# Plan de Recuperación para Incidencias

## 1. Introducción

Este documento establece un **Plan de Recuperación ante Incidencias** para mitigar el impacto de futuros ataques o fallos de seguridad en el servidor Debian Hackeado. Este plan detalla los procedimientos para la identificación, contención, erradicación y recuperación del sistema en caso de una nueva intrusión. Además, incluye medidas preventivas para fortalecer la seguridad y minimizar el tiempo de inactividad.

El objetivo es garantizar la continuidad operativa del sistema, reducir el riesgo de pérdida de datos y permitir una respuesta eficiente y estructurada ante incidentes de seguridad.

---

## 2. Identificación de Incidentes

### 2.1 Monitoreo de registros y alertas

- Implementación de `fail2ban` para detectar intentos de acceso sospechosos.
- Revisión periódica de `/var/log/auth.log`, `/var/log/syslog` y `/var/log/secure`.
- Configuración de alertas automáticas mediante herramientas como **OSSEC** o **Wazuh**.

### 2.2 Análisis de tráfico y actividad anómala

- Uso de `iptables` y `netstat` para monitorear conexiones activas.
- Implementación de `Snort` o `Suricata` para análisis de tráfico malicioso.
- Revisión de procesos activos mediante `ps aux` y `htop`.

### 2.3 Verificación de integridad del sistema

- Implementación de `AIDE` (Advanced Intrusion Detection Environment) para detectar cambios en archivos críticos.
- Uso de `chkrootkit` y `rkhunter` de manera periódica.

## 3. Contención del Incidente

### 3.1 Aislamiento del sistema comprometido

- Se identificaron y detuvieron procesos sospechosos (`speech-dispatcher`, `orca`) que no eran necesarios para el funcionamiento del servidor.
- Se eliminaron archivos y directorios con código sospechoso en `/usr/lib/ruby/`, `/usr/lib/libreoffice/` y `/home/debian/.local/share/orca`.
- Se ejecutaron herramientas de análisis (`chkrootkit` y `rkhunter`) para verificar la existencia de rootkits y malware.

### 3.2 Reforzamiento del Sistema

- Desconectar la máquina afectada de la red para evitar la propagación del ataque.
- Deshabilitar servicios críticos como SSH (`systemctl stop ssh`), HTTP (`systemctl stop apache2`) y FTP (`systemctl stop vsftpd`).
- Revocar accesos de usuarios sospechosos (`sudo userdel -r usuario_sospechoso`).

### 3.3 Restricción de accesos

- Modificación temporal de `iptables` para bloquear tráfico externo no autorizado.
- Cambio de contraseñas de administradores y usuarios críticos.

---

## 4. Erradicación del Ataque

### 4.1 Eliminación de archivos maliciosos

- Revisión y eliminación de archivos sospechosos en `/usr/lib/`, `/var/log/`, `/opt/` y `/tmp/`.
- Ejecución de `find / -type f -mtime -7` para identificar archivos recientemente modificados.

### 4.2 Eliminación de procesos sospechosos

- Identificación de procesos maliciosos con `ps aux | grep sospechoso`.
- Detención y eliminación de procesos (`kill -9 PID`).

### 4.3 Auditoría y reconfiguración de servicios

- Revisión de configuraciones en `/etc/ssh/sshd_config` para restringir accesos.

- Reconfiguración de `fail2ban` y `ufw` para mayor control de accesos.

---

## 5. Recuperación y Restauración del Sistema

### 5.1. Restauración de copias de seguridad

- Uso de **snapshots** previos del sistema en caso de daño irreversible.
- Restauración de archivos críticos desde backups seguros (`rsync -av /backup /etc/`).

### 5.2. Reinstalación y actualización del sistema

- Ejecución de `apt update && apt upgrade -y`.
- Reinstalación de servicios afectados (`apt reinstall servicio`).
- Verificación de integridad con `dpkg --verify`.

### 5.3. Rehabilitación de accesos

- Habilitación progresiva de servicios críticos (SSH, Apache, MySQL).
- Monitoreo intensivo durante las primeras 72 horas tras la recuperación.

---

## 6. Medidas Preventivas

### 6.1. Fortalecimiento de la autenticación

- Implementación de **autenticación en dos factores (2FA)** para accesos administrativos.
- Uso exclusivo de claves SSH (`PasswordAuthentication no`).

### 6.2. Políticas de gestión de usuarios

- Auditoría de cuentas activas en `/etc/passwd` y `/etc/shadow`.
- Restricción de privilegios a usuarios según el principio de **mínimos privilegios**.

### 6.3. Revisión periódica de logs y configuraciones

- Implementación de **scripts automatizados** para análisis de logs cada 24 horas.
- Alertas en tiempo real mediante `logwatch`.

## Conclusión

Este plan de recuperación establece los procedimientos detallados para detectar, contener, erradicar y recuperar el sistema en caso de incidentes de seguridad. La aplicación de este plan garantizará el aguante y la resiliencia del servidor y permitirá mantener un entorno seguro y estable.

Se recomienda realizar pruebas periódicas de este plan y capacitar a los administradores del sistema en su implementación.