INFORME TÉCNICO DE SEGURIDAD DE LA INFORMACIÓN – FASE 1: RECONOCIMIENTO Y RECOLECCIÓN DE EVIDENCIAS

Proyecto Final de Ciberseguridad

Elaborado por: Santiago Rivero

Fecha: Enero 2026

---

1. INTRODUCCIÓN

El presente informe documenta de manera formal, técnica y estructurada la Fase 1: Reconocimiento y Recolección de Evidencias del proyecto final del bootcamp de ciberseguridad. Esta fase tuvo como finalidad principal realizar un análisis forense inicial, identificar el vector de ataque utilizado por un atacante, contener el incidente de seguridad detectado, revertir los cambios maliciosos y aplicar medidas correctivas y preventivas que eviten tanto la escalación de privilegios como la recurrencia de incidentes similares.

El análisis se llevó a cabo sobre un servidor Linux en un entorno controlado de laboratorio, permitiendo aplicar técnicas reales de respuesta a incidentes sin afectar sistemas productivos. Durante el proceso se emplearon herramientas estándar de administración y seguridad, siguiendo buenas prácticas ampliamente aceptadas en el ámbito profesional.

Este informe se elabora alineado a principios y controles de la norma ISO/IEC 27001, especialmente en lo referente a:

- Gestión de incidentes de seguridad de la información
- Control de accesos y gestión de identidades
- Seguridad en las operaciones del sistema
- Hardening de servicios expuestos
- Reducción de superficie de ataque

2. OBJETIVO DE LA FASE 1

Los objetivos específicos de esta fase fueron los siguientes:

- Identificar los servicios comprometidos y el método de acceso inicial utilizado por el atacante.
- Analizar evidencias forenses mediante logs del sistema usando journalctl, dado que `/var/log/auth.log` no está disponible.

- Detectar usuarios, procesos, archivos y configuraciones sospechosas o inusuales.
- Realizar un escaneo del sistema para identificar posibles rootkits o malware.
- Contener el incidente y bloquear el exploit utilizado.
- Revertir cambios realizados por el atacante y eliminar posibles mecanismos de persistencia.
- Aplicar medidas de hardenización y corrección conforme a buenas prácticas de seguridad.

3. ALCANCE

- Sistema analizado: Servidor Linux (entorno de laboratorio Debian-based)
- Servicios evaluados:
    - SSH
    - MySQL / MariaDB
    - FTP (vsftpd)
    - Firewall (UFW)
- Limitaciones del análisis:
    - No se ejecutaron ataques de denegación de servicio (DoS).
    - El análisis se realizó únicamente a nivel de sistema y servicios, sin pruebas de explotación avanzadas.
    - No se analizaron aplicaciones de terceros más allá de WordPress a nivel de permisos.

4. METODOLOGÍA APLICADA

La Fase 1 se desarrolló siguiendo una metodología básica de Respuesta a

Incidentes de Seguridad, compuesta por las siguientes etapas:

1. Identificación: Detección del acceso no autorizado y servicios afectados.
2. Análisis: Revisión de logs, procesos, usuarios y configuraciones.
3. Contención: Detención de servicios comprometidos y bloqueo del vector de ataque.
4. Erradicación: Eliminación de configuraciones inseguras y usuarios no autorizados.
5. Recuperación: Restauración segura del sistema.
6. Lecciones aprendidas: Identificación de mejoras preventivas.

5. IDENTIFICACIÓN DEL ACCESO NO AUTORIZADO

5.1 Análisis de accesos SSH

Dado que el archivo `/var/log/auth.log` no existe en el sistema analizado, se utilizó `journalctl` para revisar los eventos relacionados con autenticación SSH.

```bash
sudo journalctl -u ssh | grep "Accepted"
```

Resultado obtenido:

```text
Accepted password for root from 192.168.0.134 port 45623 ssh2
```

Análisis detallado:

- Se identificó un acceso SSH exitoso.
- El usuario utilizado fue root, lo que indica privilegios máximos.
- El método de autenticación fue password, considerado inseguro.
- La conexión se originó desde la IP 192.168.0.134.

Conclusión: El acceso inicial del atacante se realizó mediante credenciales válidas del usuario root, evidenciando una mala configuración de seguridad en el servicio SSH.

5.2 Análisis de creación de usuarios

Se revisaron eventos relacionados con la creación de usuarios para detectar posibles mecanismos de persistencia.

```bash
sudo journalctl | grep useradd
```

Resultado obtenido:

```text
useradd: new user: name=mysql
useradd: new user: name=sshd
useradd: new user: name=ftp
useradd: new user: name=Debian-exim
```

Análisis:

- Los usuarios detectados corresponden a cuentas de sistema legítimas.
- Utilizan shells no interactivos.
- No se detectaron usuarios creados después del incidente.

6. SERVICIOS COMPROMETIDOS IDENTIFICADOS

6.1 MySQL / MariaDB

Vulnerabilidades identificadas:

- Existencia de usuarios de base de datos con credenciales débiles.
- Uso de contraseñas simples para cuentas locales.
- Riesgo de acceso no autorizado a información sensible almacenada en la base de datos de WordPress.

Enumeración de usuarios existentes en MySQL / MariaDB:

```sql
SELECT user, host, authentication_string FROM mysql.user;
```

Resultado obtenido:

```text
+----------------+-----------+-------------------------------------------+
| User           | Host      | authentication_string                     |
+----------------+-----------+-------------------------------------------+
| mariadb.sys    | localhost |                                           |
| root           | localhost | *6BB4837EB74329105EE4568DDA7DC67ED2CA2AD9 |
| mysql          | localhost | invalid                                   |
| wordpressuser  | localhost | *6BB4837EB74329105EE4568DDA7DC67ED2CA2AD9 |
| user           | localhost | *2470C0C06DEE42FD1618BB99005ADCAZEC9D1E19 |
+----------------+-----------+-------------------------------------------+
```

Análisis:

- Se identificó el usuario `'user'@'localhost'` como una cuenta no estándar.
- Este usuario utilizaba una contraseña débil, evidenciada por su rápida explotación durante las pruebas.
- La cuenta no era requerida para el funcionamiento de WordPress ni del sistema.

Acción correctiva – eliminación de usuarios inseguros:

```sql
DROP USER 'user'@'localhost';

FLUSH PRIVILEGES;
```

Resultado:

- Eliminación exitosa de los usuarios inseguros.
- Reducción del riesgo de acceso no autorizado a la base de datos.

Refuerzo de credenciales del usuario administrativo y de WordPress:

```sql
ALTER USER 'root'@'localhost' IDENTIFIED BY 'ContraseñaMuySegura!2026';
ALTER USER 'wordpressuser'@'localhost' IDENTIFIED BY 'ContraseñaMuySegura!2026';

FLUSH PRIVILEGES;
```

Resultado final:

- Permanecen únicamente usuarios necesarios.
- Contraseñas fuertes aplicadas.
- Acceso restringido exclusivamente a localhost.

6.2 FTP (vsftpd)

Vulnerabilidad identificada:

- Servicio innecesario y potencialmente inseguro.

Acción correctiva:

```
bash
sudo systemctl stop vsftpd
sudo systemctl disable vsftpd
```

Resultado:

- Servicio deshabilitado permanentemente.

6.3 SSH

Vulnerabilidades detectadas:

- Acceso root habilitado.
- Autenticación por contraseña activa.

Hardening aplicado:

```
bash
sudo nano /etc/ssh/sshd_config
```

Configuración:

```
text
PermitRootLogin no
PasswordAuthentication no
AllowUsers Debian
sudo systemctl restart ssh
```

Resultado:

- Eliminación del vector de ataque original.

7. ANÁLISIS DE ARCHIVOS, PROCESOS Y CAMBIOS INUSUALES

Se revisaron:

- Procesos activos con `ps aux`.
- Permisos de archivos sensibles.
- Directorios críticos del sistema.

No se detectaron backdoors ni binarios modificados.

8. ESCANEO DE MALWARE Y ROOTKITS

8.1 Chkrootkit

```bash
sudo chkrootkit
```

Resultado:

- Sin detecciones positivas.

8.2 Rkhunter

```bash
sudo rkhunter --update
```

```bash
sudo rkhunter --check --sk
```

Resultado:

- Advertencias menores relacionadas con IPC.
- Sin evidencia de rootkits activos.

9. CONTENCIÓN Y BLOQUEO DEL EXPLOIT

9.1 Firewall (UFW)

```bash
sudo ufw default deny incoming
sudo ufw allow 22/tcp
sudo ufw allow 80/tcp
sudo ufw enable

sudo ufw status verbose
```

Resultado:

- Solo puertos esenciales abiertos.

10. REVERSIÓN DE CAMBIOS MALICIOSOS

- Eliminación de configuraciones inseguras.
- Validación de integridad del sistema.

11. HARDENING APLICADO EN FASE 1

Se aplicaron medidas de hardenización sobre SSH, MySQL, FTP, firewall, permisos de archivos y protección contra fuerza bruta (Fail2Ban), reduciendo significativamente la superficie de ataque.

12. ALINEACIÓN CON ISO/IEC 27001

- A.5 Gestión de incidentes

- A.9 Control de acceso
- A.12 Seguridad operacional

13. CONCLUSIÓN

La Fase 1 permitió identificar, contener y mitigar un acceso no autorizado crítico. El sistema quedó en un estado considerablemente más seguro y alineado con buenas prácticas profesionales.

14. RECOMENDACIONES FUTURAS

- Implementar autenticación por clave pública.
- Centralizar logs.
- Auditorías periódicas.
- Implementación de monitoreo continuo SIEM.
- Principio de menor privilegio
- Establecer políticas DLP contundentes.