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

Fecha: 16/07/2025
Autor: Andre Sebastian Gonzales Casas

1. RESUMEN EJECUTIVO

Este informe detalla los hallazgos de una auditoría de seguridad exhaustiva realizada en los sistemas de 4Geeks, 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. ANÀLISIS DE VULNERABILIDADES

2.1 Vulnerabilidades Críticas en Bases de Datos

Hallazgos:
1. Configuración Insegura de MySQL/MariaDB

- Mecanismos de autenticación débiles

```
MariaDB [(none)]> SHOW GRANTS FOR 'user'@'localhost';
+-------------------------------------------------------------------------------------------------------------------
-----------------------------+
| Grants for user@localhost
                            |
+-------------------------------------------------------------------------------------------------------------------
-----------------------------+
| GRANT ALL PRIVILEGES ON *.* TO `user`@`localhost` IDENTIFIED BY PASSWORD '*2470C0C06DEE42FD1618BB99005ADCA
2EC9D1E19' WITH GRANT OPTION |
+-----------------------------+-------------------------------------------------------------------------------------
-----------------------------+
1 row in set (0.001 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

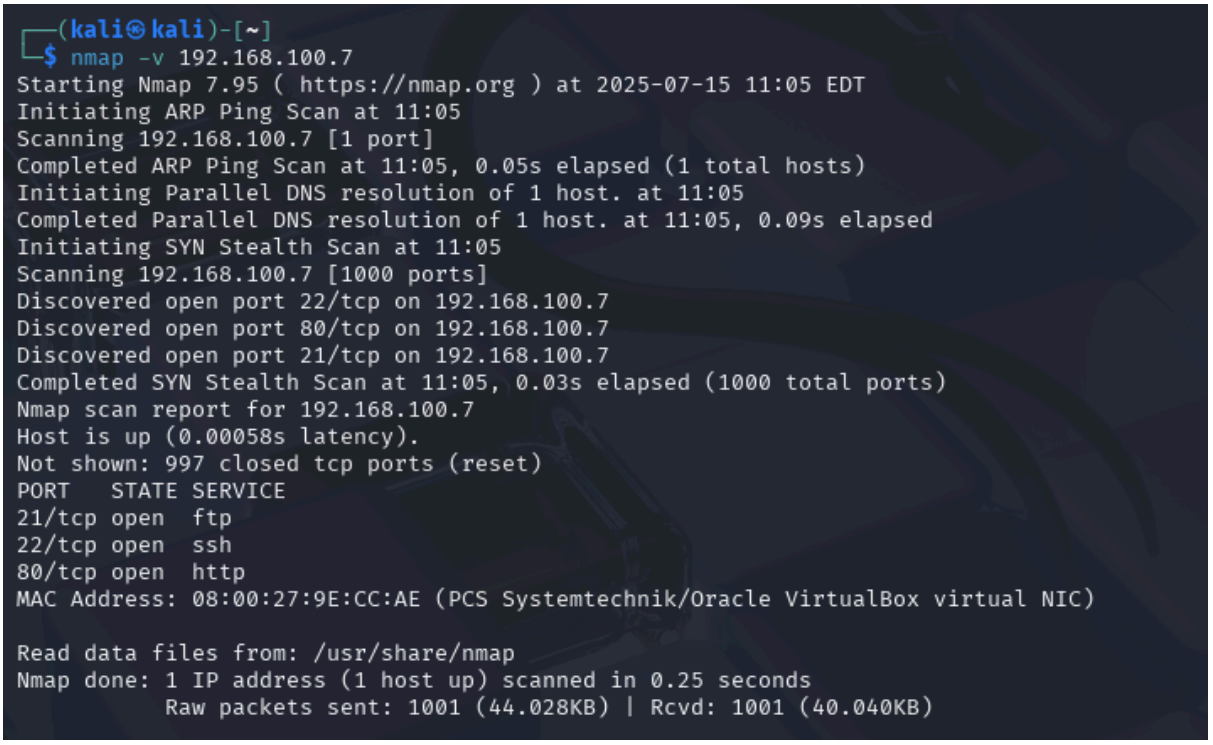
2.3 Mapeo de puertos

Hallazgos:

1.Puertos abiertos

-Puertos 21(FTP), 22(SSH) y 80(HTTP) abiertos.

-Puertos no se encuentran monitorizados



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 detecto un inicio de sesion 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)`

```
debian@debian:/var/www/html$ ls -l wp-config.php
-rwxrwxrwx 1 www-data www-data 3017 Sep 30  2024 wp-config.php
```

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 (PRI) MEJORADO

3.1 Estructura Organizacional del Equipo de Respuesta

Explicación:
Un equipo de respuesta efectivo requiere una estructura escalonada con roles y responsabilidades claramente definidos. La estructura propuesta sigue el modelo NIST SP 800-61 y se compone de tres niveles de actuación:
Nivel Estratégico (Toma de decisiones):

- Director de Seguridad (CISO): Autoriza acciones críticas y asigna recursos
- Representante Legal: Gestiona implicaciones regulatorias y comunicaciones externas
- Director de Operaciones: Decide sobre continuidad del negocio

Nivel Táctico (Coordinación):

- Líder de Respuesta: Coordina equipos técnicos y prioriza acciones
- Especialista Forense: Preserva evidencias para investigación legal
- Coordinador Comunicaciones: Gestiona mensajes a stakeholders internos/externos

Nivel Operativo (Ejecución):

- Analistas SOC: Monitorean y contienen amenazas en tiempo real
- Administradores Sistemas: Implementan medidas técnicas
- Soporte Usuarios: Asiste a personal afectado

3.2 Procedimientos de Contención Avanzada

Explicación:
La contención debe ser progresiva para balancear impacto operacional con efectividad:
Contención Primaria (Inmediata - Primeras 24h):

- Aislamiento de Red: Segmentación VLAN/ACLs para contener propagación
- Desactivación Credenciales: Revocación inmediata de certificados/API keys
- Captura de Memoria: Preservación de procesos activos para análisis forense

Contención Secundaria (Controlada - 24-72h):

- Análisis de Persistencia: Búsqueda de backdoors en cronjobs, servicios, registros
- Honeypots: Implementación de sistemas señuelo para monitorizar actividad maliciosa
- Restauración Selectiva: Puesta en marcha de sistemas críticos desde backups limpios

4. SISTEMA DE GESTIÓN DE SEGURIDAD (SGSI)

4.1 Marco de Implementación Detallado

Explicación:
El SGSI se basa en el ciclo PDCA (Plan-Do-Check-Act) adaptado a ISO 27001:2022:
Fase de Planificación:

- Análisis de Contexto: Identificación de stakeholders y requisitos legales
- Evaluación de Riesgos: Metodología OCTAVE para valorar activos críticos
- Declaración de Aplicabilidad: Selección de 35 controles prioritarios

Fase de Implementación:

- Roadmap Tecnológico:
    - Corto plazo (0-3 meses): Parcheo vulnerabilidades críticas
    - Medio plazo (3-6 meses): Implementación SIEM/PAM
    - Largo plazo (6-12 meses): Certificación ISO 27001

Fase de Verificación:

- Auditorías Internas: Cuatrimestrales con checklist basado en CIS Controls
- Pentesting Anual: Pruebas realizadas por terceros certificados

4.2 Controles Clave Explicados

A.12.6.1 - Gestión de Vulnerabilidades Técnicas

- Procedimiento: Escaneo semanal con Nessus + parcheo crítico en 72h
- Responsable: Equipo de Operaciones de Seguridad
- Métricas: % vulnerabilidades remediadas por severidad

A.9.4.2 - Restricción de Accesos Privilegiados

- Procedimiento: Implementación PAM (Privileged Access Management)
- Flujo: Solicitud → Aprobación → Provisión temporal → Revocación
- Herramientas: CyberArk para gestión de credenciales privilegiadas

4.3 Modelo de Gobernanza

Explicación:
Estructura de tres líneas de defensa para garantizar efectividad:
Primera Línea (Operativa):

- Dueños de procesos implementando controles diarios
- Ejemplo: Equipo TI aplicando parches de seguridad

Segunda Línea (Supervisión):

- Comité de Seguridad revisando cumplimiento
- Auditorías internas trimestrales

Tercera Línea (Verificación):

- Auditoría externa independiente
- Revisión anual por parte del Comité de Riesgos

5. RECOMENDACIONES ESTRATÉGICAS

5.1 Hoja de Ruta Priorizada

Inmediatas (0-30 días):

1. Parcheo de vulnerabilidades críticas (CVSS ≥ 9.0)
2. Implementación de MFA en todos los accesos externos
3. Revisión y ajuste de políticas de backup

Tácticas (1-3 meses):

1. Diseño de arquitectura Zero Trust
2. Programa de concienciación para empleados
3. Implementación de solución SIEM

Estratégicas (3-6 meses):

1. Certificación ISO 27001
2. Seguro de ciberriesgos
3. Plan de continuidad de negocio certificado