulnerabilidades encontradas de acuerdo a su nivel de gravedad e impacto: bajo, medio y alto, así mismo se pueden obtener porcentajes tanto de impacto como de reducción luego de aplicado los controles de seguridad, los cuales se aplican en el presente trabajo de investigación.

- (9) planteó el objetivo de realizar un modelo de niveles de seguridad para las aplicaciones web mediante las pruebas de intrusión en una PYME, se basa en una lista de metodologías que brindan las mejores prácticas. En conclusión, “la metodología que obtuvo un mayor puntaje fue OWASP, ya que esta metodología se encuentra en constante actualización”. El diseño de modelo que se obtuvo “incorpora distintos niveles de seguridad para pruebas de intrusión en aplicaciones web que permitió determinar el grado de protección en la que se encuentran las aplicaciones web”. El modelo aplicado a una PYME revela que “se identifican vulnerabilidades sobre el 87%. Esto es de beneficio para la organización, ya que el modelo es de fácil uso porque provee una lista de pruebas de intrusión y además ayuda a reducir el riesgo de ataques cibernéticos de las aplicaciones web cuando éstas se encuentren en el ambiente de producción”. Basado en este estudio es importante seguir una metodología de Pentesting ya que esta influirá en los resultados que se obtengan. OWASP Ton Ten ofrece un listado de tipo checklist de vulnerabilidades web, las cuales fueron tomadas en consideración para el presente informe.

- (10) mencionó que el uso de herramientas de Ethical Hacking facilita el diagnóstico de vulnerabilidades, permite identificar el número de puertas abiertas en una red, los puertos y servicios que se encuentran activos, así como también identificar e implementar las políticas de seguridad para fortalecer la seguridad de la información. Es importante mencionar que el Ethical Hacking contiene al Pentesting. Ambos se deben realizar de forma ética. Respecto al Pentesting en su fase de exploración deja claro e importante determinar cuan expuestos se encuentra un sistema o red. La aplicación de pruebas de penetración se realizan de forma ética y consentida por ambas partes, pentester y cliente. Por tanto se ha realizado un contrato donde se limitan los recursos sometidos a las pruebas así como el tiempo de duración, niveles de acceso y la confidencialidad de la información que se debe mantener.

2.1.3 ANTECEDENTES REGIONALES

- (11) tuvo por objetivo determinar que la aplicación de controles de seguridad apropiados y correctamente implementados reducen en gran medida el impacto por fallos o vulnerabilidades. Dichos controles incluso optimizan el funcionamiento de los activos a los que fueron aplicados. La aplicación de controles y medidas deben ser sostenibles en el tiempo y contribuir al funcionamiento, no deben degradar el servicio, el objetivo es brindar una seguridad por capas y el conjunto de controles deben operar centralizadamente.

2.2. BASES TEÓRICAS

2.2.1 SEGURIDAD DE LA INFORMACIÓN

La seguridad de la información protege, salvaguarda, preserva la información, pero también busca potenciar el negocio a través de ella como un elemento estratégico. La seguridad de la información no solo es infraestructura, también incluye a las personas como entes que utilizan la información y también la generan. Se dice de la seguridad que es iterativa y resiliente es decir busca aprender. (12)

Se conocen como activos de información a todos aquellos recursos que apoyan el modelo de negocios tales como: bases de datos, archivos, manuales, hardware, personas y otros.

En el marco de seguridad de la información debemos tener en consideración la triada de principios como se muestra en la Figura N° 1, los cuales se busca garantizar:

• Confidencialidad. Es la garantía de protección de algo que queremos proteger. La información no puede ser accedida por quienes no tienen el acceso autorizado.

• Integridad. La información y los datos no serán alterados o modificados. La información permanece tal cual se originó.

• Disponibilidad. Los activos se encuentran disponibles en el momento que se requieren.

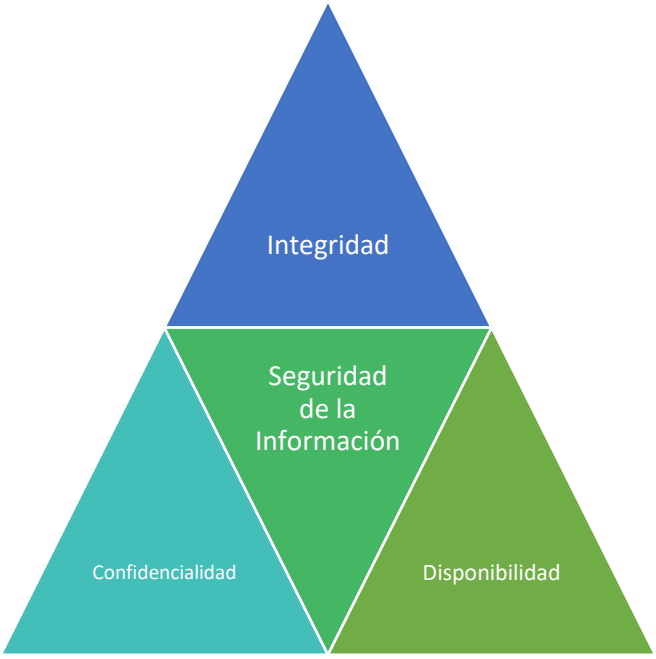


FIGURA N° 1: TRIADA DE PRINCIPIOS DE LA SEGURIDAD DE LA INFORMACIÓN

Adicionalmente se consideran:

• Autenticación. Es la primera capa de seguridad utilizando un usuario y contraseña. En algunos modelos de seguridad se utiliza el factor de doble autenticación.

• Autorización. Está relacionado a autorizar o denegar el acceso y permisos a un recurso.

• No repudio. Indica que un remitente no puede negar algo que envió o declaro.

2.2.2 VULNERABILIDADES Y RIESGOS

Una vulnerabilidad se define como la falla, inconsistencia o debilidad de un sistema o red que pone en riesgo la seguridad de lo que se protege. Por otro lado una amenaza es considerada como cualquier cosa, situación o persona que tiene el potencial de hacer daño a los sistemas de información. Por tanto un riesgo es la probabilidad de que una amenaza se aproveche de una vulnerabilidad y que

cause daño, impacto económico, de imagen u otro. En este punto el impacto producido es la diferencia del estado de seguridad antes y después del ciberataque o materialización del riesgo. Ver Figura N°2. (12)

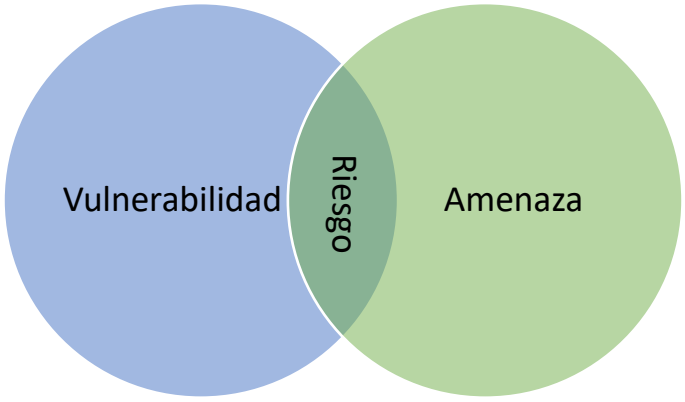


FIGURA N° 2: RELACIÓN DE VULNERABILIDAD, RIESGO Y AMENAZA.

Los tipos de vulnerabilidades más conocidas son:

a) Desbordamiento de buffer. Sucede cuando una aplicación recibe gran cantidad de datos que superan el tamaño del buffer. La información excedente es almacenada en memoria adyacente provocando un fallo en la programación.
b) Error en la gestión de recursos. Sucede cuando una aplicación consumen recursos de manera desmedida afectando la disponibilidad de dichos recursos para otras aplicaciones o la misma.
c) Errores de configuración. Los errores de configuración en software son muy comunes así como también en servidores y aplicaciones dejando en su mayoría la configuración por defecto.
d) Error en validación de datos de entrada. La falta de validación de datos de entrada deja una puerta abierta al ingreso de código malicioso o puede causar la inconsistencia de datos.

e) Fallos en Permisos y accesos. Falta de control en los permisos y accesos que se asignan a los recursos y aplicaciones. Dejando abierta la posibilidad de abuso de privilegios.

De acuerdo a las vulnerabilidades mencionadas algunas de las amenazas que se aprovechan de ellas, tomar como ejemplo la Figura N° 3:

a) Cross Site Scripting. El XSS inyecta código en las páginas web a fin de captar contraseñas, datos de tarjeta u otro tipo de datos de valor. Los sitios web que no se encuentran protegidos contra XSS quedan vulnerables.
b) Inyección SQL. Consiste en el ingreso de código SQL externo con el objetivo de obtener información directamente de la base de datos.
c) Comandos de Inyección. Los comandos del sistema son inyectados usando una terminal o interfaz gráfica disponible para el atacante.
d) Denegación de Servicios (DOS). Es un ataque a un sistema o red que causa que un servicio sea inaccesible por los usuarios legítimos.

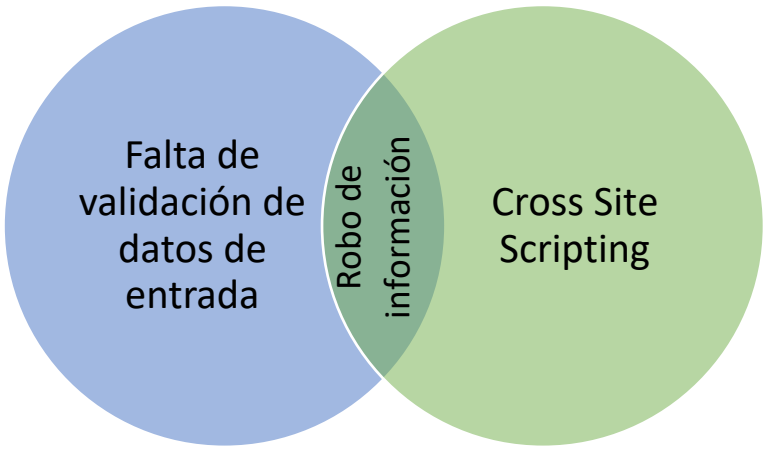


FIGURA N° 3: EJEMPLO DE VULNERABILIDAD, RIESGO Y AMENAZA.

Otras amenazas de acuerdo (8) se listan a continuación:

- Manipulación de Log
- Manipulación de configuración
- Suplantación de identidad de usuario
- Abuso de privilegios de acceso
- Uso no previsto
- Difusión de malware
- Reencaminamiento de mensajes
- Alteración de secuencia
- Acceso no autorizado
- Análisis de tráfico
- Interceptación de información
- Modificación deliberada de información
- Destrucción de información
- Divulgación de información
- Manipulación de programas
- Manipulación de equipos
- Ingeniería Social

2.2.3 PENTESTING O PENETRATION TESTING

Penetration Testing o Pentesting se define como la ejecución de pruebas de seguridad para determinar que un sistema de información protege y mantiene la funcionalidad según lo previsto según (13). De acuerdo a su definición la Seguridad no es un producto es un proceso, ya que es un esfuerzo constante por proteger y reducir el impacto que podría generarse en los activos de valor para las empresas ante los ciberataques. Las fases de dividen principalmente en 4 fases:

a) Recolección de Información o Reconocimiento. En esta etapa se definen los objetivos y alcance del Pentesting. Basado en ello se recolectan datos relevantes, identificar información clave sobre nuestros objetivos. En esta etapa de reconocimiento, recopilamos la información de los sistemas y/o redes que serán parte del Pentesting. La información comprende nombre del software que utilizan los sistemas, versiones, puertos, etc. Solo de acuerdo a lo definido en el alcance. En vista de que el Pentesting de acceso legal y autorizado en este punto se debe definir un Acuerdo de Nivel de Servicio u otro documento que evidencie la autorización de la empresa a realizar el Pentesting solo a lo que se definió en el alcance.

b) Búsqueda de vulnerabilidades o escaneo. Es esta etapa analizamos toda la información recopilada en el paso anterior a fin de determinar las vulnerabilidades. Escaneo para diferentes protocolos, identificación de vulnerabilidades y análisis de riesgos potenciales. En algunos casos el Pentesting finaliza en esta fase, depende de los objetivos y alcance establecido inicialmente.

c) Explotación de vulnerabilidades. En esta etapa utilizamos exploits para aprovechar las vulnerabilidades encontradas con el objetivo de acceder al sistema o red. El objetivo es obtener privilegios o información relevante.

d) Post Explotación. Luego de conseguir el ingreso al sistema o red el objetivo es obtener credenciales o información adicional que sea de valor para la empresa el fin es mantener o conservar el acceso o privilegios o generar nuevos accesos.

Finalmente se emite un Informe de Pentesting en el cual se documenta todo lo realizado: técnicas utilizadas, información relevante encontrada, herramientas utilizadas, vulnerabilidades encontradas, accesos concedidos, etc. Así mismo incluye en análisis de riesgos potenciales y las recomendaciones de seguridad apropiadas por cada hallazgo. Ver Figura N° 4.

FIGURA N° 4: FASES DEL PENTESTING.

FUENTE: FUNDAMENTOS DEL PENTESTING 2019 CAPÍTULO 2 – PLATAFORMA PLATZI

2.2.4 OSSTMM

El Manual de la Metodología Abierta de Testeo de Seguridad OSSTMM es un estándar para realizar auditorías de seguridad. Describe 6 áreas de evaluación: Seguridad de la Información, Seguridad de los Procesos, Seguridad en las Tecnologías de Internet, Seguridad en las comunicaciones, Seguridad Inalámbrica y Seguridad Física.

La primera área Seguridad de la Información incluye una revisión de la inteligencia competitiva, revisión de la privacidad y recolección de documentos. La sección de Seguridad de Procesos abarca testeo de solicitud,

sugerencia dirigida y testeo de personas confiables. La tercera sección Seguridad en las Tecnologías de Internet comprende dentro de los puntos más importantes y aplicables al presente informe: exploración de la red, identificación de los servicios del sistema, búsqueda y verificación de vulnerabilidades, testeo de aplicaciones de internet, testeo de control de acceso, testeo de sistemas de detección de intrusos y evaluación de políticas de seguridad. La sección de Seguridad en las Comunicaciones se enfoca en testeo de VoIP, FAX, Correo de voz y PBX. La sección de Seguridad Inalámbrica se enfoca en testeo de dispositivos y servicios que se comunican sin conexión a cables. Finalmente la sección Seguridad Física se enfoca en la seguridad perimetral, controles de acceso, monitoreo mediante cámaras de seguridad y respuesta de alarmas ante amenazas o catástrofes.

De acuerdo a (14) la metodología propone "un proceso de evaluación de debilidades de una serie de áreas que refleja de manera fiel los niveles de seguridad presentes en la infraestructura a ser auditada". Ver Tabla N° 1.

Fase Pentesting	Áreas de OSSTMM
Recolección de Información	Seguridad de la información
Escaneo	Seguridad de las Tecnologías de Internet
Búsqueda de vulnerabilidades	Seguridad de las Tecnologías de Internet
Explotación de vulnerabilidades	Seguridad de las Tecnologías de Internet

TABLA N° 1: RELACIÓN DE FASES DEL PENTESTING CON OSSTMM.

FUENTE: HTTPS://WWW.DRAGONJAR.ORG/OSSTMM-MANUAL-DE-LA-METODOLOGIA-ABIERTA-DE-TESTEO-DE-SEGURIDAD.XHTML

2.2.5 NIST SP-800-115

La NIST SP 800-115 es la Guía Técnica para pruebas y evaluación de seguridad de la información del Instituto Nacional de Estándares y Tecnología del gobierno de los EE.UU. que incluye las fases de evaluación inicial, evaluación de técnicas, definición de objetivos, planificación, ejecución y post ejecución en pruebas de vulnerabilidad como se muestra en la Figura N°5.

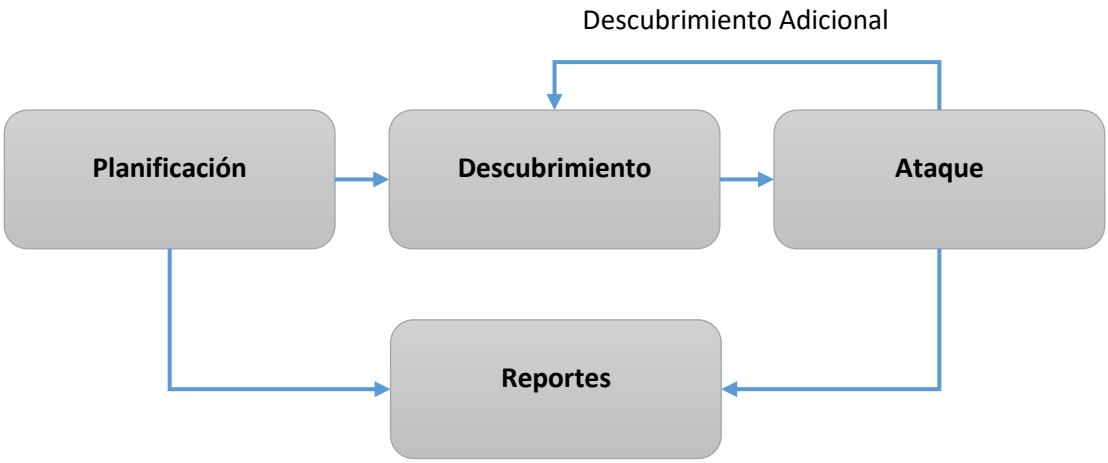


FIGURA N° 5: FASES DE NIST SP-800-115

FUENTE: NIST SP-800-115

Según (15) "las pruebas de intrusión o Pentesting puede ser utilizado para determinar: la manera en que el sistema tolera los patrones de ataques del mundo real, el nivel de sofisticación que un atacante necesita para comprometer con efectividad el sistema, las medidas adicionales que se deben emplear para mitigar las amenazas contra el sistema y la habilidad de los defensores para detectar los ataques y responder apropiadamente a estos". Siendo las medidas para mitigar el ciberataque el punto más relacionado para el presente informe.

2.2.6 OWASP Top Ten

OWASP es un proyecto de código abierto que se dedica a determinar y reducir las causas que hacen que un software sea inseguro. OWASP Top Ten es uno de los proyectos con las que cuenta la fundación. Es un documento estándar para desarrolladores y profesionales en seguridad, presenta los riesgos de seguridad más críticos en aplicaciones web. Los 10 riesgos incluyen:

1. Inyección. Las fallas de inyección, como SQL, NoSQL, OS y LDAP.
2. Autenticación rota ante las fallas en la administración de sesiones.
3. Exposición de datos sensibles debido a una falta de protección adecuada.
4. Entidades externas XML que se pueden utilizar para divulgar archivos internos, recursos compartidos de archivos internos, escaneo de puertos internos, ejecución remota de código y ataques de denegación de servicio.
5. Control de acceso roto hace referencia al acceso del atacante a cuentas de usuario con accesos incorrectamente restringidos.
6. Mala configuración de seguridad como resultado de configuraciones predeterminadas inseguras o configuraciones incompletas.
7. Secuencias de comandos entre sitios conocidos como XSS.
8. Ejecución remota de código.
9. Uso de componentes con vulnerabilidades conocidas.
10. Registro y monitoreo insuficientes e ineficacia en la respuesta ante incidentes.

2.3. HERRAMIENTAS DEL PENTESTING

2.3.1 VIRTUAL BOX Y KALI LINUX

Para crear un entorno de pruebas se utilizan algunas opciones como máquinas virtuales. Las máquinas virtuales abstraen el software del hardware. Crea una

máquina con componentes como memoria RAM, disco duro, etc. los cuales son virtuales. La máquina host distribuye sus recursos físicos a las máquinas virtuales. En su mayoría las máquinas virtuales se usan en servidores para mantener software antiguo, así también ejecutar aplicaciones en un sistema operativo diferente al del origen. La tecnología de virtualización permitió que se desarrollará la primera generación de aplicaciones cloud. Algunos de los softwares de virtualización más conocidos como VMWare Workstation, Virtual Box de Oracle y Hyper-V de Microsoft.

Por otro lado tenemos el sistema operativo Kali Linux el cual fue utilizado por sus herramientas orientadas a Pentesting. Kali Linux incluye las aplicaciones más utilizadas como: Aircrak-ng, Burpsuite, Hydra, John, Maltego, Metasploit Framework, Nmap, OWASP-Zap y Wireshark. Si se requiere de otras herramientas se tienen que instalar. El sistema operativo Kali Linux está basado en Debian GNU/Linux Este sistema está orientado a seguridad informática teniendo como fecha de lanzamiento el 13 de marzo de 2013 llegando a ser el sucesor de BackTrack.

2.3.2 HERRAMIENTAS POR FASES

2.3.2.1 RECONOCIMIENTO

HTTRACK. Es una aplicación que permite copias sitios web en Internet, permite la descarga de los directorios, imágenes u otros archivos desde el servidor web. Httrack organiza la estructura de enlaces relativa del sitio original. Al abrir una página del sitio web en el navegador se podrá navegar por el sitio de enlace en enlace, como si estuviera en línea.

WHOIS. Es una base de datos que contiene nombres de información de resolución DNS. El protocolo DNS asocia un nombre de dominio a una o más direcciones IP.

NETCRAFT. Es una compañía de seguridad informática que realiza auditorías y presta servicios de consultoría. Poseen una herramienta pública que permite analizar rápidamente servidores y subdominios para identificar qué versiones de sistemas están utilizando y así identificar vulnerabilidades.

RECON-NG. Es una suite que se compone de varios módulos y que permite recolectar información a partir de dominios, direcciones IP y sitios web. Este framework está escrito en el lenguaje Python.

2.3.2.2 ESCANEO

NMAP. Es un programa de código abierto de rastreo de puertos. Envía diferentes paquetes TCP y UDP para descubrir que puertos están abiertos o cerrados, a fin de conocer que servicios se encuentran activos.

WIRESHARK. Es un programa que analiza protocolos en una red a fin de realizar un análisis profundo, dar solución a problemas u otros.

OPENVAS. Es un framework tiene una base de datos extensa con una colección de muchas vulnerabilidades de muchos sistemas o aplicaciones conocidos. OpenVas escanea el objetivo a atacar y luego compara con su propia base de datos para identificar posibles vulnerabilidades que estén disponibles.

2.3.2.3 EXPLOTACIÓN DE VULNERABILIDADES

METASPLOIT. Es un framework para desarrollo y prueba de exploits que aprovecha diferentes vulnerabilidades. Utiliza una gran base de datos donde se encuentran payloads y exploits que se pueden usar dependiendo de las debilidades encontradas.

INYECCIONES SQL. Es método de inserción de código de lenguaje de consulta estructurado en un campo de entrada de datos en un formulario web, con el objetivo de conseguir acceso al sistema, modificar y/o eliminar datos de la base datos.

XSS. Cross-site scripting ataca sitios web que utilizan motores de bases de datos. El código interpretado es un código que está cargándose dinámicamente, se construye el sitio web cada vez que hay una solicitud a partir de una base de datos.

Con el XSS ponemos código en la base de datos de ese sitio y este código va a quedar permanentemente almacenado. Al momento en que un usuario acceda al contenido, va a mostrarse el contenido que nosotros elijamos. Se suele utilizar el lenguaje JavaScript.

POST EXPLOTACIÓN

METERPRETER. Es un intérprete de consola de Metasploit que permite establecer sesiones remotas, garantiza las comunicaciones encriptadas. Se debería evitar la creación de un nuevo proceso en el sistema, que contenga toda la actividad dentro del alcance del payloads en sí. Debería permitir la escritura de scripts, pero sin crear

nuevos archivos en el disco, ya que esto podría activar el software antivirus.

2.4. SISTEMA WEB DE GESTIÓN ADMINISTRATIVA

El sistema web de Gestión Administrativa de la empresa Devhuayra SAC se encarga de registrar el control de asistencia del personal que labora en la empresa. El trabajador inicia sesión con su usuario y contraseña. Luego registra la hora de ingreso o salida, ya que las horas de trabajo son contabilizadas por el sistema. Ver figura N° 6.

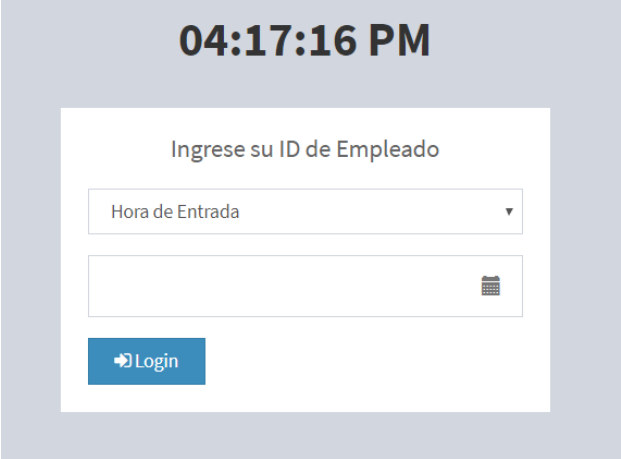


FIGURA N° 6: REGISTRO DE ENTRADA

El administrador ingresa al panel de control para revisar las asistencias de los trabajadores así como los registros de las actividades realizadas. Las actividades se muestran en un listado a partir del cual se cuentan los objetivos alcanzados por cada trabajador al día. Así mismo registrar a un nuevo trabajador. A continuación se muestra el formulario de inicio de sesión del administrador y creación de nuevo trabajador. Ver Figura N° 7 y 8.

FIGURA N° 7: INICIO SESIÓN ADMINISTRADOR

FIGURA N° 8: REGISTRO DE NUEVO TRABAJADOR

Otras opciones relacionadas a los trabajadores son: registro y seguimiento de las horas extras, adelantos e incentivos. Ver Figura N° 9.

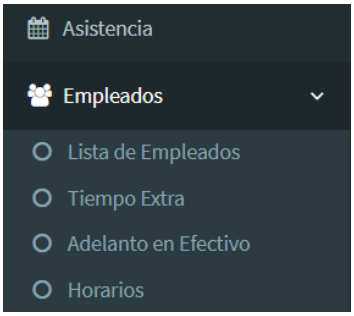


FIGURA N° 9: ACCIONES ADICIONALES PARA EMPLEADOS

Por otro lado se registran los ingresos y egresos, transacciones, préstamos, pago a proveedores, entre otros para mantener un control monetario. Ver Figura N° 10.

FIGURA N° 10: REGISTRO DE TRANSACCIONES

Finalmente se registran los datos de los clientes, los servicios que se prestan, precios de servicios, duración y recursos a utilizar, luego se registra el seguimiento para la evaluación final de los servicios prestados. Ver Figura N° 11.

FIGURA N° 11: REGISTRO DE CLIENTES EMPRESA

2.5. DEFINICIÓN DE TÉRMINOS BÁSICOS

- **Pentesting.** "Una prueba de penetración o pentest es un ataque simulado y autorizado contra un sistema informático con el objetivo de evaluar la seguridad del sistema. Durante la prueba, se identifican las vulnerabilidades presentes en el sistema y se explotan tal como haría un atacante con fines maliciosos. Esto permite al pentester realizar una evaluación de riesgos en la actividad comercial del cliente basándose en los resultados de la prueba y sugerir un plan de medidas correctivas." (16)
- **Vulnerabilidad.** "Es un fallo en un sistema que puede ser explotada por un atacante generando un riesgo para la organización o para el mismo sistema. Existen dos tipos de vulnerabilidades que se mencionan a continuación: lógicas y físicas." (17)
- **Sistema Web**. "Es una estructura de información y/o comunicación generada en el nuevo ámbito espacio de comunicación (Internet), creado por la aplicación de las tecnologías de la información (tecnologías de creación, mantenimiento y desarrollo de los sitios web), que posee dos elementos fundamentales (acciones de los sujetos y contenidos) y en donde se plantean un conjunto de prestaciones que los usuarios que visitan dicho web pueden ejercitar para satisfacer una o varias necesidades que posean." (18)
- **Seguridad de la Información.** "La seguridad informática se encarga de la seguridad del medio informático, según varios autores la informática es la ciencia encargada de los procesos, técnicas y métodos que buscan procesar almacenar y transmitir la información, mientras tanto la seguridad de la información no se preocupa sólo por el medio informático, se preocupa por todo aquello que pueda contener información, en resumen, esto quiere decir que se preocupa por casi todo, lo que conlleva a afirmar que existen varias diferencias, pero lo más relevante es el universo que manejan cada uno de los conceptos en el medio informático." (17)

CAPÍTULO III

METODOLOGÍA

3.1 MÉTODO DE INVESTIGACIÓN

3.1.1 MÉTODO ANALÍTICO

Descomponer el Pentesting en cada una de sus fases para ejecutar cada una de ellas como parte de un todo.

3.1.2 MÉTODO INDUCTIVO – DEDUCTIVO

Partimos de los hechos de la realidad para formular una hipótesis para nuestro problema, en esta primera parte utilizamos la inducción. Luego llegamos a la deducción a través de la teoría existente para luego contrastarla nuevamente con la realidad. En el caso de la aplicación del Pentesting, formulamos la hipótesis a

través de la inducción de los hechos reales sobre la importancia de utilizarlo para reducir el nivel de impacto en los ciberataques como parte de las medidas de control. Luego de la aplicación basada en la teoría existente como metodologías, herramientas, casos reales, análisis de expertos, etc. llegamos a la contrastación con la realidad.

3.2 TIPO DE INVESTIGACIÓN

El tipo de investigación es aplicada, ya que utiliza el conocimiento teórico para resolver problemas concretos. Se busca la aplicación de los conocimientos adquiridos relacionados al Pentesting mediante su aplicación. Por ello nos concentramos en dar solución a la identificación de vulnerabilidades dentro del sistema web de la empresa para luego recomendar los controles de seguridad más apropiados y así apoyar a la seguridad de la información, tomando como herramienta el Pentesting basado en las metodologías de OSSTMM, NIST SP-800-115 y OWASP Top Ten, así mismo las herramientas de software para la ejecución de cada fase del Pentesting.

3.3 NIVEL DE INVESTIGACIÓN

El nivel de investigación es de tipo aplicada. Se establece como prioridad dar solución a problemas y reconstruir procesos basándonos en descubrimientos ya realizados. En el caso del Pentesting existen muchas metodologías, herramientas y documentación relacionada, la aplicación, por ello se busca la mejor forma de llevar a cabo su funcionamiento contribuyendo y garantizando los principios de la seguridad: integridad, disponibilidad y confidencialidad.

3.4 DISEÑO DE INVESTIGACIÓN

Dentro del diseño de investigación se realiza de manera no experimental, es aquella en la que no se controlan ni manipulan las variables del estudio. Los datos son obtenidos a partir de las fases del Pentesting: reconocimiento, escaneo, explotación y post explotación de vulnerabilidades. Ya que en cada fase se van recolectando datos reales mediante el uso de herramientas de software para conocer a fondo el sistema web.

3.5 POBLACIÓN Y MUESTRA

El sistema web de Gestión Administrativa que incluye:

1. El registro de marcación de horario de trabajo de los colaboradores.
2. El sistema interno de manejo de servicios que presta la empresa y la nómina de colaboradores. Así mismo el control y manejo de ingresos y egresos.

3.6 TÉCNICA Y HERRAMIENTA DE RECOLECCIÓN DE DATOS

3.6.1 TÉCNICAS

- **Observación.** Observar y analizar el impacto que se produce del aprovechamiento de vulnerabilidades y materialización de riesgos luego de un ciberataque.

- **Experimentación.** Se experimentará con cada una de las herramientas de software enfocadas a cada una de las fases del Pentesting a fin de recolectar datos e identificar vulnerabilidades.

- **Checklist.** Utilizar una lista de verificación para conocer si la empresa cuenta con controles o medidas de seguridad enfocadas en el tratamiento de vulnerabilidades o fallos del sistema.

3.6.2 RECOLECCIÓN DE DATOS

Para la recolección de datos se utilizó un Checklist para la evaluación inicial del sistema web. Ver Figura N° 12.

Checklist – Evaluación Nivel de Seguridad Inicial

Evaluador: Margaret Lesly Palacios Gallardo

Empresa: Devhuayra SAC Huancayo

DATOS				
N°	**Descripción**	**SI**	**NO**	**Observaciones**
1	¿Se realizan copias de seguridad a la base de datos?			
2	¿Se realizan las actualizaciones correspondientes a los gestores de base de datos u otro software que soporten las BD?			
APLICACIONES				
N°	**Descripción**	**SI**	**NO**	**Observaciones**
3	¿Las aplicaciones de desarrollo in house son desarrolladas bajo estándares de seguridad?			
4	¿Se realiza el mantenimiento a las aplicaciones?			
POLÍTICAS				
N°	**Descripción**	**SI**	**NO**	**Observaciones**
5	¿Cuenta con políticas de seguridad actualizadas y difundidas a toda la empresa?			
INCIDENTES DE SEGURIDAD				
N°	**Descripción**	**SI**	**NO**	**Observaciones**
6	¿Cuenta con un plan de acción ante los incidentes de seguridad?			
7	¿Cuenta con medidas de acción ante vulnerabilidades encontradas en la infraestructura o sistemas?			

FIGURA N° 12: CHECKLIST EVALUACIÓN INICIAL

Así mismo se recolectó datos en cada una de las fases del Pentesting:

FASE 1: Reconocimiento

Técnica de Pentesting	Herramienta de Software
Obtención de la estructura de un sitio web mediante la clonación	Httrack
Reconocimiento del dominio	Whois
Reconocimiento del sitio web	NetCraft

FASE 2: Escaneo

Técnica de Pentesting	Herramienta de Software
Barrido de puertos	NMAP
Obtención de información de Banner de los puertos y posibles vulnerabilidades	NMAP Scripting
Análisis de tráfico de Red	Wireshark
Reconocimiento de la red	Nikto

FASE 3: Explotación de vulnerabilidades

Técnica de Pentesting	Herramienta de Software
Explotación de vulnerabilidades encontradas en las fases previas	Metasploit
Inyección SQL	Comandos SQL

Las vulnerabilidades encontradas se detallan en el CAPÍTULO IV Resultados.

3.6.3 ANÁLISIS DE DATOS

- **Análisis e interpretación.** Se realizará el análisis e interpretación de los datos y resultados obtenidos en cada fase del Pentesting.

- **Gráficos y Tablas.** Los gráficos nos permiten ver la relación de los datos con mayor claridad y de forma sencilla. Los gráficos se enfocarán a la relación de las vulnerabilidades encontradas con los principios de la seguridad. También se realizará la matriz de riesgos a fin fijar de manera clara los controles y recomendaciones de seguridad que se deben aplicar.

CAPITULO IV

RESULTADOS Y DISCUSIÓN

4.1 RESULTADOS OBTENIDOS

4.1.1 ANTES DE LA APLICACIÓN DEL PENTESTING

Se llevó acabo la aplicación del Pentesting al sistema web de Gestión Administrativa de la empresa Devhuayra SAC en Huancayo bajo autorización de la empresa, prueba de ello se anexa el *Acuerdo de Aplicación de Pentesting* Anexo 01, dicho documento también determina el alcance y las pruebas permitidas. Donde se indica que las pruebas de Pentesting solo se realizan de manera externa y sin brindar información adicional al dominio.

Los resultados de la aplicación de Pentesting serán útiles para la toma de decisiones y posterior implementación y mejora de la seguridad de la información al sistema web de la empresa, así como también ser extensible a todos los activos de información de Devhuayra SAC como parte de su estrategia de seguridad.

Para la aplicación del Pentesting se utilizó el virtualizador Virtual Box, en el cuál se configuró la máquina virtual con el sistema operativo Kali Linux 2020 v4 descargado del sitio oficial www.kali.org/downloads/, el cual se utilizó para ejecutar cada una de las herramientas de software para las 4 fases. Se configuró la máquina virtual con 8GB de disco duro, 1024MB de memoria RAM y una tarjeta de red modo NAT para acceder a Internet, ver Figura N° 13.

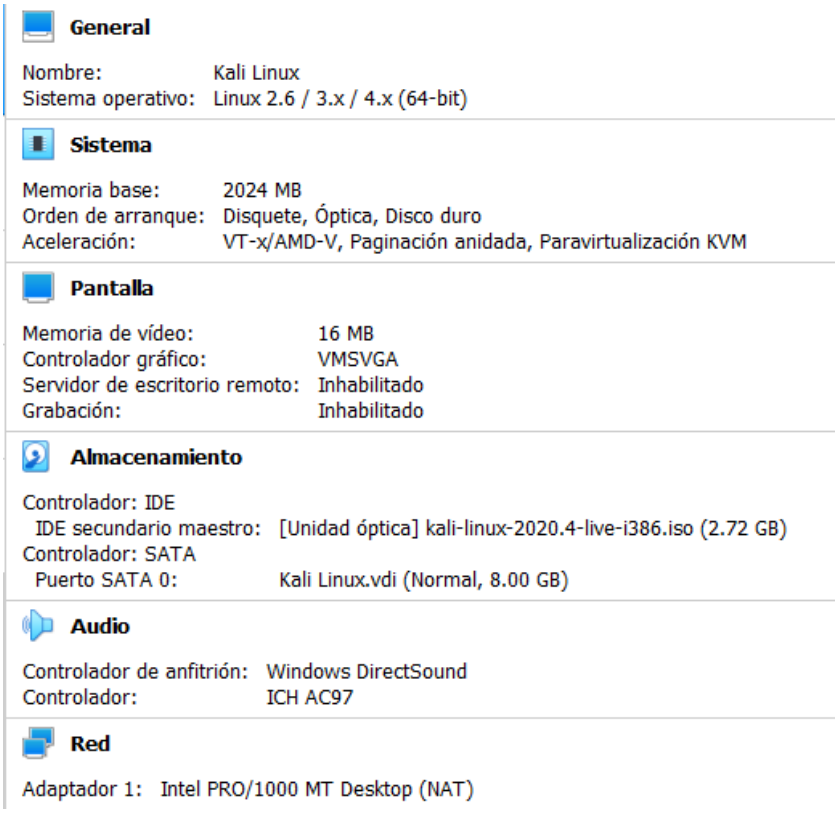


FIGURA N° 13: CONFIGURACIÓN DE LA MÁQUINA VIRTUAL KALI LINUX.

Se consideró como características principales del equipo de cómputo anfitrión: procesador Core i5 Octava Generación, memoria RAM de 12 GB y sistema operativo Windows 10 64 bits. Ver Figura N° 14.

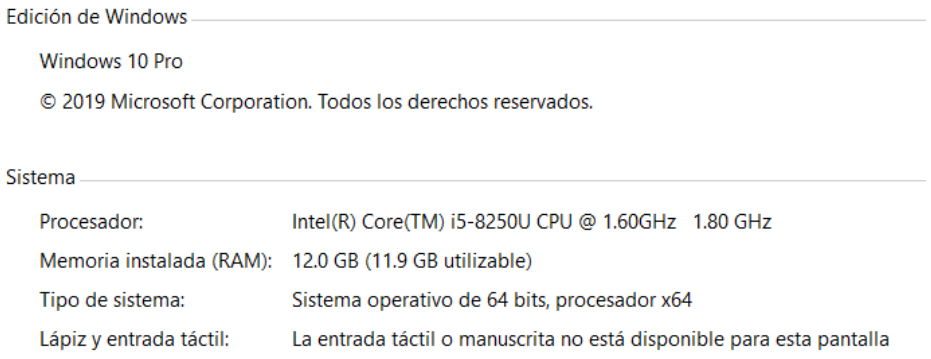


FIGURA N° 14: CARACTERÍSTICAS DEL EQUIPO DE CÓMPUTO ANFITRIÓN.

La conexión entre el S.O. Kali Linux y el sistema web de la empresa se da mediante la tarjeta de red modo NAT de la máquina virtual en Virtual Box la cual utiliza la IP del anfitrión para dar salida a Internet. El sistema web se aloja en un servidor web en la nube. Ver Figura N° 15 para detalles.

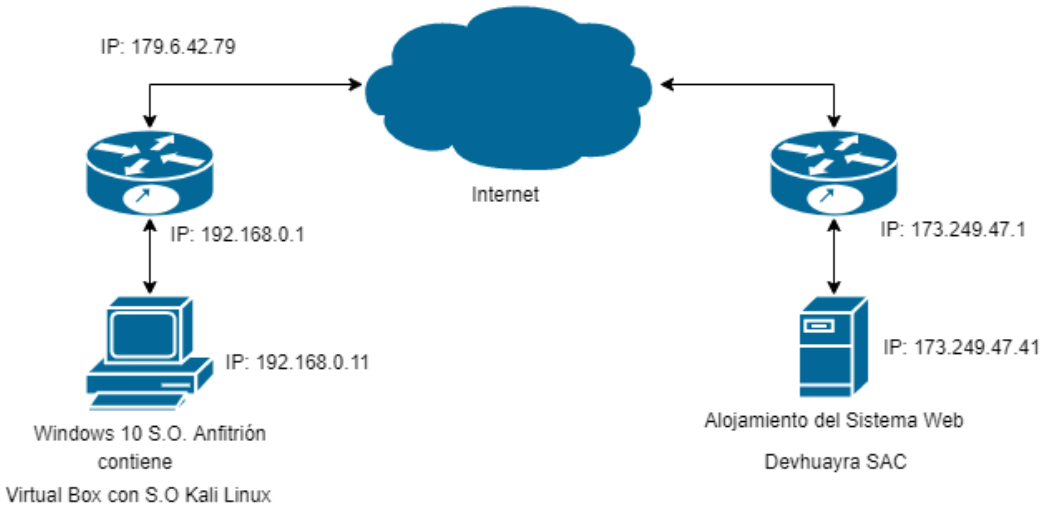


FIGURA N° 15: DIAGRAMA DE CONEXIÓN ENTRE EL SISTEMA WEB Y EL S.O. DE PRUEBAS

Se realizó una evaluación inicial mediante un checklist dando como resultado la falta de controles y políticas de seguridad respecto a copias de seguridad, actualización del software que se utiliza y un plan de acción ante incidentes de seguridad. Ver Anexo 02.

4.1.2 IDENTIFICACIÓN Y CLASIFICACIÓN DE VULNERABILIDADES

Se dio inicio a la aplicación del Pentesting con la actualización de Kali Linux con los comando *sudo apt Update* ver Figura N° y *sudo apt dist-upgrade* ver Figura N° 16 y 17.

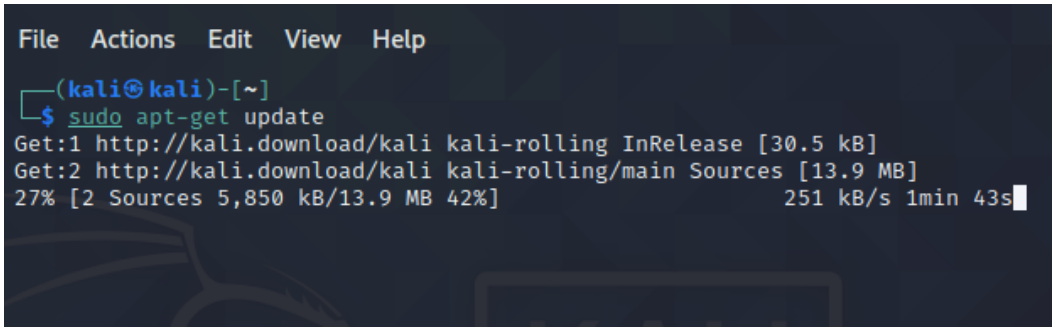


FIGURA N° 16: ACTUALIZACIÓN EN PROCESO UPDATE.

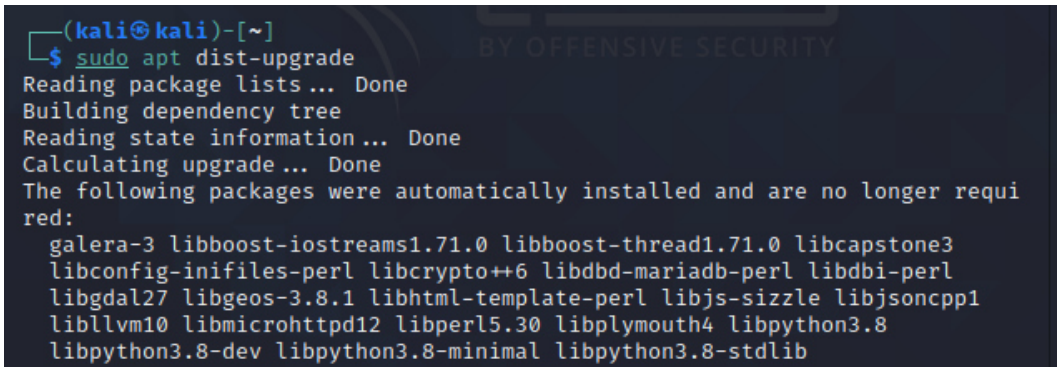


FIGURA N° 17: ACTUALIZACIÓN DISTRIBUCIÓN DE KALI LINUX EN PROCESO.

FASE 1: Reconocimiento

Durante la primera etapa se realizó el reconocimiento de la información relacionada al sistema web de la empresa. Los resultados que se obtuvieron con cada una de las herramientas destinadas a esta fase fueron:

HTTRACK

Se utilizó la herramienta Httrack para verificar que el sistema web no permita la descarga de todos los archivos. Obteniendo como resultado la descarga de la mayor parte de archivos del sistema web. Se puede observar en la Figura N° 18 la descarga de los archivos luego de la ejecución del comando *httrack --mirror -bN -sN 173.249.47.41 -O /copia.* En el cual se indica "mirror" para realizar una copia exacta del sitio web, la opción "bN" permite la descarga de las cookies del sitio, la opción "sN" permite el seguimiento a etiquetas meta de robots. Finalmente la opción "O" indica que los archivos descargados serán almacenados en la carpeta que se señala luego.

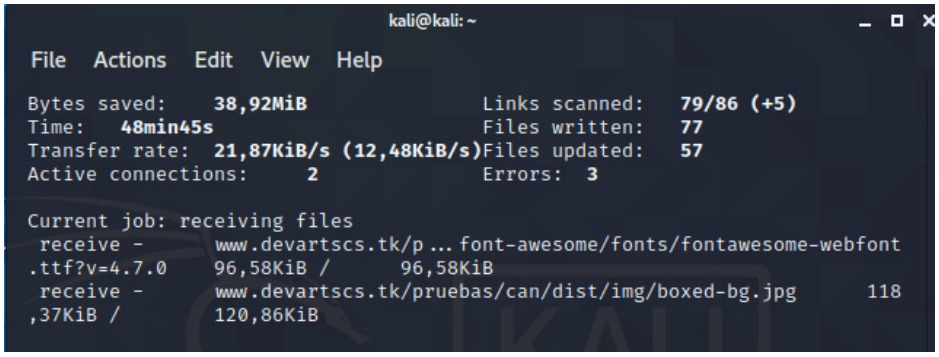


FIGURA N° 18: HTTRACK DESCARGANDO LOS ARCHIVOS DEL SISTIO WEB ORIGINAL

Los resultados de la descarga de archivos se almacenan en la carpeta Copia previamente definida como se ve en la Figura N° 19.

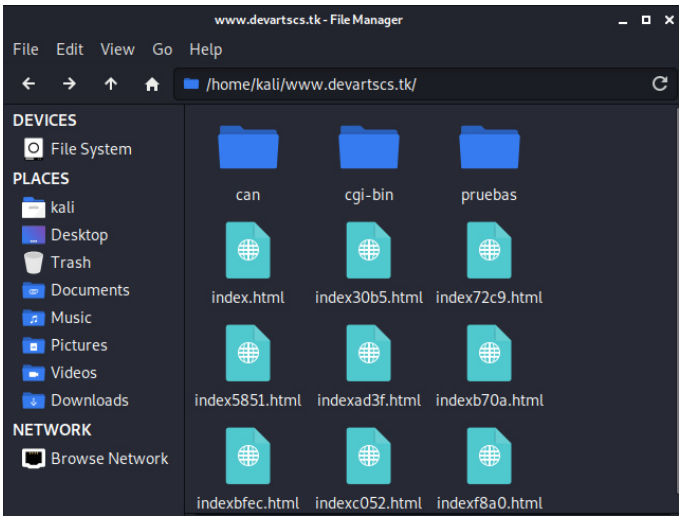


FIGURA N° 19: SE EVIDENCIAN LOS ARCHIVOS DESCARGADOS EN EL /HOME.

La descarga de archivos con Httrack también incluyo las carpetas que estaban indexadas al dominio principal ya que estas no estaban protegidas, teniendo como resultado el inicio de sesión del sistema interno de Gestión Administrativa como se muestra en la Figura N° 20. Por otro lado se obtuvo una copia idéntica del formulario de marcación de horarios de los colaboradores de la empresa el cual se ejecutó localmente en Kali Linux, ver Figura N° 21.

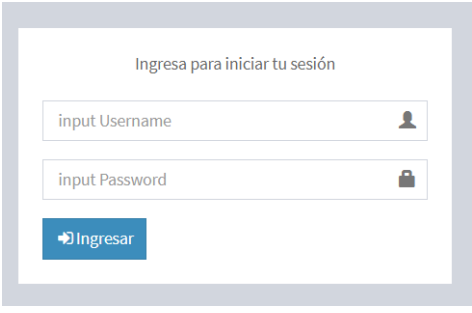


FIGURA N° 20: INICIO DE SESIÓN DEL SISTEMA WEB.

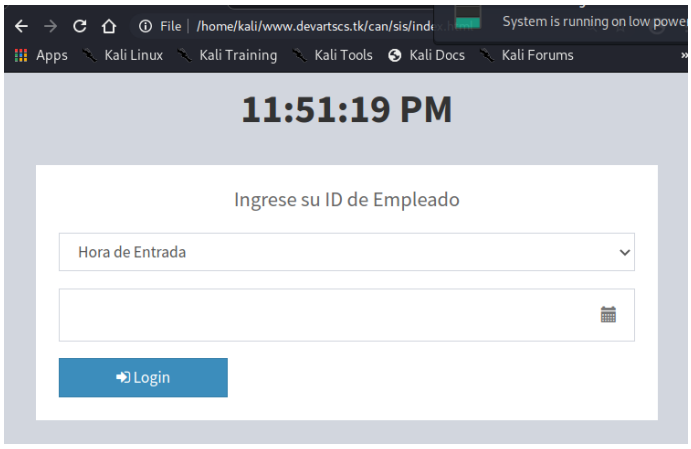


FIGURA N° 21: FORMULARIO DE MARCACIÓN DE ASISTENCIA DE COLABORADORES.

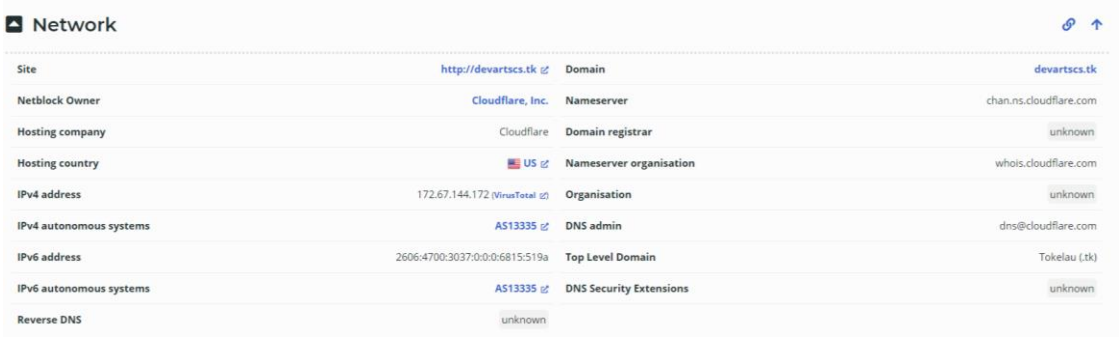
WHOIS

Se utilizó WHOIS como parte del reconocimiento pasivo mediante el dominio del sitio web. El reconocimiento pasivo hace una recolección de toda la información disponible de manera pública relacionada al dominio. Luego de la ejecución del comando whois devartscs.tk se obtienen datos del lugar de procedencia del dominio como se muestra en la Figura N° 22.

FIGURA N° 22: DATOS DEL LUGAR DE REGISTRO DEL DOMINIO.

NETCRAFT

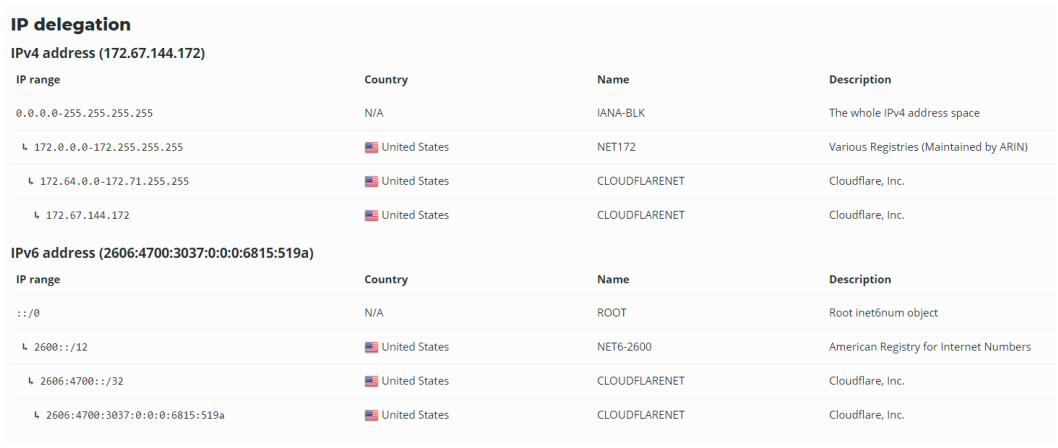
La herramienta Netcraft también fue utilizada para realizar el reconocimiento pasivo. Obteniendo como resultados datos de la red ver Figura N° 23, direcciones IP del servidor web, ver Figura N° 24 y principalmente que el sitio no cuenta con certificado SSL/TLS calificándolo como inseguro ver Figura N° 25.



Network

Site	http://devartscs.tk	Domain	devartscs.tk
Netblock Owner	Cloudflare, Inc.	Nameserver	chan.ns.cloudflare.com
Hosting company	Cloudflare	Domain registrar	unknown
Hosting country	US	Nameserver organisation	whois.cloudflare.com
IPv4 address	172.67.144.172 (VirusTotal)	Organisation	unknown
IPv4 autonomous systems	AS13335	DNS admin	dns@cloudflare.com
IPv6 address	2606:4700:3037:0:0:0:6815:519a	Top Level Domain	Tokelau (.tk)
IPv6 autonomous systems	AS13335	DNS Security Extensions	unknown
Reverse DNS	unknown		

FIGURA N° 23: SE MUESTRA EL NOMBRE DEL SERVIDOR PERTENECE A CLOUDFLARE INC.



IP delegation

IPv4 address (172.67.144.172)

IP range	Country	Name	Description
0.0.0.0-255.255.255.255	N/A	IANA-BLK	The whole IPv4 address space
↳ 172.0.0.0-172.255.255.255	United States	NET172	Various Registries (Maintained by ARIN)
↳ 172.64.0.0-172.71.255.255	United States	CLOUDFLARENET	Cloudflare, Inc.
↳ 172.67.144.172	United States	CLOUDFLARENET	Cloudflare, Inc.

IPv6 address (2606:4700:3037:0:0:0:6815:519a)

IP range	Country	Name	Description
::/0	N/A	ROOT	Root inet6num object
↳ 2600::/12	United States	NET6-2600	American Registry for Internet Numbers
↳ 2606:4700::/32	United States	CLOUDFLARENET	Cloudflare, Inc.
↳ 2606:4700:3037:0:0:0:6815:519a	United States	CLOUDFLARENET	Cloudflare, Inc.

FIGURA N° 24: SE EVIDENCIA EL RANGO DE DIRECCIONES IP QUE HACEN USO DEL DOMINIO.

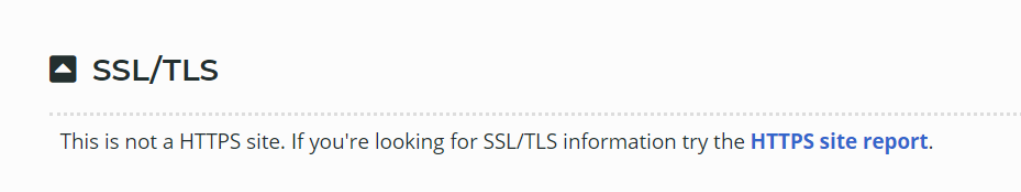


FIGURA N° 25: SE EVIDENCIA QUE EL SITIO NO CUENTA CON CERTIFICADO SSL/TLS.

FASE 2: Escaneo

NMAP

Se realizó un primer escaneo con la herramienta NMAP para conocer los puertos en funcionamiento y servicios que se encuentran disponibles. Nmap utiliza el protocolo TCP para realizar el descubrimiento también conocido como Discovery. TCP está orientado a la conexión y garantiza la conectividad de un punto a otro, por medio del saludo de tres vías SYN (saludo), SYN (saludo de retorno)+ACK (confirmación de recepción), ACK (confirmación) y finaliza la comunicación con FIN ACK en el origen y FIN ACK en el destino. Basado en ello se obtuvo el listado de puertos y servicios en respuesta luego del barrido de puertos de acuerdo a la Figura N° 26.

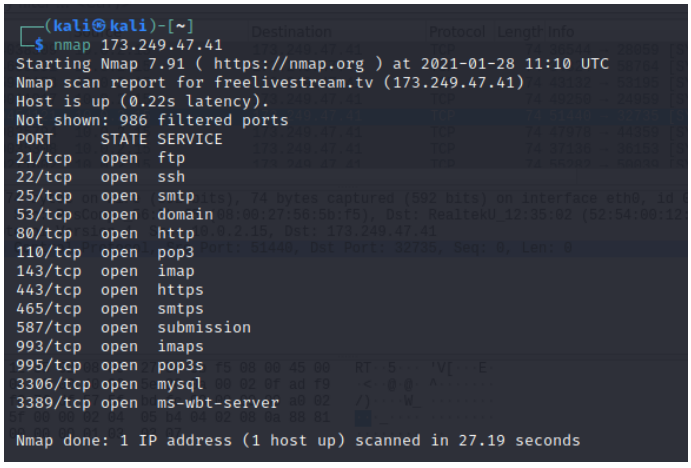


FIGURA N° 26: LISTADO DE PUERTOS EN FUNCIONAMIENTO.

NMAP Scripting

El motor de Scripts de NMAP permite utilizar los diferentes parámetros o recursos disponibles propios de la herramienta, automatizar tareas u otros. El script banner de NMAP obtiene la cabecera de la información que se envía a través de los primeros paquetes que se iniciado una comunicación TCP después que se completa el saludo de 3 vías envía información sobre el puerto. El script recorre todos los puertos que estén disponibles y recoge todos los banner para brindar mayor información sobre los servicios que están ejecutándose. Luego de ejecutar el comando *nmap –script banner <ip>* se muestran las versiones y otros detalles de los diferentes servicios como muestran la Figura N° 27 y 28.

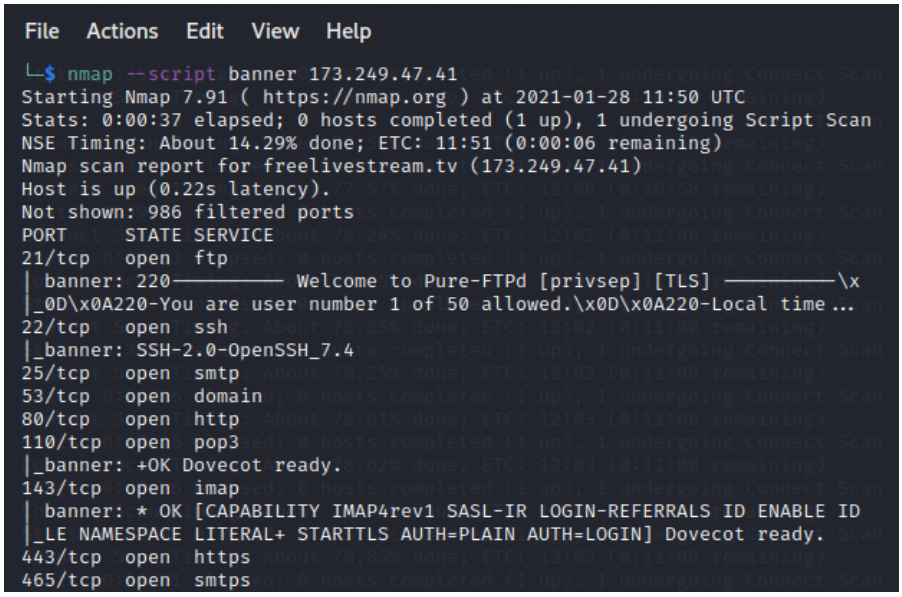


FIGURA N° 27: DESCRIPCIÓN DEL BANNER DE LOS PUERTOS 21, 22, 25, 53,80, 110, 143, 443 Y 465

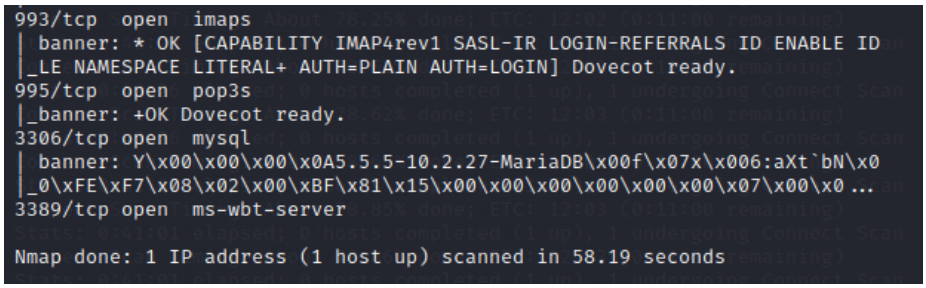


FIGURA N° 28: DESCRIPCIÓN DEL BANNER DE LOS PUERTOS 993, 995, 3306 Y 3389

Otra script de Nmap es *vuln*, el cual permite realizar un primer análisis de vulnerabilidades de la máquina, luego de la ejecución del comando nmap –script vuln <ip> se muestran los puertos filtrados, ver Figura N° 29.

FIGURA N° 29: PUERTO 21, 22, 25 Y 53 FILTRADOS POR VULN.

Se obtuvo el hallazgo de 1 vulnerabilidad en el puerto 80 de la cual podría ser aprovechada por Slowloris DDOS Attack, ver Figura N° 30.

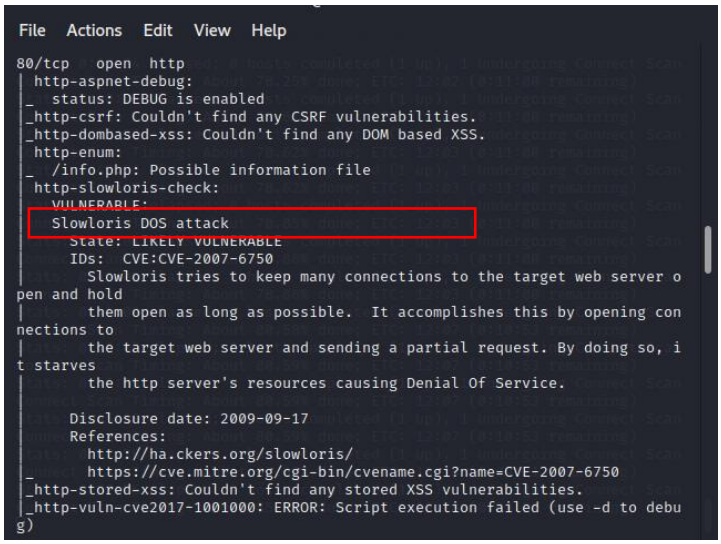


FIGURA N° 30: PUERTO 80 VULNERABLE A ATAQUE SLOWLORIS DOS.

El puerto 443 utilizado por HTTPS también se identificó la vulnerabilidad susceptible a Ataque Slowloris DOS. Ver Figura N° 31.

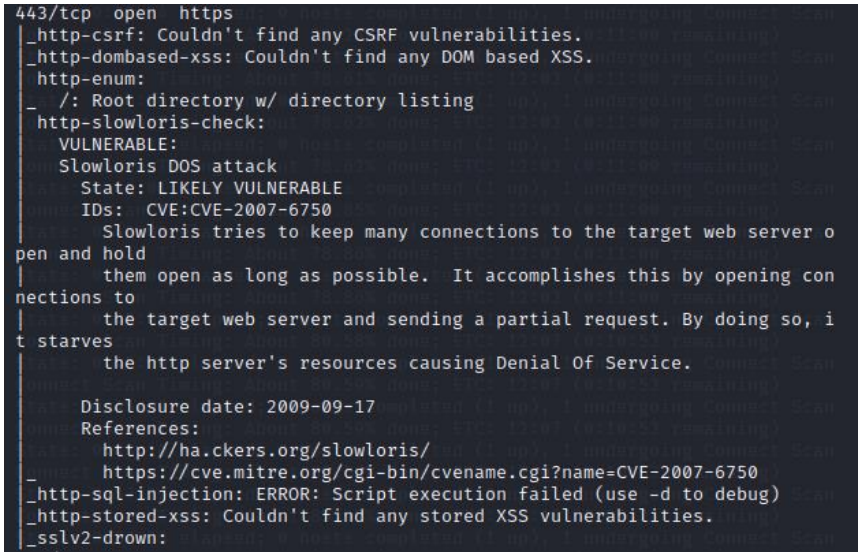


FIGURA N° 31: PUERTO 443 VULNERABLE A ATAQUE SLOWLORIS DOS.

Por otro lado se encontró la vulnerabilidad susceptible a explotación del cifrado criptográfico Diffie-Hellman Key Exchange en el puerto 110 que utiliza el protocolo pop3. Diffie-Hellman permite negociar una conexión segura en muchos protocolos como HTTPS, SSH, IPSEC, SMTP y otros. El ataque LOGJAM se aprovecha de la longitud de llave pública, siendo actualmente una llave de 2048 bits. La longitud actual de la llave es de 1024 bits como se muestra en la Figura N° 32.

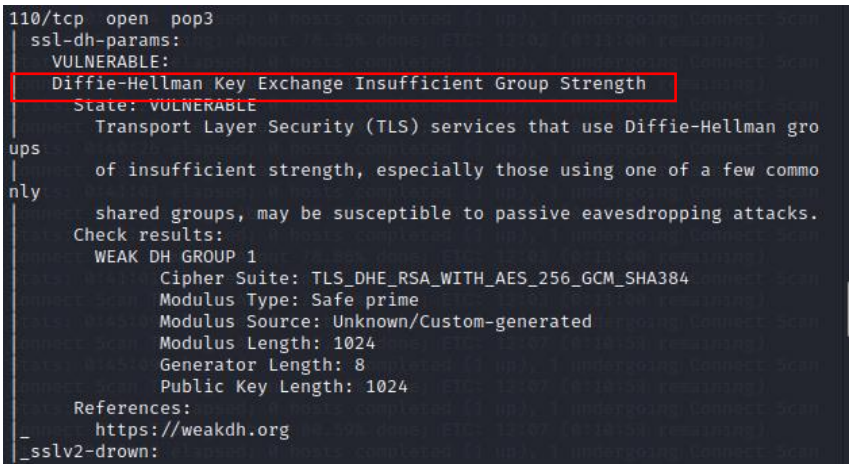


FIGURA N° 32: DIFFIE-HELLMAN KEY EXCHANGE VULNERABILIDAD EN EL PUERTO 110.

El Puerto 142 utilizado por IMAP presenta una vulnerabilidad que podría ser aprovechada por el ataque LOGJAM que permite a un atacante intermediario o *man in the middle* que degrada las conexiones TLS vulnerables a criptografía de grado de exportación de 512 bits. Ver Figura N° 33.

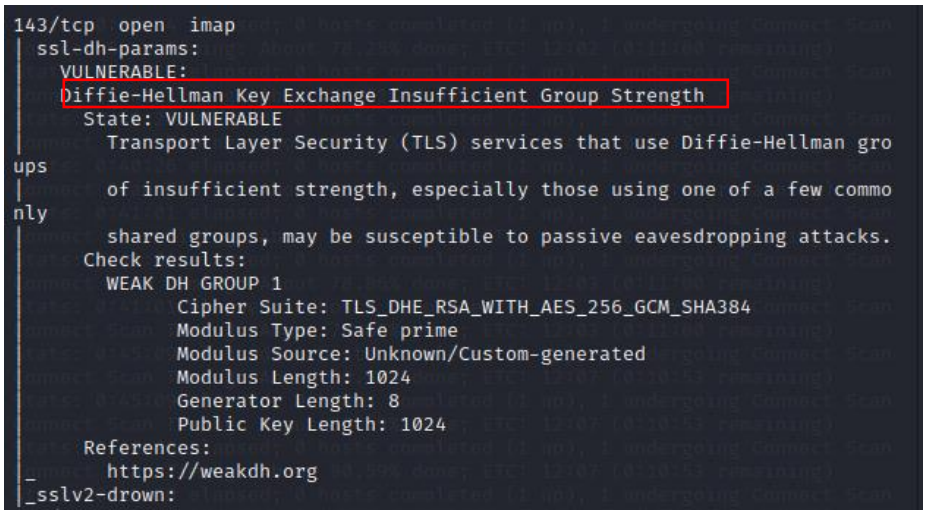


FIGURA N° 33: DIFFIE-HELLMAN KEY EXCHANGE VULNERABILIDAD EN EL PUERTO 143.

El puerto 993 IMAPS, 995 POP3S tal como se muestra en las Figuras N° 34 y 35 evidencias la misma vulnerabilidad.

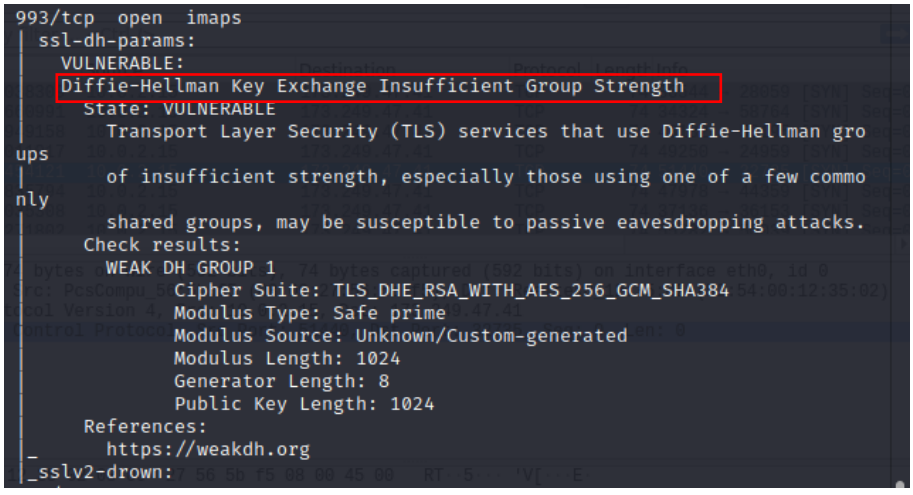


FIGURA N° 34: DIFFIE-HELLMAN KEY EXCHANGE VULNERABILIDAD EN EL PUERTO 993.

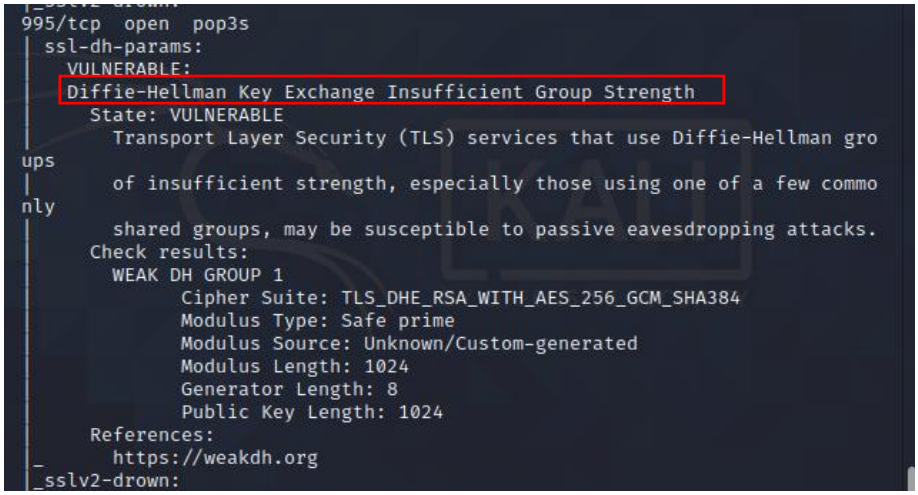


FIGURA N° 35: DIFFIE-HELLMAN KEY EXCHANGE VULNERABILIDAD EN EL PUERTO 995.

El puerto 465 utilizado por SMTPS y 587 SMTP presentan la vulnerabilidad CVE2010-4344 con una variante del 2018. Consiste en el desbordamiento de búfer que permite a atacantes remotos ejecutar código arbitrario a través de una sesión SMTP que incluye dos comandos MAIL junto con un mensaje grande que contiene encabezados elaborados. Ver Figura N° 36.

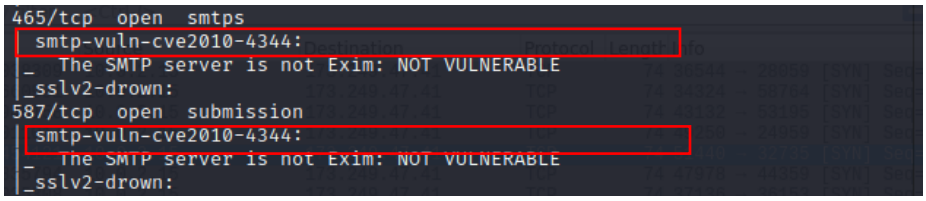


FIGURA N° 36: PUERTO 465 Y 587 VULNERABLE A CVE2010-4344.

El puerto 3306 utilizado por MYSQL tiene la vulnerabilidad CVE2012-2122 puede afectar a todas las versiones 5.1.61, 5.2.11, 5.3.5, 5.5.22 y anteriores de los motores de base datos MySQL y MariaBD, que permite a un atacante evadir la autenticación de la base de datos. Ver Figura N° 37.

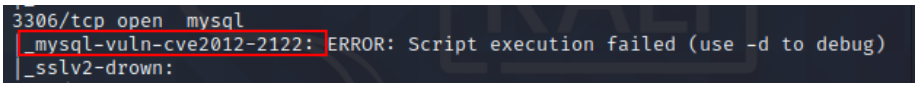


FIGURA N° 37: PUERTO 3306 VULNERABLE A CVE2012-2122.

Respecto al puerto 3389 utilizado por RDP Remote Desktop Protocol, la vulnerabilidad CVE-2012-020 no procesa correctamente los paquetes en la memoria, lo que permite a atacantes remotos ejecutar código arbitrario mediante el envío de paquetes RDP modificados. Ver Figura N° 38.

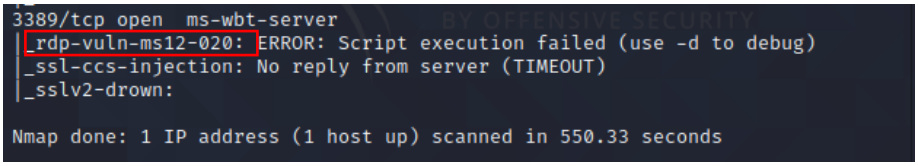


FIGURA N° 38: PUERTO 3389 VULNERABLE A CVE-2012-020.

NIKTO

NIKTO escanea las vulnerabilidades en busca de archivos peligrosos, software desactualizado y otros fallos. Se ejecutó el comando *sudo nikto –h <ip>* para realizar la búsqueda. Se obtuvo que no existe una definición de protección contra XSS. Ver Figura N° 39.

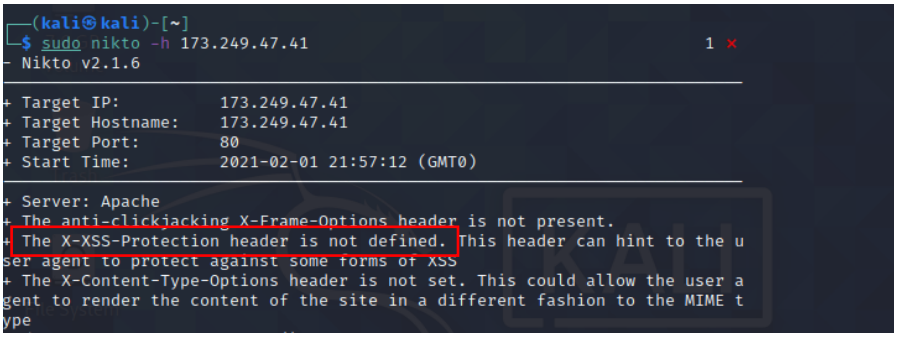


FIGURA N° 39: LA CABECERA NO DEFINE PROTECCIÓN CONTRA XSS.

Se encontró directorios del sistema web indexados como muestra la Figura N° 40.

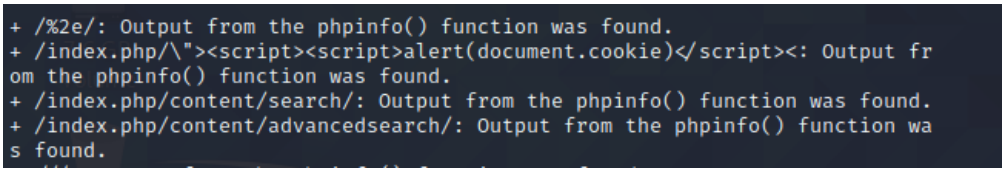


FIGURA N° 40: LOS DIRECTORIOS INDEXADOS SON PÚBLICOS.

FASE 3. Explotación de vulnerabilidades

Se realizó un análisis a la entrada de datos de los formularios de inicio de sesión del sistema interno y al formulario de marcación de asistencia.

INYECCIONES SQL

Mediante el uso de código SQL se realizaron pruebas para lograr acceso mediante el formulario de inicio de sesión del sistema web interno. El uso de nombres de usuario y contraseña muy comunes es bastante utilizado por usuarios. Se verificó que el nombre de usuario admin existe dentro de la base de datos, se logró realizar mediante una consulta al listado de nombres de usuarios más utilizados. Ver Figura N° 41.

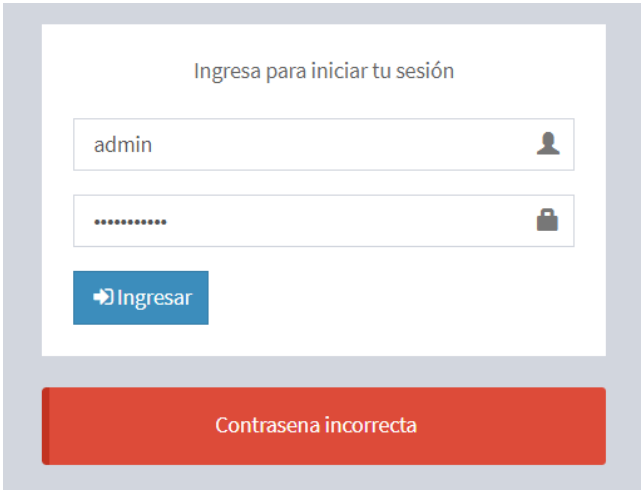


FIGURA N° 41: INICIO DE SESIÓN CON NOMBRE DE USUARIO ADMIN.

Mediante la verificación de una sentencia verdadera 0 = 0 logramos validar que no requerimos el nombre de usuario para conocer la contraseña. Ver Figura N° 42.

FIGURA N° 42: USO DE INYECCIÓN SQL PARA CONSEGUIR INFORMACIÓN ADICIONAL.

Para obtener más datos se ingresando otras consultas SQL dando como resultados la obtención de la cantidad de campos de la tabla que almacena a los usuarios, para ello se ingresa *%' or '0' = '0' unión select null, null, null, versión()*. El uso del símbolo % permite ingresar. Ver Figura N° 43.

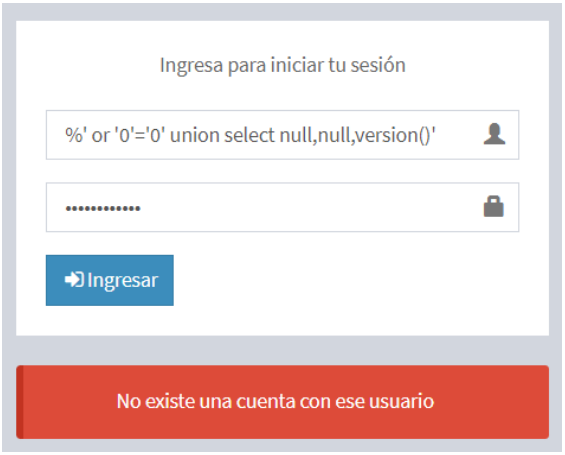


FIGURA N° 43: INGRESO DE CÓDIGO SQL.

Se determina que existen siete campos en la tabla que almacena a los usuarios. Ya que el mensaje de salida indica que la contraseña es incorrecta por tanto el valor introducido en el campo nombre de usuario resulta verdadero. Ver Figura N° 44.

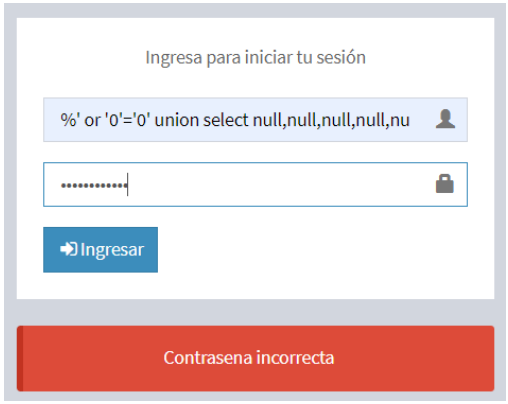


FIGURA N° 44: CONFIRMACIÓN DE LOS 7 CAMPOS DE LA TABLA USUARIOS.

Si ingresamos nuevamente el código SQL la devolución es un listado de los datos del usuario *admin.* Se muestra la devolución de datos desde la base de datos como resultado de la consulta de usuario. Ver Figura 45.

FIGURA N° 45: FILA DE DATOS DEL USUARIO ADMIN.

Finalmente para verificar los datos completos que se han devuelto, inspeccionamos el código dentro de navegador como muestra la Figura N° 46. Se evidencia que la contraseña almacenada en la base de datos no se encuentra encriptada.

FIGURA N° 46: DATOS DEVUELTOS LUEGO DE LA CONSULTA SQL.

Finalmente se logró acceder mediante el usuario y contraseña obtenida a través de la inyección de código SQL. Ver Figura N° 47.

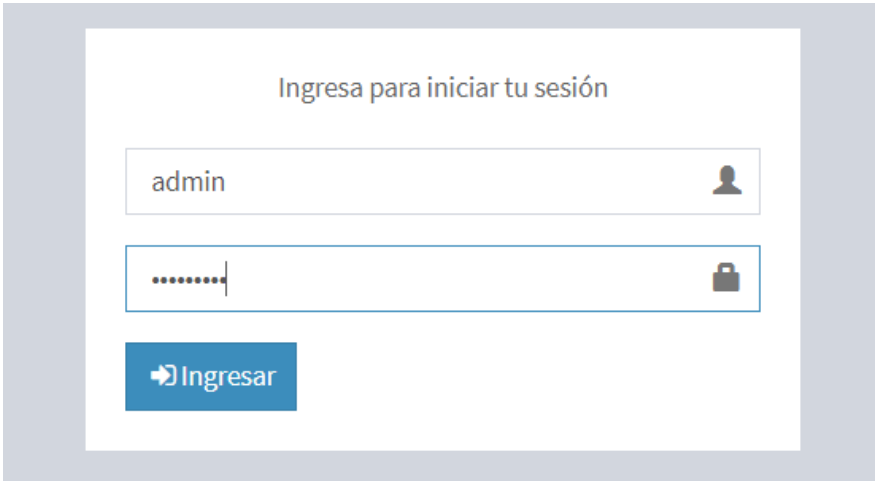


FIGURA N° 47: INICIO DE SESIÓN CON EL NOMBRE DE USUARIO Y CONTRASEÑA OBTENIDA.

Resumen de vulnerabilidades encontradas:

Luego de la ejecución de cada una de las fases se analizó la información obtenida dando como resultados el listado de vulnerabilidades que se muestran en la tabla N° 2.

N°	Vulnerabilidad	Descripción	Origen	Herramienta	Calificación
1	El sitio permite la réplica de sus archivos.	La clonación o replica de sitios web permite la copia del mismo pero no es absoluto ya que cambia de servidor web al subirse nuevamente a Internet.	Fase Reconocimiento	Httrack	
2	El sitio no cuenta con un certificado SSL/TLS.	Un certificado SSL/TLS asegura la transmisión encriptada de datos punto a punto.	Fase Reconocimiento	Netcraft	
3	Puerto 80 y 443 vulnerables a ataque DDOS. CVE_2007_6750	El servidor Apache permite es susceptible a ataque de denegación de servicios a través de una petición HTTP.	Fase Escaneo	Nmap Scripting y Vuln	
4	Puertos 110, 142, 993 y 995 con vulnerabilidad Diffie-	El intercambio de claves Diffie-Hellman es un algoritmo criptográfico que permite que los	Fase Escaneo	Nmap Scripting y Vuln	

	Hellman Key Exchange	protocolos de Internet acuerden una clave compartida y negocien una conexión segura. La vulnerabilidad presente permite al atacante leer y modificar la data que pasa por la conexión generada.			
5	Vulnerabilidad CVE2012-2122 presente en MySql.	Este bug permite el acceso del atacante saltándose la etapa de autenticación a la base de datos. Las versiones afectadas son todas las versiones anteriores a 5.5 en MySQL y MariaBD.	Fase Escaneo	Nmap Scripting y Vuln	
6	Vulnerabilidad CVE-2012-020 presente en el protocolo RDF.	Windows Server 2008 SP2, R2 y R2 SP1 y Windows 7 SP1 tiene un fallo que permite a atacantes ejecutar código arbitrario mediante el envío de paquetes RDP modificados.	Fase Escaneo	Nmap Scripting y Vuln	
7	No se ha definido la protección contra XSS	La protección contra código mediante JavaScript u otro lenguaje en el sitio no se ha bloqueado. El	Fase Escaneo	Nikto	

		código malicioso puede seguir ejecutándose aún después de realizado el ataque.			
8	Los directorios indexados se encuentran públicos.	Los directorios que no son públicos se encuentran disponibles, a los cuales se puede acceder a través de la URL, visualizando archivos internos.	Fase Escaneo	Nikto	
9	El formulario de inicio de sesión no está protegido contra inserción de código SQL.	El formulario permite el ingreso de código SQL dando como resultado la devolución de los datos consultados a través del campo de entradas de datos.	Fase Explotación	Comandos SQL	
10	Las contraseñas de la base de datos no están encriptadas.	Las contraseñas son considerados datos sensibles por los que deben ser encriptadas. Se recomienda utilizar encriptación superior a SHA1.	Fase Explotación	Comandos SQL	

TABLA N° 2: CALIFICACIÓN DE VULNERABILIDADES POR NIVEL DE GRAVEDAD.

Leyenda de la clasificación de las vulnerabilidades encontradas:

Descripción	Calificación	Color
Vulnerabilidad débil o muy compleja de aprovechar. Causa un impacto mínimo.	Baja	
Vulnerabilidad moderada que compromete moderadamente uno o más principios de seguridad. Causa un impacto menor.	Moderada	
Vulnerabilidades más peligrosas. Afecta a un nivel alto los principios CIA. Cauda un impacto moderado.	Importante	
Fallo de seguridad crítico. Compromete gravemente los principios CIA. Causa un grave impacto.	Crítica	

TABLA N° 3: LEYENDA DE CLASIFICACIÓN DE VULNERABILIDADES DE ACUERDO A NIVEL DE GRAVEDAD.

4.1.3 MATRIZ DE RIESGOS INICIAL

Se asocia cada vulnerabilidad a una o más amenazas que podrían aprovecharse de la misma, también se relaciona al principio de seguridad de la información que afecta principalmente tal como se muestra en las Tablas N° 4 al 13. La probabilidad de ocurrencia y el nivel de impacto se definen mediante una escala de 5, ver Tabla N° 3.

		Impacto				
		Poco Significativo	**Menor**	**Moderado**	**Mayor**	**Catastrófico**
Probabilidad	**Casi Seguro**	**Medio**	**Alto**	**Alto**	**Muy Alto**	**Muy alto**
	Probable	**Medio**	**Medio**	**Alto**	**Alto**	**Muy Alto**
	Posible	**Bajo**	**Medio**	**Medio**	**Alto**	**Alto**
	Improbable	**Bajo**	**Bajo**	**Medio**	**Medio**	**Medio**
	Raro	**Bajo**	**Bajo**	**Bajo**	**Medio**	**Medio**

TABLA N° 4: LEYENDA DE IMPACTO X OCURRENCIA

1	**Activo:** Sistema Web	**Afecta:** Confidencialidad
Descripción: El sistema web permite la réplica de sus archivos mediante el uso de herramientas de software de clonación. La clonación de sitios web engaña a los usuarios, mostrando una web como si fuera la original, el objetivo es obtener		

credenciales de los usuarios para luego acceder a la información de ellos.	
Amenaza: Clonación de una web **Riesgo:** Suplantación de la web de la empresa para obtener credenciales de acceso. **(R1)**	
Probabilidad: Probable	**Impacto:** Mayor

TABLA N° 5: TABLA DE RIESGOS ASOCIADA A LA VULNERABILIDAD 1.

2	**Activo:** Sistema Web	**Afecta:** Integridad y confidencialidad
Descripción: El sitio no cuenta con un certificado SSL/TLS el cual sirve para mantener encriptados los datos que viajan a través de la red. El sitio es inseguro y los ciberdelincuentes aprovechan interceptar la información que se transmite punto a punto. El protocolo SSL/TLS cifra los nombres de usuario, contraseñas, u otros datos sensibles cuando se envían a través de la red.		
Amenaza: Man in the Middle, Malware **Riesgo:** Pérdida y/o robo de información que navega a través de la red. **(R2)**		
Probabilidad: Casi seguro	**Impacto:** Mayor	

TABLA N° 6: TABLA DE RIESGOS ASOCIADA A LA VULNERABILIDAD 2.

3	**Activo:** Servidor Web	**Afecta:** Disponibilidad

Descripción: Los puerto 80 y 443 son vulnerables a ataque DDOS, especialmente Slowloris DDOS Attack que permite a un atacante sobrecargar un servidor objetivo abriendo y manteniendo muchas conexiones HTTP simultáneas entre el atacante y el objetivo.	
Amenaza: Slowloris DDOS Attack **Riesgo:** No disponibilidad del sistema web. **(R3)**	
Probabilidad: Probable	**Impacto:** Mayor

TABLA N° 7: TABLA DE RIESGOS ASOCIADA A LA VULNERABILIDAD 3.

4	**Activo:** Sistema Web	**Afecta:** Confidencialidad
Descripción: Los puertos 110, 142, 993 y 995 con vulnerabilidad Diffie-Hellman Key Exchange. La vulnerabilidad Logjam permite a un atacante debilitar la complejidad del cifrado y, en consecuencia, descifrar los datos fácilmente sin el conocimiento del usuario. El cifrado vulnerable es el que va de 512 a 1024 bits.		
Amenaza: Ataque LOGJAM **Riesgo:** Robo de información que transita por los puertos vulnerables. **(R4)**		
Probabilidad: Posible	**Impacto:** Mayor	

TABLA N° 8: TABLA DE RIESGOS ASOCIADA A LA VULNERABILIDAD 4.

5	**Activo:** Base de Datos MySQL	**Afecta:** Confidencialidad
Descripción: La vulnerabilidad CVE2012-2122 presente en MySql permite conceder el acceso a un atacante utilizar la misma contraseña incorrecta repetidamente y eventualmente provoca una comparación de token con resultado de éxito en una variable de retorno no válida.		
Amenaza: Exploit **Riesgo:** Robo o pérdida de información de la Base de Datos. **(R5)**		
Probabilidad: Improbable debido a la complejidad del ataque.	**Impacto:** Mayor	

TABLA N° 9: TABLA DE RIESGOS ASOCIADA A LA VULNERABILIDAD 5.

6	**Activo:** Servidor Web	**Afecta:** Confidencialidad
Descripción: La vulnerabilidad CVE-2012-020 presente en el protocolo RDF no procesa correctamente los paquetes en la memoria, lo que resulta ejecutar código arbitrario mediante envío de paquetes RDP. Por defecto, RDP no está habilitado en sistemas operativos Windows. Es un riesgo tener habilitado RDP.		
Amenaza: Exploit **Riesgo:** Obtener acceso a través del puerto 3389. **(R6)**		
Probabilidad: Posible	**Impacto:** Moderado	

TABLA N° 10: TABLA DE RIESGOS ASOCIADA A LA VULNERABILIDAD 6.

7	**Activo:** Sistema Web	**Afecta:** Confidencialidad
Descripción: No se ha definido la protección contra XSS en la cabecera del sitio. El XSS puede redirigir a otro sitio para robar información del usuario o puede insertar código HTML para descargar malware y se ejecute en el sistema del usuario.		
Amenaza: Cross Site Scripting **Riesgo:** Engaño a los usuarios y daño reputacional a la empresa. **(R7)**		
Probabilidad: Posible		**Impacto:** Mayor

TABLA N° 11: TABLA DE RIESGOS ASOCIADA A LA VULNERABILIDAD 7.

8	**Activo:** Sistema Web	**Afecta:** Confidencialidad
Descripción: Los directorios indexados se encuentran públicos. Dichos directorios son accesibles a todos aquellos que agreguen al dominio la ruta de carpetas. El sistema web debe mantener protegidos dichos directorios. Los directorios expuestos contienen imágenes y otros recursos multimedia.		
Amenaza: Buscadores de directores indexados **Riesgo:** Robo de información de los directorios públicos. **(R8)**		
Probabilidad: Posible		**Impacto:** Moderado

TABLA N° 12: TABLA DE RIESGOS ASOCIADA A LA VULNERABILIDAD 8.

9	**Activo:** Sistema web	**Afecta:** Confidencialidad e integridad
Descripción: El formulario de inicio de sesión no está protegido contra inserción de código SQL. Permite el ingreso de comandos SQL y muestra como resultados las consultas que se realizan. La ejecución de sentencias SQL están codificadas en el código del sistema, no se utilizaron procedimientos almacenados u otras técnicas para mantener separado los comandos SQL del lenguaje de programación del sistema.		
Amenaza: Inyección SQL **Riesgo:** Robo o pérdida de datos de la BD. **(R9)**		
Probabilidad: Probable	**Impacto:** Mayor	

TABLA N° 13: TABLA DE RIESGOS ASOCIADA A LA VULNERABILIDAD 9.

10	**Activo:** Base de Datos	**Afecta:** Confidencialidad
Descripción: Las contraseñas de la base de datos no están encriptadas. Los datos sensibles dentro de una base de datos deben estar encriptados, a fin de asignarles una capa adicional de seguridad. Otros datos sensibles deben estar encriptados a fin de asegurar la Protección de Datos Personales.		
Amenaza: Captura de datos vulnerables por parte de ciberdelincuentes **Riesgo:** Violación a la Protección de Datos Personales y Sensibles. **(R10)**		
Probabilidad: Probable	**Impacto:** Mayor	

TABLA N° 14: TABLA DE RIESGOS ASOCIADA A LA VULNERABILIDAD 10.

Luego del análisis de cada vulnerabilidad se ubica su riesgo asociado en la Matriz de Riesgo Inicial, esta matriz revela el estado actual de la seguridad de la información del sistema web sin la aplicación de los controles de seguridad apropiados. Se entiende como controles a todas aquellas medidas, técnicas, herramientas u otros que se aplicaran ya sean a nivel de software, hardware, procedimiento o personas para reducir el nivel de impacto de la materialización del riesgo asociado. Ver Tabla N° 15.

		Impacto				
		Poco Significativo (1)	**Menor (2)**	**Moderado (3)**	**Mayor (4)**	**Catastrófico (5)**
Probabilidad	**Casi Seguro (5)**				**(R2)**	
	Probable (4)				**(R9) (R10) (R3) (R1)**	
	Posible (3)			**(R6) (R8)**	**(R7) (R4)**	
	Improbable (2)				**(R5)**	
	Raro (1)					

TABLA N° 15: MATRIZ DE RIESGOS INICIAL.

4.1.4 MATRIZ DE RIESGO RESIDUAL

Los controles de Seguridad recomendados a la empresa se detallan en las Tablas N° 16 al 25:

1	**Riesgo: R1**	**Principio:** Confidencialidad
Control Recomendado: Se recomienda realizar el bloqueo de crawlers o rastreadores en el archivo robots.txt que se encuentra en el directorio raíz del sitio web. Se sugiere elaborar un listado de crawlers conocidos. Mediante el siguiente código se bloquea el uso de WGET que realiza la descarga. *User-agent: wget* *Disallow: /* Otra opción recomendable es editar el archive HTACCES y añadir la lista de crawlers más conocidos y los que se van reconociendo a fin de bloquearlos. **Dirigido a :** Gerente de Devhuayra SAC		
Probabilidad: Improbable		**Impacto:** Moderado

TABLA N° 16: CONTROL RECOMENDADO PARA EL RIESGO 1.

2	**Riesgo: R2**	**Principio:** Integridad y confidencialidad
Control Recomendado: Se recomienda con sum urgencia instalar un certificado de seguridad SSL/TLS versión 3. El certificado de seguridad permite la comunicación cifrada de un punto a punto, garantiza la privacidad de datos. SSL/TLS funciona mediante una llave pública y privada las cuales se utilizan para crear una clave de sesión en la comunicación inicial. Luego esta última clave se utilizará para cifrar y descifrar los datos que se intercambien. El uso del certificado radica principalmente para asegurar la autenticación, trasmitir datos seguros y cumplir con estándares o normas respecto a la protección de datos.		

Dirigido a : Gerente de Devhuayra SAC	
Probabilidad: Improbable	**Impacto:** Moderado

TABLA N° 17: CONTROL RECOMENDADO PARA EL RIESGO 2.

3	**Riesgo: R3**	**Principio:** Disponibilidad
Control Recomendado: Para la protección de ataques DDOS y DOS se utiliza un firewall de aplicaciones web (WAF), monitoreo constante de la red y otras acciones que detecten tráfico inusual .En el caso del R3 es susceptible a Slowloris DDOS Attack el cual puede mitigarse siguiendo las siguientes recomendaciones: limitar el números de conexiones solo a IPs permitidas y restringir el tiempo de conexión que es permitido a un cliente. Así mismo emplear los siguientes módulos de Apache Web Server que están diseñados para la protección DOS: Mod_limitipconn, Mod_qos, Mod_evasive, Mod_security, Mod_noloris y Mod_antiloris. **Dirigido a :** Gerente de Devhuayra SAC		
Probabilidad: Improbable		**Impacto:** Moderado

TABLA N° 18: CONTROL RECOMENDADO PARA EL RIESGO 3.

4	**Riesgo: R4**	**Principio:** Confidencialidad
Control Recomendado: Los puertos 110, 142, 993 y 995 con vulnerabilidad Diffie-Hellman Key Exchange, por ello se recomienda utilizar 2048 bits o más		

para todas las claves del certificado SSL/TLS. Por el lado del cliente se recomienda actualizar los navegadores a las versiones más recientes. **Dirigido a :** Gerente de Devhuayra SAC
Probabilidad: Posible | **Impacto:** Menor

TABLA N° 19: CONTROL RECOMENDADO PARA EL RIESGO 4.

5	**Riesgo: R5**	**Principio:** Confidencialidad
Control Recomendado: Se recomienda mantener actualizado con los parches de seguridad para la base de datos de MySQL y MariaBD. No utilizar las versiones 5.1.61, 5.2.11, 5.3.5, 5.5.22 y anteriores. Por otro lado los sistemas vulnerables Ubuntu Linux 64-bit 10.04, 10.10, 11.04, 11.10, 12.04, OpenSuSE 12.1 64-bit MySQL 5.5.23-log y Fedora 16 64-bit. Se recomienda revisar los sitios web oficiales de los diferentes sistemas operativos y motores de base de datos para instalar los parches de seguridad que se van generando cada periodo. **Dirigido a :** Gerente de Devhuayra SAC		
Probabilidad: Raro		**Impacto:** Moderado

TABLA N° 20: CONTROL RECOMENDADO PARA EL RIESGO 5.

6	**Riesgo: R6**	**Principio:** Confidencialidad
Control Recomendado: Se recomienda mantener actualizado los sistemas operativos Windows. Instalar todos los parches de seguridad que se lanzan		

periódicamente. Por otro lado los sistemas Windows por defecto no tienen habilitada el protocolo RDP. Configurar el firewall de Windows para evitar accesos no autorizados. Si no se utiliza la conexión remota es recomendable mantener desactivado dicho protocolo. No utilizar versiones de Windows que han dejado de recibir soporte y actualizaciones. **Dirigido a :** Gerente de Devhuayra SAC	
Probabilidad: Raro	**Impacto:** Moderado

TABLA N° 21: CONTROL RECOMENDADO PARA EL RIESGO 6.

7	**Riesgo: R7**	**Principio:** Confidencialidad
Control Recomendado: Se recomienda utilizar el módulo Mod_security de Apache Web Server para el filtrado de peticiones. Por otro lado el encabezado de respuesta HTTP X-XSS-Protection es una característica de navegadores actuales, restringe la carga de un sitio cuando detecta ataques XSS. Se recomienda utilizar navegadores actuales ya que implementan Content-Security-Policy. CSP es un estándar de seguridad informática que evita y detecta la ejecución de código malicioso en el contenido de sitios web. **Dirigido a :** Gerente de Devhuayra SAC		
Probabilidad: Improbable	**Impacto:** Menor	

TABLA N° 22: CONTROL RECOMENDADO PARA EL RIESGO 7.

8	**Riesgo: R8**	**Principio:** Confidencialidad
Control Recomendado: Se recomienda a través de Cpanel ingresar a la opción Administración de Directorios y cambiar la configuración de los directorios a "No indexar". Por otro lado también se recomienda la restringir el acceso desde Htaccess utilizando el redireccionamiento a una ruta en específico. **Dirigido a :** Gerente de Devhuayra SAC		
Probabilidad: Improbable		**Impacto:** Menor

TABLA N° 23: CONTROL RECOMENDADO PARA EL RIESGO 8.

9	**Riesgo: R9**	**Afecta:** Confidencialidad e integridad
Control Recomendado: Se recomienda crear listas blancas para filtrar las entradas de usuario. Por otro lado es recomendable utilizar procedimientos almacenados para interactuar con la base de datos donde se definen parámetros específicos para el tratamiento de datos. Así mismo utilizar códigos captchas en los formularios para validar las peticiones del usuario. De acuerdo al lenguaje de programación y tecnologías que se hayan utilizado para la construcción de la web se recomienda convertir caracteres especiales con htmlspecialchars y escapar caracteres especiales con addslashes. **Dirigido a :** Gerente de Devhuayra SAC		
Probabilidad: Posible		**Impacto:** Moderado

TABLA N° 24: CONTROL RECOMENDADO PARA EL RIESGO 9.

10	**Riesgo: R10**	**Afecta:** Disponibilidad
Control Recomendado: Se recomienda encriptar los datos sensibles de la base de datos a fin de proteger la privacidad de los usuarios y clientes. Además el cifrado de datos ofrece una capa adicional de seguridad y un nivel extra de complejidad para descifrarlo. Así mismo es muy importante realizar copias de seguridad a la base de datos y mantener a salvo. **Dirigido a :** Gerente de Devhuayra SAC		
Probabilidad: Posible		**Impacto:** Moderado

TABLA N° 25: CONTROL RECOMENDADO PARA EL RIESGO 10.

Finalmente, la Matriz de Riesgo Residual se construye a través de la evaluación del impacto y la probabilidad de ocurrencia de la materialización de los riesgos luego de aplicados los controles. Ver Tabla N° 26.

		Impacto				
		Poco Significativo (1)	**Menor (2)**	**Moderado (3)**	**Mayor (4)**	**Catastrófico (5)**
Probabilidad	**Casi Seguro (5)**					
	Probable (4)					
	Posible (3)		**(R4)**	**(R10) (R9)**		
	Improbable (2)		**(R8) (R7)**	**(R1) (R3) (R2)**		
	Raro (1)			**(R5) (R6)**		

TABLA N° 26: MATRIZ DE RIESGOS RESIDUAL.

4.1.5 RESULTADOS

La clasificación de vulnerabilidades según la gravedad muestra que se identificaron 4 vulnerabilidades de tipo Crítica que representa el 40%, 1 vulnerabilidad tipo importante 10%, 3 vulnerabilidades de tipo moderado que ocupa un 30% y 2 vulnerabilidades de nivel bajo con un porcentaje del 20%.

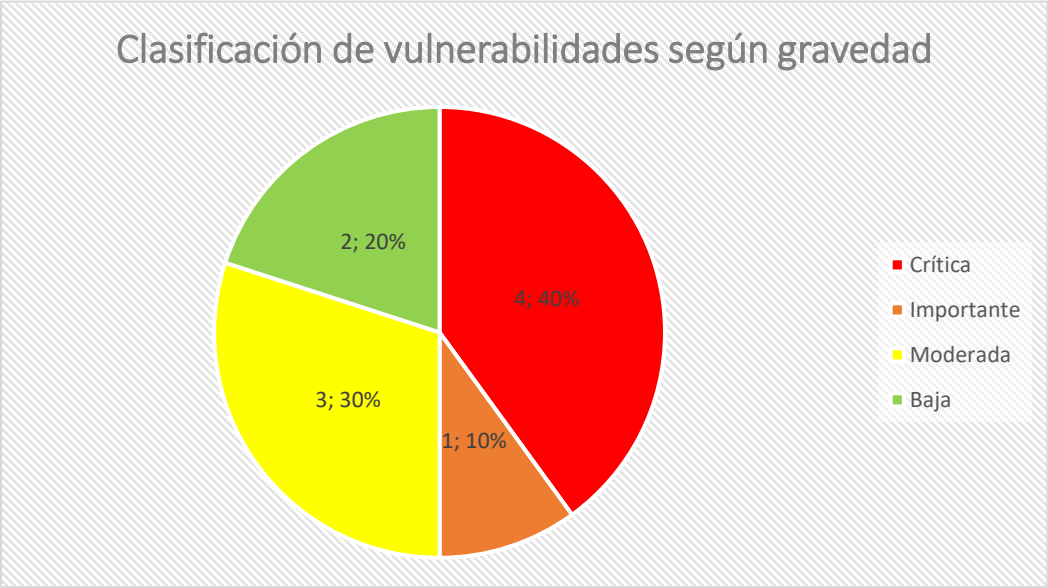


FIGURA N° 48: CLASIFICACIÓN DE VULNERABILIDADES SEGÚN GRAVEDAD.

Finalmente el resultado de la evaluación de riesgos en posibles escenarios luego de aplicado el control de seguridad es una reducción del 39.72% en el impacto general y una reducción mínima de 16.67% y máxima de 55.56% del impacto del aprovechamiento de una vulnerabilidad.

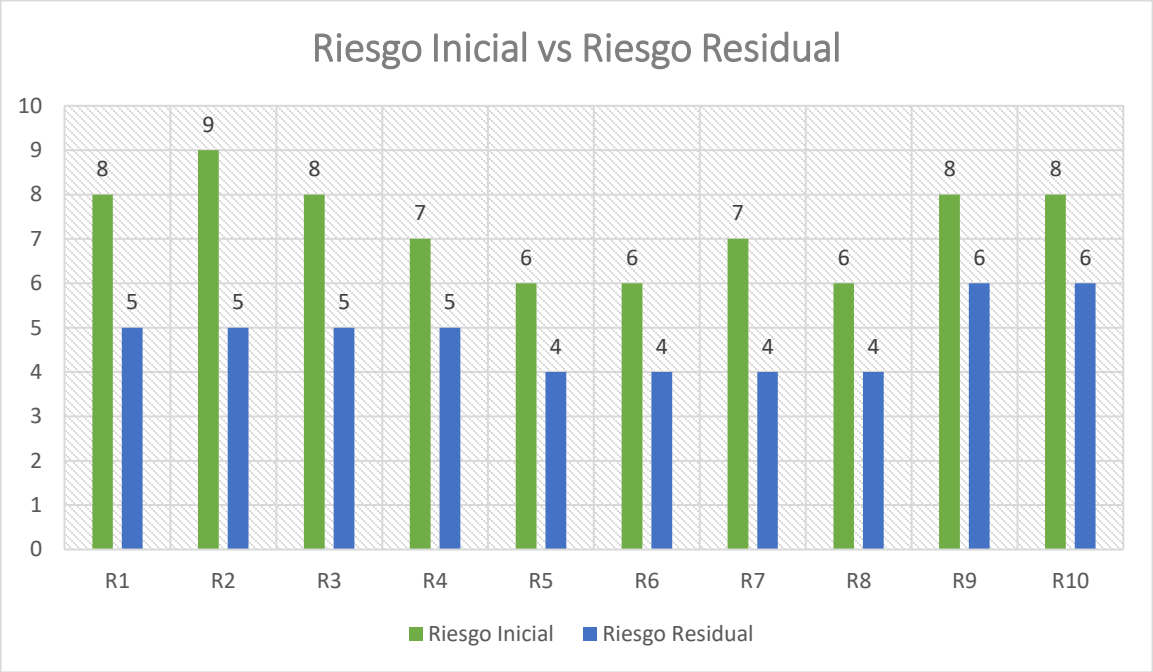


FIGURA N° 49: RIESGO INICIAL VS RIESGO RESIDUAL.

4.2 DISCUSIÓN

Se aplicó el Pentesting de forma legal y autorizada además de ser realizado con ética. Se facilitó el análisis de vulnerabilidades del sistema web de Gestión Administrativa de la empresa Devhuayra SAC Huancayo. Se realizó la evaluación inicial de la seguridad del sistema web mediante un checklist que muestra principalmente la falta de políticas de copias de seguridad, actualización de software y un plan de acción ante incidentes de seguridad.

Los resultados de la aplicación del Pentesting Durante la fase de Reconocimiento se identificaron 2 vulnerabilidades. La primera vulnerabilidad de tipo BAJA es el sitio permite la réplica de sus archivos, se descubrió utilizando la herramienta Httrack. Así mismo se identificó una vulnerabilidad de tipo CRÍTICO, El sitio no cuenta con un certificado SSL/TLS con Netcraft. En la fase Escaneo se identificaron 6 vulnerabilidades, la primera de tipo IMPORTANTE en el puerto 80 y 443 vulnerables a ataque DDOS, lo puertos 110, 142, 993 y 995 con vulnerabilidad Diffie-Hellman Key Exchange de tipo

CRÍTICO, vulnerabilidad CVE2012-2122 presente en MySql de tipo MODERADO y vulnerabilidad CVE-2012-020 presente en el protocolo RDF de tipo MODERADO se identificaron a través de Nmap Scripting y Vuln. Por otro lado utilizando Nikto se verificó que no se ha definido la protección contra Cross Site Scripting representado una vulnerabilidad de tipo MODERADO. Algunos directorios del sistema web se encuentran indexados por tanto son públicos y accesibles a todos los usuarios representando una vulnerabilidad de tipo BAJO. En la fase de explotación de identificaron 2 vulnerabilidades de tipo CRÍTICO. Una de ellas el formulario de inicio de sesión no está protegido contra inserción de código SQL y las contraseñas de la base de datos no están encriptadas.

Se obtuvo una matriz de riesgos inicial a partir del hallazgo de vulnerabilidades para luego valorar el impacto y probabilidad de ocurrencia. Nos permite conceptualizar gráficamente los riesgos y mostrarlos a la Alta Dirección y Gerencia a fin de concientizarlos y comprometerlos con el desarrollo de políticas y controles de seguridad que protegerán los activos de valor en su negocio. Se realizaron las recomendaciones adecuadas para cerrar las vulnerabilidades existentes en el sistema web. Las recomendaciones se brindaron tomando en consideración que el control no debe superar en costo y esfuerzo al activo que se protege. Los controles de seguridad deben ser monitoreados y mejorados constantemente. Se evidencia que la aplicación del Pentesting facilita el análisis de vulnerabilidades para su posterior tratamiento y reducción.

Las matrices de riesgo inicial y residual reflejan una reducción en el impacto ante un posible ciberataque hasta en un 55.56%. Lo cual evidencia la importancia de la implementación de los controles de seguridad apropiados.

Se identifica que no se toma la debida importancia a la seguridad de la información en la empresa, ya que muchas de las vulnerabilidades presenten evidencias falta de un programa de seguridad que actualice las versiones y parches de seguridad. La aplicación del Pentesting deja la base para establecer políticas y controles de seguridad.

Finalmente es importante destacar que las pruebas de Pentesting se realizaron de manera externa, es decir no se concedió ningún acceso o nombre de usuario y contraseña. Solo se

brindó el nombre de dominio a partir del cual se fue recopilando información y obteniendo hallazgos principales. La mayoría de vulnerabilidades hubieran sido difíciles de encontrar sin la utilización de herramientas de software orientadas a la seguridad informática.

CONCLUSIONES

Se aplicó el Pentesting en el análisis de vulnerabilidades web de Gestión Administrativa de la empresa Devhuayra SAC Huancayo. Se ejecutó las fases: Reconocimiento, Escaneo y Explotación de Vulnerabilidades, tomando como guía las metodologías OSSTMM, NIST SP-800-115 y OWASP Top Ten. Las metodologías proporcionaron la guía para la utilización de las herramientas de software y realizar el análisis adecuado de las vulnerabilidades.

La aplicación del Pentesting permitió clasificar las vulnerabilidades sistema web de Gestión Administrativa. Se identificaron 10 vulnerabilidades: las cuales comprometen el sistema web las cuales se clasificaron en una escala respecto a la gravedad: bajo, moderado, importante y crítico. Obteniendo un 40% de tipo CRÍTICO, 10% de tipo IMPORTANTE, 30% de nivel MODERADO y 20% de tipo BAJO.

La aplicación del Pentesting redujo las vulnerabilidades del sistema web de Gestión Administrativa. La evaluación de riesgos luego de aplicado el control de seguridad redujo un 39.72% en el impacto general y un máximo de 55.56% del impacto del aprovechamiento de una vulnerabilidad.

RECOMENDACIONES

Se recomienda que se utilicen herramientas o técnicas como el Pentesting para identificar vulnerabilidades, se debe tener presente que los ciberataques no cesarán al contrario se realizan de forma más constante y sofisticada. Tomar la seguridad de la información no solo como la protección o preservación de la información sino como una estrategia generadora de confianza para potenciar los negocios. Tomemos la seguridad como un proceso resiliente en constante aprendizaje de los errores.

Para identificar las vulnerabilidades también se recomienda utilizar otras herramientas como Nexus, Acunetix o Nexpose. La clasificación de vulnerabilidades se puede dar por tipo: error en la configuración, error causado por un humano, error en la validación de entrada de datos, entre otros. Otro criterio de clasificación es de acuerdo a su relación con las amenazas a las que se encuentra asociado.

Se recomienda utilizar frameworks de seguridad para una adecuada gestión de vulnerabilidades y riesgos. El Cybersecurity Framework de NIST abarca 5 funciones dentro del marco de los riesgos: identificar, proteger, detectar, responder y recuperar. Así mismo en la ISO 27001 Anexo A se encuentra una lista de controles de seguridad por activos de información los cuales se pueden tomar como referencia. Dicha ISO también cuenta con un apartado orientado a la Gestión de Riesgos.

REFERENCIAS BIBLIOGRÁFICAS

1. **Organización Estados Americanos y Banco Interamericano de Desarrollo.** https://publications.iadb.org. [En línea] 1 de Julio de 2020. [Citado el: 20 de Agosto de 2020.] https://publications.iadb.org/publications/spanish/document/Reporte-Ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-America-Latina-y-el-Caribe.pdf.

2. **ESET.** https://www.welivesecurity.com. [En línea] 2020. [Citado el: 10 de Septiembre de 2020.] https://www.welivesecurity.com/wp-content/uploads/2020/08/ESET-Security-Report-LATAM_2020.pdf.

3. —. https://www.welivesecurity.com. [En línea] 8 de Marzo de 2018. [Citado el: 15 de Agosto de 2020.] https://www.welivesecurity.com/la-es/2018/03/08/ataques-ddos-mas-grandes-historia-registraron-solo-cuatro-dias/.

4. **Eleven Paths.** https://www.elevenpaths.com. [En línea] 2020. [Citado el: 14 de Octubre de 2020.] https://pro-cdo-web-resources.s3.eu-west-1.amazonaws.com/elevenpaths/uploads/2021/1/20210118-cybersecurityreport-20h2-es.pdf.

5. **Talón, Rafael Manuel Martí.** *Desarrollo e Implementación de una práctica de Pentest.* Gandia : Universidad Politécnica de Valencia, 2016.

6. **Phong, Chiem Trieu.** *A study of Penetration Testing Tools and Approaches.* Auckland : School of Computing and Mathematical Sciences, 2014.

7. **Castro, Carlos.** *Pruebas de Penetración e Intrusión.* Bogotá : Universidad Piloto de Colombia, 2018.

8. **Saavedra, Walter Gonzalo Cruz.** *Aplicación de Auditoría Penetration Testing para contribuir con la seguridad de la información en los sistemas informáticos de la empresa Data Business SAC, Trujillo.* Trujillo : Universidad Privada del Norte, 2014.

9. **Wendy Bernal, Norhelia Echevarria.** *Modelo de Niveles de Seguridad para Pruebas de Intrusión en Aplicaciones Web para PYMES en el Perú.* Lima : Universidad Peruana de Ciencias Aplicadas (UPC), 2019.

10. **Breiner, Gonzales Cotera.** *Uso de herramientas de Ethical Hacking con Kali Linux para el diagnóstico de vulnerabilidades de la seguridad de la información de la red de la Sede Central de la Univesidad de Huánuco.* Huánuco : Universidad de Huánuco, 2016.

11. **Kenedy, Riveros Paraguay Jhon.** *Implementación de Políticas de Seguridad Informática para mejorar el acceso y la seguridad lógica de la red en la Oficina Departamental de Estadística e Informática de Junín.* Huancayo : Universidad Nacional del Centro del Perú, 2019.

12. **Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica.** *MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.* Madrid : Ministerio de Hacienda y Administraciones Públicas, 2012.

13. **Cardwell, Kevin.** *Construyendo un Laboratorio Virtual de Pentesting para Pruebas Avanzadas de Pentración Tercera Edición.* Birmingham : Packt Publishing Ltd, 2019.

14. **Danilo, Nuela Guananga Byron.** *Auditoría de la Seguridad Informática para el Honorable Gobierno Provincial de Tungurahua mediante la metodología Open Source Security Testing Methodology Manual.* Ambato : Universidad Técnica de Ambato, 2015.

15. **Leonardo, Meza Castillo Andrés.** *Diseño de un Marco de Referencia para el análisis de vulnerabilidaes a un segmento de la red corporativa de una empresa de telecomunicaciones en Quito basado en las principales metodologías de pruebas de seguridad informática.* Quito : Universidad Internacional SEK, 2019.

16. **Zafra, Jose Luis Guillén.** *Introducción al Pentesting.* Barcelona : Universitat de Barcelona, 2017.

17. **Castro, Martha Irene Romero.** *Introducción a la Seguridad Informática y el Análisis de Vulnerabilidades.* Alicante : Editorial Área de Innovación y Desarrollo,S.L., 2018.

18. **Alonso, Jaime.** *El sitio web como unidad básica de información y comunicación.* Murcia : Universidad de Murcia, 2008.

19. **Vyacheslav Fadyushin, Andrey Popo.** *Construyendo un Laboratorio de Pentesting para Redes Inalámbricas.* Birmingham : Packt Publishing Ltd, 2016.

ANEXOS

Anexo 01. Acuerdo de Aplicación de Pentesting

ACUERDO DE APLICACIÓN DE PENTESTING

Reunidos de una parte Héctor Arturo Vivanco Nuñez con domicilio en Psje. Miculicich 141 El Tambo - Huancayo, identificado con DNI 70019168 y en representación de la empresa Devhuayra SAC con dirección fiscal en Calle Real N° 945 Int 0001 y RUC 20602257020 y de otra parte Margaret Lesly Palacios Gallardo identificado con DNI 72706266 con domicilio en la calle Santa Isabel 127 San Carlos, Huancayo. Exponen:

1. Autorización

   La empresa Devhuayra SAC autoriza la aplicación del Pentesting al Sistema Web de Gestión Administrativa, el cual conlleva la evaluación de vulnerabilidades y penetración al sistema.

2. Confidencialidad

   Ambas partes mantendrán la confidencialidad de la información que se obtenga de cada una de las fases del Pentesting. Toda la información obtenida será tratada como confidencial. Ambas partes se comprometen a usar la información de manera reservada, no divulgarla, ni comunicarla, se impide la copia o revelación a terceros. No se debe utilizar la información para fines ajenos al presente acuerdo. Toda información es propiedad exclusiva de donde proceda.

3. Duración

   Este acuerdo tendrá una duración de 2 meses. Dando como fecha de inicio del 30 de septiembre de 2020 y finalizando el 30 de noviembre. En caso de no renovarse el contrato ambas partes deberán devolver toda la información obtenida entre sí, independientemente del soporte o formato en el que se encuentren.

4. Alcance de las Pruebas

   El pentester establecerá las herramientas necesarias para la aplicación de las pruebas de vulnerabilidad dentro de las cuales se contempla la aplicación sobre el sistema web de Gestión Administrativa.

   Todas las pruebas se realizan de manera externa. No se brinda información del sistema web, base de datos, IPs u otros.

   Sobre las pruebas permitidas:

   a) Fase de Escaneo

      - Revisión de puertos TCP

- Revisión de puertos UDP disponibles.
- Usuarios y contraseñas del sistema web
- Revelación de información a través de protocolos inseguros.

b) Identificación de Servicios

- Verificación del servicio existente en cada puerto
- Realizar chequeo de Banners para identificar versiones o actualizaciones instaladas del servicio.
- Extracción de nombres de usuarios u otros datos de la base de datos.

c) Identificación de vulnerabilidades

- Utilización de escáneres de vulnerabilidad para determinar las vulnerabilidades existentes.
- Identificación de vulnerabilidades de los servicios web y puertos.

d) Explotación de vulnerabilidades

- Aprovechamiento de la vulnerabilidad para obtener acceso al sistema.
- Explotación solo de las vulnerabilidad relacionadas al Sistema Web.

e) Post Explotación

- En caso de activar una puerta trasera para mantener el acceso, se deberá informar y posteriormente eliminar.

En prueba de la conformidad de cuanto antecede, firman el presente acuerdo por duplicado ambas partes.

Huancayo, 21 de septiembre de 2020

Representante Devhuayra SAC
Héctor Arturo Vivanco Nuñez
70019168

Pentester
Margaret Lesly Palacios Gallardo
72706266

Anexo 02. Resultados del Checklist

Checklist – Evaluación Nivel de Seguridad Inicial

Evaluador: Margaret Lesly Palacios Gallardo

Empresa: Devhuayra SAC Huancayo

DATOS				
N°	**Descripción**	**SI**	**NO**	**Observaciones**
1	¿Se realizan copias de seguridad a la base de datos?		X	No se han realizado copias de seguridad desde la implementación.
2	¿Se realizan las actualizaciones correspondientes a los gestores de base de datos u otro software que soporten las BD?		X	Tampoco se realizaron actualizaciones desde la implementación.
APLICACIONES				
N°	**Descripción**	**SI**	**NO**	**Observaciones**
3	¿Las aplicaciones de desarrollo in house son desarrolladas bajo estándares de seguridad?		X	No se utilizan estándares de desarrollo seguro, por ejemplo Open Web Application Security Proyect (OWASP)
4	¿Se realiza el mantenimiento a las aplicaciones?	X		Se realizan el mantenimiento correctivo al sistema.
POLÍTICAS				
N°	**Descripción**	**SI**	**NO**	**Observaciones**
5	¿Cuenta con políticas de seguridad actualizadas y difundidas a toda la empresa?		X	No se cuenta con ninguna política de seguridad relacionada al sistema web.
INCIDENTES DE SEGURIDAD				
N°	**Descripción**	**SI**	**NO**	**Observaciones**
6	¿Cuenta con un plan de acción ante los incidentes de seguridad?		X	No se cuenta con un plan de acción ante incidentes de seguridad.
7	¿Cuenta con medidas de acción ante vulnerabilidades encontradas en la infraestructura o sistemas?		X	Las medidas ante fallos se toman en el momento que suceden.