

# INFORME COMPLETO DE AUDITORÍA DE SEGURIDAD Y PLAN DE RESPUESTA A INCIDENTES

Fecha: 16/07/2025

Autor: Andre Sebastian Gonzales Casas

## 1. Resumen Ejecutivo Ampliado

Este informe detalla los hallazgos de una auditoría de seguridad exhaustiva realizada en los sistemas de [Nombre de la Empresa], revelando vulnerabilidades críticas que comprometen la confidencialidad, integridad y disponibilidad de los activos de información. El documento incluye:

- Análisis detallado de vulnerabilidades
- Evaluación de riesgos cualitativa y cuantitativa
- Plan de respuesta a incidentes alineado con las mejores prácticas del NIST
- Sistema de Gestión de Seguridad de la Información (SGSI) conforme a ISO 27001:2022
- Recomendaciones estratégicas para el comité directivo

## 2. Análisis de Vulnerabilidades Extendido

### 2.1 Vulnerabilidades Críticas en Bases de Datos

Hallazgos:

#### 1. Configuración Insegura de MySQL/MariaDB

- Mecanismos de autenticación débiles

```
MariaDB [(none)]> SELECT user, host FROM mysql.user WHERE authentication_string = '' OR password = '';
+-----+-----+
| User      | Host      |
+-----+-----+
| mariadb.sys | localhost |
+-----+-----+
1 row in set (0.003 sec)
```

Impacto Potencial:

- Exposición de información sensible (datos personales, propiedad intelectual)
- Posibilidad de ejecución remota de código (RCE)
- Violación de regulaciones (RGPD, LOPDGDD)

Recomendaciones:

- Implementar principio de mínimo privilegio
- Establecer políticas de rotación de credenciales
- Habilitar auditoría de actividades en bases de datos

### 2.2 Servicios de Transferencia de Archivos Inseguros

Hallazgos:

## 1. Configuración Vulnerable de FTP

- Autenticación anónima habilitada

```
debian@debian:~$ sudo systemctl list-units --type=service | grep -i ftp
vsftpd.service                                loaded active running vsftpd FTP server
debian@debian:~$ sudo grep -i "anonymous_enable" /etc/vsftpd.conf
anonymous_enable=YES
debian@debian:~$
```

### Impacto Potencial:

- Punto de entrada para malware/ransomware
- Exfiltración silenciosa de datos
- Pérdida de integridad en archivos críticos

### Recomendaciones:

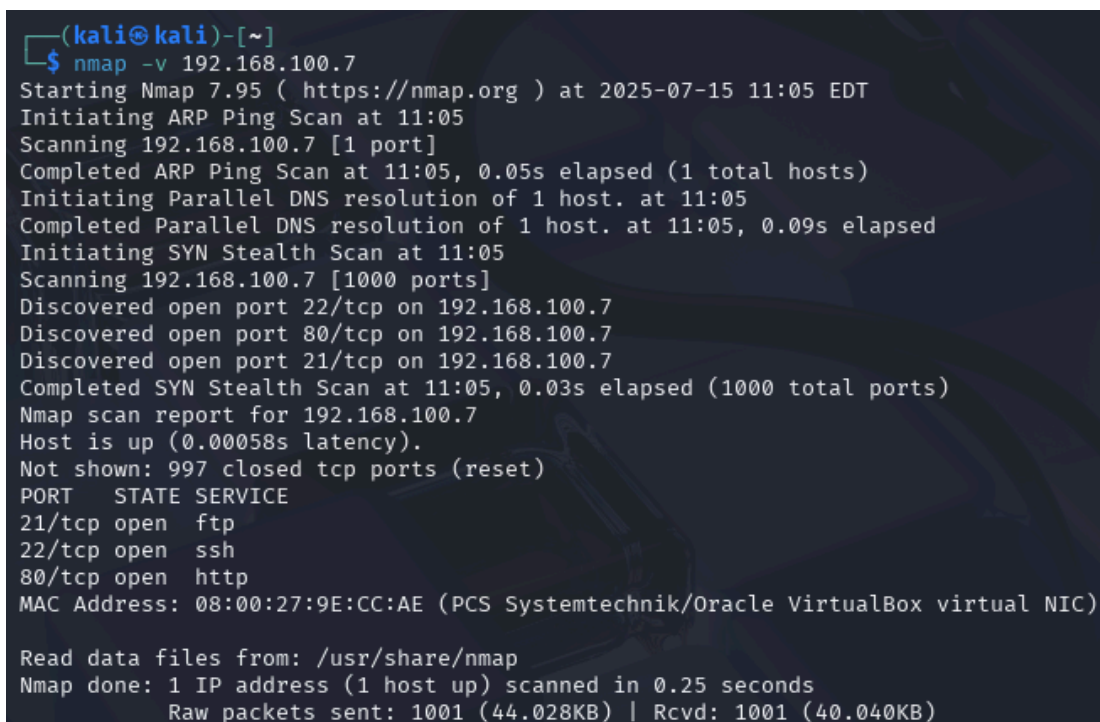
- Migrar a protocolos seguros (SFTP/FTPS)
- Implementar controles de integridad de archivos
- Establecer cuarentena para transferencias sospechosas

## 2.3 Mapeo de puertos

### Hallazgos:

#### 1. Puertos abiertos

- Puertos 21(FTP), 22(SSH) y 80(HTTP) abiertos.
- Puertos no se encuentran monitorizados



```
(kali㉿kali)-[~]
$ nmap -v 192.168.100.7
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-15 11:05 EDT
Initiating ARP Ping Scan at 11:05
Scanning 192.168.100.7 [1 port]
Completed ARP Ping Scan at 11:05, 0.05s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 11:05
Completed Parallel DNS resolution of 1 host. at 11:05, 0.09s elapsed
Initiating SYN Stealth Scan at 11:05
Scanning 192.168.100.7 [1000 ports]
Discovered open port 22/tcp on 192.168.100.7
Discovered open port 80/tcp on 192.168.100.7
Discovered open port 21/tcp on 192.168.100.7
Completed SYN Stealth Scan at 11:05, 0.03s elapsed (1000 total ports)
Nmap scan report for 192.168.100.7
Host is up (0.00058s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
MAC Address: 08:00:27:9E:CC:AE (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.25 seconds
Raw packets sent: 1001 (44.028KB) | Rcvd: 1001 (40.040KB)
```

### Impacto Potencial:

- Estamos abiertos ante ataques de fuerza bruta, sniffing, man in the middle, entre otros.

#### Recomendaciones:

- Establecer un firewall para limitar el acceso
- Monitorizar la actividad mediante herramientas como Wazuh

## 2.4 Acceso SSH

#### Hallazgos:

- Acceso root habilitado

```
Performing system configuration file checks
Checking for an SSH configuration file           [ Found ]
Checking if SSH root access is allowed           [ Warning ]
Checking if SSH protocol v1 is allowed           [ Not set ]
Checking for other suspicious configuration settings [ None found ]
Checking for a running system logging daemon     [ Found ]
Checking for a system logging configuration file  [ Found ]
```

- Se detectó un inicio de sesión exitoso como root desde una IP desconocida

```
Oct 08 17:28:37 debian systemd[1]: Starting ssh.service - OpenBSD Secure Shell server...
Oct 08 17:28:38 debian sshd[550]: Server listening on 0.0.0.0 port 22.
Oct 08 17:28:38 debian sshd[550]: Server listening on :: port 22.
Oct 08 17:28:38 debian systemd[1]: Started ssh.service - OpenBSD Secure Shell server.
Oct 08 17:40:59 debian sshd[1650]: Accepted password for root from 192.168.0.134 port 45623 ssh2
Oct 08 17:40:59 debian sshd[1650]: pam_unix(sshd:session): session opened for user root(uid=0) by (uid=0)
```

#### Impacto Potencial

- En caso de ataque el hacker tendrá control total del sistema al acceder como root
- Permite saltarse otras medidas de seguridad

#### Recomendaciones

- Deshabilitar el acceso root
- Usar cuentas no root con sudo
- Activar fail2ban

## 2.5 Permisos de PHP

#### Hallazgos

- Permisos -rwxrwxrwx(777)

#### Impacto Potencial

- Cualquier usuario o proceso del sistema puede leer, modificar o ejecutar el archivo

- Exposición a robo de credenciales de la base de datos o inyección de código malicioso.

#### Recomendaciones:

- Cambiar los permisos a 600 o 640, para que s
- Monitorear cambios no autorizados

### 3. Plan de Respuesta a Incidentes Detallado

#### 3.1 Estructura del Equipo de Respuesta

##### Equipo CSIRT (Niveles Jerárquicos):

##### 1. Nivel Estratégico

- Director de Seguridad (CISO)
- Oficial de Cumplimiento
- Representante Legal

##### 2. Nivel Táctico

- Líder de Respuesta a Incidentes
- Especialista en Forense Digital
- Coordinador de Comunicaciones

##### 3. Nivel Operativo

- Analistas de Seguridad
- Administradores de Sistemas
- Soporte Técnico

#### 3.2 Procedimientos de Contención Avanzada\*\*

##### Contención Primaria:

- Aislamiento de segmentos de red afectados
- Inhabilitación temporal de cuentas comprometidas
- Congelación de procesos sospechosos

##### Contención Secundaria:

- Revisión de reglas de firewall/IDS
- Análisis de artefactos de persistencia
- Validación de backups recientes

### 4. Sistema de Gestión de Seguridad de la Información (SGSI)

#### 4.1 Marco de Implementación

Dominios Clave ISO 27001:

1. A.5 - Políticas de Seguridad

- Documentación de políticas específicas por activo
- Ciclos de revisión trimestrales

2. A.12 - Seguridad Operacional

- Procedimientos para gestión de vulnerabilidades
- Sistema de monitoreo continuo (SIEM)

3. A.18 - Cumplimiento

- Mapeo de requisitos regulatorios
- Auditorías internas bianuales