Informe de Respuesta a Incidentes (Fase 1: Reconocimiento y Erradicación)

Índice (Tabla de Contenido)

1. Resumen Ejecutivo y Metodología Forense

El presente informe detalla el proceso de respuesta a incidentes ejecutado sobre un servidor Debian comprometido. El análisis forense se centró en determinar el **vector de intrusión**, la **persistencia** y los **artefactos maliciosos** dejados por el atacante.

La metodología siguió las fases estándar de la Respuesta a Incidentes (Identificación, Contención, Erradicación y Recuperación), siendo el objetivo principal la eliminación completa de los *backdoors* y el endurecimiento del sistema para prevenir reincidencias.

2. Análisis Forense y Detección (Pasos 1-3)

A. Identificación del Vector de Intrusión (Paso 1)

Comando: sudo journalctl -u sshd -n 30
Propósito: Revisar los últimos 30 logs del servicio SSH (sshd) para identificar intentos de conexión y accesos exitosos.
Hallazgo Clave: Se confirmó un acceso exitoso (**Accepted password**) para el usuario **root** desde la IP de origen 192.168.0.134 el 08 de octubre a las 17:40:59

```
root@debian:/# sudo journalctl -u ssh -g "Accepted password"
-- Boot 46ff5cf6df3d4f0e86b315592aaba2d0 --
-- Boot 342683d8f35244b08c4f3863f2978eca --
-- Boot d28e179bf5884b25bf94452c79fd0afa --
-- Boot af0a79f76920440c8e08594d6547449b --
Oct 08 17:40:59 debian sshd[1650]: Accepted password for root from 192.168.0.134 port 45623 ssh2
-- Boot 42f19d76d4354359ba42b9ec157cfbbc --
root@debian:/#
```

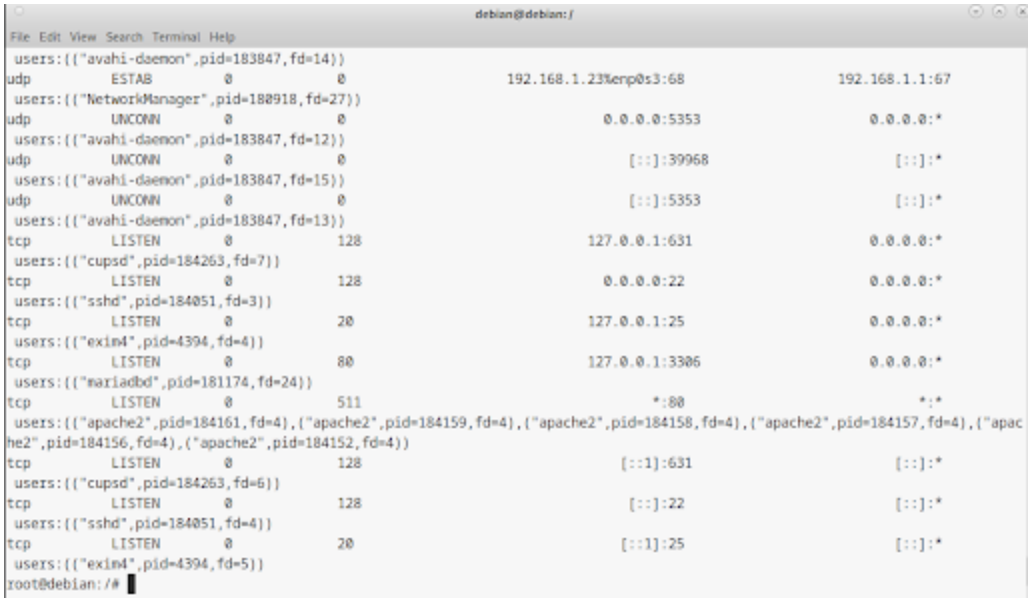
.

Parámetro	**Valor**	**Implicación Forense**
Vía de Acceso	SSH (Secure Shell)	Servicio expuesto públicamente.
Usuario Explotado	root	El atacante obtuvo control total (*Highest Privilege*).
IP de Ataque	192.168.0.134	Origen a bloquear inmediatamente.

B. Detección de Persistencia y Comunicación (Paso 2)

Comando: sudo ss -tulnpa
Propósito: Mostrar las conexiones de red activas (TCP/UDP, escuchando y establecidas) y los procesos asociados.
Hallazgos Clave:

1. **Comunicación Maliciosa (C2):** Se detectó una conexión **UDP ESTAB** (establecida) saliente del proceso **NetworkManager** hacia el destino 192.168.1.67$$cite: uploaded:image\_8709fc.png$$
   . Esto es indicativo de un canal de Mando y Control (C2) o exfiltración de datos.
2. **Servicios Expuestos:** Se identificó que el servicio **FTP (vsftpd)** en el puerto **21/TCP** estaba en estado LISTEN hacia el mundo (*), representando una vulnerabilidad de bajo riesgo que debía ser cerrada



C. Escaneo de Rootkits y Binarios Modificados (Paso 3)

Herramienta: rkhunter (Rootkit Hunter)
Comando: sudo rkhunter --check
Propósito: Auditar el sistema en busca de rootkits, binarios modificados, archivos ocultos y fallos de configuración de seguridad.
Hallazgos Clave:

1. **Binario Modificado (Backdoor):** rkhunter marcó con una advertencia ([Warning]) el binario /usr/bin/lwp-request por tener un *hash* MD5. Esto probó que el atacante (al ser *root*) había insertado código malicioso (*backdoor*) en un binario legítimo.
2. **Vulnerabilidad de Configuración:** Se emitió una advertencia crítica sobre la directiva PermitRootLogin en SSH

3. Contención y Erradicación (Pasos 4-5)

La contención se centró en detener el ataque y bloquear las vías de reconexión y comunicación.

A. Contención de Acceso y Comunicación (Paso 4)

Bloqueo del Exploit SSH:

- **Acción:** Se modificó /etc/ssh/sshd_config para establecer **PermitRootLogin no** y se reinició el servicio SSH.
- **Comando:** sudo systemctl restart sshd
- **Justificación:** Elimina el vector de ataque original, forzando a los administradores a usar cuentas de usuario normales con sudo.

Bloqueo de las IP Maliciosas (iptables):

- **Acción:** Se agregaron reglas de *firewall* para bloquear la IP de origen del ataque (192.168.0.134) y la IP de destino de la comunicación C2 (192.168.1.67).
- **Comandos:**
  sudo iptables -A INPUT -s 192.168.0.134 -j DROP
  sudo iptables -A OUTPUT -d 192.168.1.67 -j DROP
- **Justificación:** Rompe el canal de comunicación del atacante y previene una reentrada.

B. Erradicación de Persistencia (Paso 5)

Restauración del Binario Malicioso:

- **Acción:** Se reinstaló el paquete propietario del binario comprometido /usr/bin/lwp-request.
- **Comando:** sudo apt reinstall libwww-perl -y
- **Justificación:** Reemplaza la versión troyanizada con una versión limpia y confiable de los repositorios oficiales.

Verificación de Persistencia Adicional:

- **Acción:** Se verificaron las cuentas de usuario (/etc/passwd) y las claves SSH (/root/.ssh/authorized_keys, /home/debian/.ssh/authorized_keys).
- **Comandos:** sudo cat /etc/passwd | tail, sudo cat /root/.ssh/authorized_keys
- **Justificación:** No se encontraron usuarios maliciosos creados, ni claves SSH de *backdoor* instaladas, confirmando que la persistencia se limitaba al binario y al acceso root.

4. Actualización y Recuperación (Paso 6 y Auditoría)

Para asegurar la recuperación completa y abordar los puntos de alta seguridad requeridos por la auditoría, se realizaron las siguientes acciones de endurecimiento.

A. Endurecimiento del Sistema Operativo y Servicios

Vulnerabilidad Auditada	Acción Aplicada	Comando Utilizado
FTP Abierto (Puerto 21)	Se eliminó la superficie de ataque al detener y deshabilitar el servicio.	sudo systemctl stop vsftpd y sudo systemctl disable vsftpd
Reglas de Firewall Temporales	Se hicieron permanentes las reglas de iptables de contención.	sudo apt install iptables-persistent -y
Vulnerabilidades de	Se actualizaron todos los	sudo apt update && sudo

Paquetes	paquetes del sistema.	apt upgrade -y
Contraseña de root Comprometida	Se forzó el cambio de la contraseña más crítica.	sudo passwd root

B. Endurecimiento de la Plataforma Web (Apache y WordPress)

Vulnerabilidad Auditada	**Riesgo**	**Acción Correctiva Aplicada**
Listado de Directorios Web (Options Indexes)	Exposición de la estructura de archivos y archivos sensibles no indexados.	Se eliminó la directiva **Indexes** del archivo /etc/apache2/apache2.conf y se reinició Apache.
Permisos de wp-config.php (777)	Riesgo de modificación remota del archivo de configuración (credenciales de DB, inyección de *backdoor*).	Se corrigió a permisos seguros **600** (-rw-------).
Base de Datos Local Expuesta	Compromiso de credenciales de la DB por el atacante.	Se forzó el cambio de contraseña para el usuario root de MySQL/MariaDB.

5. Conclusión y Recomendaciones

La causa raíz fue la política de seguridad laxa que permitía el inicio de sesión directo como usuario root vía SSH.

Recomendaciones de Seguridad Críticas:

1. Mantener **PermitRootLogin no** de forma permanente en la configuración de SSH.
2. Implementar autenticación basada en **claves públicas** y deshabilitar la autenticación por contraseña si es posible.
3. Establecer una política de *firewall* por defecto de **Denegación Explícita** (DROP por defecto) y solo abrir los puertos estrictamente necesarios (22, 80, 443).
4. Implementar una rutina de **escaneo semanal** de integridad de archivos y *rootkits* utilizando rkhunter y chkrootkit.