Informe de Incidente de Seguridad

1. Introducción

Este informe documenta en detalle el análisis forense realizado tras la detección de una intrusión en el servidor Debian Hackeado. Se expone un análisis de los eventos que llevaron a la vulnerabilidad del sistema, la metodología utilizada por el atacante, la recopilación de evidencias clave y las acciones correctivas implementadas para garantizar la seguridad del servidor.

Se describen los procedimientos utilizados para detectar actividad maliciosa, las herramientas empleadas para el análisis y mitigación de amenazas, y las recomnedaciones para la prevención de futuros ataques. El objetivo final de este informe es proporcionar un entendimiento detallado del incidente y establecer protocolos de seguridad que fortalezcan la infraestructura informática de la organización.

---

2. Descripción del Incidente

2.1 Contexto

El servidor Debian en cuestión opera en un entorno simulado que representa un sistema de producción crítico. Se identificó una posible intrusión tras notar comportamientos anómalos en los servicios del sistema y en los registros de accesos. El análisis inicial evidenció múltiples intentos de acceso remoto sospechosos y configuraciones débiles en los servicios de autenticación del servidor, lo que permitió a un atacante explotar dichas debilidades para comprometer el sistema.

2.2 Hallazgos Clave

Intentos de acceso sospechosos:

- Se analizaron los registros de acceso en `/var/log/lastlog` y se encontraron conexiones desde la IP no reconocida `192.168.1.133`, lo que sugiere un acceso no autorizado.
- Se observaron intentos de fuerza bruta contra el servicio SSH, lo que indica un esfuerzo deliberado por vulnerar credenciales débiles.
- Se encontraron rastros de accesos repetidos con contraseñas incorrectas, lo que refuerza la hipótesis de un ataque de diccionario contra el sistema.

2. **Procesos sospechosos:**
    - Se identificaron servicios no esenciales en ejecución, como `speech-dispatcher` y `orca`, que no corresponden a la configuración habitual del servidor.
    - Se detectaron procesos en ejecución sin un usuario o propósito claro, lo que podría sugerir la presencia de malware o puertas traseras dejadas por el atacante.
3. **Archivos modificados recientemente:**
    - Se realizó una búsqueda de archivos recientes en `/usr/lib/ruby/`, `/usr/lib/libreoffice/` y `/var/log/`, donde se encontraron múltiples modificaciones sin justificación aparente.
    - Se detectaron archivos con nombres inusuales en directorios de sistema, algunos de los cuales contenían scripts con referencias a conexiones remotas.
    - Se identificó una posible manipulación de registros de autenticación para ocultar rastros del acceso ilegítimo.
4. **Configuraciones inseguras:**
    - Se verificó el archivo de configuración de SSH en `/etc/ssh/sshd_config`, donde se encontró la directiva `PermitRootLogin yes`, permitiendo que el usuario root se autenticara remotamente.
    - `PasswordAuthentication yes` estaba habilitado, lo que permitió la autenticación mediante contraseñas en lugar del uso de claves públicas, reduciendo la seguridad del servicio.
    - Se identificó que el usuario `debian` tenía credenciales débiles y privilegios elevados, facilitando una escalación de privilegios por parte del atacante.
5. **Explotación del sistema:**
    - Mediante la herramienta `hydra`, el atacante realizó un ataque de fuerza bruta contra SSH y logró acceder al sistema con la combinación de usuario y contraseña `debian:123456`.
    - Una vez dentro del sistema, el atacante aprovechó la configuración de `sudo` sin restricciones para escalar privilegios a root y obtener control total del servidor.
    - Se detectaron intentos de establecer conexiones externas, lo que sugiere la posible instalación de herramientas de acceso remoto o backdoors.

3. Acciones Correctivas

3.1 Eliminación de Amenazas

- 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

- Configuraciones de SSH:
  - Se editó el archivo `/etc/ssh/sshd_config` para deshabilitar accesos inseguros:
    - `PermitRootLogin no`
    - `PasswordAuthentication no`
  - Se configuró el uso exclusivo de claves SSH para la autenticación remota.
  - Se restringió el acceso al puerto SSH solo a direcciones IP de confianza mediante reglas de firewall.
- Actualización de software y paquetes utilizando `apt update && apt upgrade -y` para corregir vulnerabilidades conocidas.
- Implementación de firewall con `iptables`:
  - Se bloquearon los puertos 80 (HTTP), 21 (FTP) y 3306 (MySQL) para reducir la exposición a ataques.
  - Se permitió únicamente el acceso por SSH restringido a IPs de confianza

3.3 Refuerzo de Contraseñas

- Se cambiaron las credenciales de los usuarios del sistema, estableciendo otras contraseñas.
- Se implementaron políticas de seguridad para la gestión de credenciales, incluyendo la expiración periódica de contraseñas.
- Se configuró el uso obligatorio de autenticación en dos factores para accesos administrativos.

Conclusión

Tras la detección y análisis del incidente, se han implementado correciones para restaurar la seguridad del servidor. Se han eliminado configuraciones inseguras, archivos maliciosos y accesos no autorizados. La implementación de un firewall, la restricción de accesos mediante SSH y el refuerzo de contraseñas han reducido significativamente la superficie de ataque del sistema.

Se recomienda establecer auditorías de seguridad regulares y continuar con la educación en ciberseguridad para prevenir futuras intrusiones. Este informe servirá como referencia para mejorar las estrategias de seguridad y respuesta ante incidentes en la infraestructura de la organización.