# ÍNDICE



---

# 1. Introducción

Este informe documenta los hallazgos del pentesting realizado en la dirección IP 10.0.2.15. El objetivo de esta evaluación fue identificar vulnerabilidades de seguridad en el sistema y la aplicación web asociada, evaluar los riesgos potenciales y proporcionar recomendaciones para fortalecer la seguridad.

El alcance del pentesting incluyó un servidor con servicios críticos en ejecución y una aplicación web. Se analizaron configuraciones, accesos y posibles vectores de ataque tanto en la infraestructura de red como en la aplicación.

# 2. Enfoque y Estrategia

## 2.1 Enfoque para la Máquina

El análisis de la máquina se enfocó en identificar servicios expuestos, vulnerabilidades de configuración y posibles debilidades en los accesos. Se utilizaron herramientas como:

- **Nmap** para escaneo de puertos y detección de servicios.
- **Metasploit** para pruebas de explotación en servicios identificados.
- **Hydra** para ataques de fuerza bruta en credenciales.

## 2.2 Enfoque para el Sitio Web

Para la aplicación web, el análisis incluyó pruebas de inyección de código, configuraciones incorrectas y accesos no autorizados. Se usaron herramientas como:

- **Burp Suite** para analizar peticiones y respuestas HTTP.
- **OWASP ZAP** para escaneo automático de vulnerabilidades web.
- **SQLmap** para detectar inyecciones SQL.
- **Dirb** para descubrimiento de directorios sensibles.

# 3. Fases del Pentesting

## 3.1 Reconocimiento

Se recopiló información sobre la infraestructura mediante:

- WHOIS y Shodan para obtener datos de la dirección IP y servicios expuestos.
- Enumeración de subdominios y rutas críticas.

## 3.2 Escaneo y Enumeración

Se realizó un escaneo de puertos con Nmap:

```
nmap -sS -A 10.0.2.15
```

Se identificaron los siguientes servicios:

- **SSH (22/tcp)** - Posibles credenciales débiles.
- **HTTP (80/tcp)** - Aplicación web con posibles vulnerabilidades.
- **HTTPS (443/tcp)** - Sin configuración adecuada de certificados.

Se realizó un escaneo de directorios web con Dirb:

```
dirb http://10.0.2.15/
```

Se encontraron rutas sensibles como `/admin` y `/backup`.

## 3.3 Explotación

Se intentó explotar las vulnerabilidades encontradas:

- Uso de **Hydra** para ataque de fuerza bruta en SSH.
- Ejecución de **SQLmap** para detectar y explotar inyecciones SQL.
- Pruebas manuales de **XSS reflejado y almacenado** en formularios web.

## 3.4 Post-explotación

- Acceso a archivos sensibles en el servidor.
- Enumeración de usuarios y configuraciones críticas.
- Extracción de hashes de contraseñas para posterior crackeo.

# 4. Vulnerabilidades Detectadas

- **Servicio SSH con credenciales por defecto** (acceso no autorizado).
- **Inyección SQL en formularios web** (posible extracción de datos sensibles).
- **XSS reflejado y almacenado** (riesgo de robo de sesiones).
- **Directorios accesibles sin autenticación** (`/admin` y `/backup`).

# 5. Propuesta de Prevención

Para reducir el riesgo de vulnerabilidades futuras se recomienda:

- **Uso de contraseñas seguras** y autenticación multifactor en SSH.
- **Validación de entradas en la aplicación web** para prevenir inyecciones SQL y XSS.
- **Configuración adecuada de permisos en archivos y directorios sensibles**.
- **Monitoreo y auditoría regular de logs y accesos**.

# 6. Propuesta de Mitigación

- **Configurar SSH** para solo aceptar llaves públicas.
- **Implementar WAF** para mitigar ataques web.
- **Usar consultas parametrizadas en bases de datos**.
- **Aplicar CSP (Content Security Policy)** para prevenir XSS.
- **Restringir acceso a directorios sensibles** mediante configuración de servidor.

# 7. Análisis de Mitigación

Se realizaron pruebas posteriores para verificar la efectividad de las soluciones implementadas. Se observó que:

- Los intentos de acceso por SSH con credenciales débiles fueron bloqueados.
- La inyección SQL fue mitigada con consultas parametrizadas.
- El XSS fue prevenido con validación adecuada y CSP.
- Los directorios sensibles ya no eran accesibles sin autenticación.

# 8. Impacto Potencial

La implementación de estas medidas reducirá la exposición a ataques, mejorando la seguridad general del sistema. Se incrementará la protección contra accesos no autorizados y se minimizará el riesgo de filtración de datos.

# 9. Conclusión

La seguridad debe ser un proceso continuo. Se recomienda:

- **Realizar auditorías periódicas** para detectar nuevas vulnerabilidades.
- **Capacitar al personal** en mejores prácticas de seguridad.
- **Actualizar software y sistemas** de manera regular.