1. Informe de Incidente de Seguridad

ID del Incidente: IS-20250403-001

Fecha y Hora de Detección: 3 de Abril de 2025, ~14:07 (Durante prueba de penetración autorizada)

Fecha y Hora de Resolución: 03/04/2025 desde las 14:07 hasta las 23:00.

Preparado por: Rodrigo Martinez

Clasificación: CRÍTICO

1.1. Resumen Ejecutivo

El presente informe detalla un incidente de seguridad crítico detectado el 3 de Abril de 2025 en el servidor Debian ubicado en la IP 10.0.2.11. Durante una prueba de penetración autorizada, se logró obtener **acceso administrativo completo (root)** al sistema mediante un ataque de fuerza bruta contra el servicio SSH. La causa raíz fue una combinación de configuraciones SSH inseguras (permiso de login root, autenticación por contraseña) y el uso de una contraseña extremadamente débil (123456) para la cuenta root, la cual además era reutilizada por otros servicios. El impacto potencial de este compromiso es máximo, incluyendo el acceso y manipulación total de datos, instalación de software malicioso y uso del servidor para fines ilícitos. Se iniciaron inmediatamente acciones de contención y erradicación, seguidas de medidas correctivas y preventivas detalladas en este documento para restaurar la seguridad del sistema y evitar recurrencias.

1.2. Descripción del Incidente

Durante la ejecución de pruebas de penetración planificadas y autorizadas sobre el servidor 10.0.2.11, se identificó que el servicio SSH (puerto 22) permitía la autenticación mediante contraseña y el inicio de sesión directo del usuario root. Se procedió a realizar un ataque de fuerza bruta dirigido a la cuenta root utilizando una lista de contraseñas comunes (rockyou.txt). Aproximadamente a las 14:07 del 3 de Abril de 2025, la herramienta Hydra confirmó éxito al identificar la contraseña 123456 para el usuario root, otorgando acceso administrativo completo al sistema.

- **Sistema(s) Afectado(s):** Servidor Debian (10.0.2.11)
- **Tipo de Incidente:** Acceso no autorizado / Compromiso de cuenta privilegiada (root).
- **Vector de Ataque:** Fuerza bruta de credenciales contra servicio SSH.
- **Método de Detección:** Prueba de penetración activa autorizada.

1.3. Análisis Forense (Causa Raíz)

El análisis determinó que el compromiso fue posible debido a una concatenación de malas configuraciones y prácticas de seguridad:

1. **Configuración SSH Insegura:** El archivo /etc/ssh/sshd_config permitía explícitamente el login como root (PermitRootLogin yes) y la autenticación basada en contraseñas (PasswordAuthentication yes).
2. **Contraseña Extremadamente Débil:** La cuenta root utilizaba la contraseña 123456, presente en diccionarios de fuerza bruta estándar.
3. **Ausencia de Firewall:** No existían reglas de firewall (ufw o nftables) que limitaran el acceso al puerto SSH (22) desde redes externas o aplicaran políticas de bloqueo tras intentos fallidos (fail2ban no estaba implementado/verificado).
4. **Reutilización de Contraseñas:** La misma contraseña débil (123456) fue identificada también para el usuario wordpressuser de la base de datos MySQL, indicando una pobre gestión de credenciales.
5. **(Factor Contribuyente) Falta de Hardening:** El sistema carecía de un endurecimiento básico en servicios críticos como SSH.

1.4. Impacto del Incidente

La obtención de acceso root representa el **máximo nivel de compromiso** posible en un sistema Linux. El impacto potencial incluye, pero no se limita a:

- **Confidencialidad:** Acceso total para leer cualquier archivo del sistema, incluyendo datos sensibles de la aplicación WordPress (configuración, base de datos), claves privadas, información de otros usuarios.
- **Integridad:** Capacidad para modificar o eliminar cualquier archivo o dato del sistema, instalar software (malware, rootkits, backdoors), alterar logs para ocultar actividad, modificar el contenido del sitio web.

- **Disponibilidad:** Posibilidad de detener servicios críticos, eliminar archivos esenciales del sistema operativo o lanzar ataques de denegación de servicio desde el servidor comprometido.
- **Reputacional y Legal:** Uso del servidor como plataforma para lanzar ataques a terceros, enviar spam, alojar contenido ilegal, etc.

Aunque el compromiso se detectó en un entorno de prueba controlado, si hubiera ocurrido en producción por un actor malicioso, las consecuencias habrían sido severas.

1.5. Acciones de Contención, Erradicación y Recuperación

Tras la detección del compromiso durante el pentest, se definieron y ejecutaron (o se planificó su ejecución inmediata) las siguientes acciones, basadas en las recomendaciones del Informe de Pentesting asociado:

- **Contención Inmediata:**
    - **(Acción Crítica 1)** Cambio inmediato de la contraseña del usuario root a una contraseña compleja, larga y única (iYpiDTm6hkUE9K).
    - **(Acción Crítica 2)** Modificación de /etc/ssh/sshd_config para establecer PermitRootLogin no y PasswordAuthentication no.
    - Implementación y obligatoriedad de autenticación basada en claves públicas SSH para todos los accesos administrativos.
    - Reinicio del servicio SSH (sudo systemctl restart sshd).
- **Erradicación:**
    - Realización de un análisis exhaustivo del sistema en busca de posibles modificaciones no autorizadas, archivos sospechosos, procesos ocultos o backdoors (usando herramientas como chkrootkit, rkhunter, análisis manual de logs y procesos). *Nota: Dada la naturaleza del compromiso root, se recomendó encarecidamente considerar una reinstalación limpia del sistema desde una fuente confiable si no se puede garantizar la eliminación completa de cualquier posible malware.*
    - Actualización completa del sistema operativo y todos los paquetes (sudo apt update && sudo apt dist-upgrade), incluyendo OpenSSH y vsftpd.

- **Recuperación y Hardening:**
    - Implementación de reglas de firewall con ufw (default deny incoming, allow outgoing, allow 80/tcp, allow 443/tcp, allow from 10.0.2.6 proto tcp to any port 22), estableciendo una política por defecto de denegación de entrada y permitiendo explícitamente solo los servicios necesarios. Activación con sudo ufw enable.
    - Corrección de los permisos inseguros (777) en toda la estructura /var/www/html aplicando permisos estándar (directorios 755, archivos 644) y asegurando la propiedad correcta (chown -R www-data:www-data).
    - Corrección de permisos del archivo wp-config.php (chmod 600).
    - Cambio de la contraseña del usuario wordpressuser de la base de datos a una contraseña robusta y única (MRmscU7HrBqOiK). Actualización de wp-config.php.
    - Generación e implementación de nuevas claves secretas y sales en wp-config.php.
    - Actualización de WordPress a la última versión estable. Revisión y actualización de temas y plugins.
    - Deshabilitación del acceso anónimo en vsftpd (anonymous_enable=NO) y reinicio del servicio. Considerar deshabilitar FTP si no es esencial.
    - Deshabilitación de servicios innecesarios (ej. CUPS: sudo systemctl stop cups; sudo systemctl disable cups).
    - Implementación de Fail2ban para protección SSH contra fuerza bruta (sudo apt install fail2ban, configuración de jail.local, sudo systemctl restart fail2ban).
    - Deshabilitación de XML-RPC en WordPress si no es requerido.
    - Configuración de HTTPS en Apache mediante certificado autofirmado.

1.6. Medidas Preventivas y Lecciones Aprendidas

Para prevenir la recurrencia de este y otros tipos de incidentes de seguridad, y basándose en las lecciones aprendidas de este compromiso crítico, se implementarán y/o reforzarán las siguientes medidas preventivas:

- **6.1. Implementación y Refuerzo de Políticas de Contraseñas Robustas:**
    - **Requisito Mandatorio:** Se establecerá una política de contraseñas obligatoria para **todas** las cuentas (usuarios finales, administradores, cuentas de servicio, aplicaciones).
    - **Complejidad Mínima:** Dicha política exigirá una longitud mínima (ej. 12-15 caracteres), el uso obligatorio de una combinación de mayúsculas, minúsculas, números y símbolos especiales.
    - **Prohibiciones Específicas:** Se prohibirá explícitamente el uso de contraseñas basadas en información personal (nombres, fechas), palabras de diccionario, secuencias obvias (ej. '123456', 'qwerty'), y, crucialmente, **se prohibirá la reutilización de contraseñas** entre diferentes sistemas o servicios, tanto internos como externos. La contraseña 123456, utilizada tanto para root como para wordpressuser, es un ejemplo claro de la práctica a erradicar.
    - **Historial y Rotación:** Se configurará un historial de contraseñas para evitar la reutilización inmediata de contraseñas antiguas y se establecerá una política de rotación periódica (ej. cada 60-90 días) obligatoria, especialmente para cuentas privilegiadas.
    - **Herramientas de Apoyo:** Se promoverá y facilitará el uso de gestores de contraseñas aprobados por la organización para ayudar a los usuarios a generar y almacenar contraseñas complejas y únicas de forma segura.
    - **Aplicación Técnica:** Se configurarán los sistemas operativos y aplicaciones (donde sea posible, ej. mediante módulos PAM en Linux, políticas de directorio activo, configuración de aplicaciones) para **forzar técnicamente** el cumplimiento de estos requisitos de complejidad, historial y rotación.
- **6.2. Programa Integral de Concienciación y Formación en Seguridad:**
    - **Audiencia:** Se desarrollarán módulos de formación adaptados tanto para **usuarios finales** como para el **personal técnico (IT y administradores)**.
    - **Contenido para Usuarios Finales:**
        - **Creación de Contraseñas Seguras:** Énfasis en los criterios de la nueva política (longitud, complejidad, unicidad), cómo evitar patrones predecibles y la importancia crítica de no reutilizar contraseñas. Uso de gestores de contraseñas.

        - **Ingeniería Social y Phishing:** Cómo reconocer correos electrónicos, mensajes y llamadas sospechosas que intentan engañar al usuario para revelar credenciales u otra información sensible. Procedimiento para reportar intentos.
        - **Navegación Segura:** Identificación de sitios web seguros (HTTPS), riesgos de descargas de fuentes no confiables, seguridad en redes Wi-Fi públicas.
        - **Seguridad Física Básica:** Bloqueo de pantallas, protección de dispositivos móviles, manejo seguro de documentos impresos.
    - **Contenido para Personal Técnico (IT/Admin):**
        - Incluye todos los temas de usuarios finales.
        - **Hardening de Sistemas y Servicios:** Aplicación de guías de configuración segura para sistemas operativos (Linux, Windows Server), bases de datos (MySQL/MariaDB), servidores web (Apache), SSH, etc. Principio de Mínima Funcionalidad (deshabilitar servicios innecesarios como CUPS o FTP si no se usan).
        - **Gestión Segura de Credenciales:** Énfasis extremo en la no reutilización de contraseñas privilegiadas, uso de claves SSH en lugar de contraseñas, gestión segura de claves y certificados.
        - **Principio de Mínimo Privilegio:** Asignación de permisos necesarios estrictamente para realizar una función, tanto a nivel de sistema operativo como de aplicaciones.
        - **Gestión de Vulnerabilidades y Parches:** Importancia de la identificación y aplicación oportuna de parches de seguridad.
        - **Monitorización y Respuesta:** Conceptos básicos de lectura e interpretación de logs, reporte de anomalías, procedimientos iniciales de respuesta a incidentes.
    - **Metodología y Frecuencia:** La formación será **obligatoria** para todo el personal, con sesiones iniciales y **refrescos anuales mandatorios**. Se complementará con comunicaciones periódicas (boletines, alertas), posters informativos y, potencialmente,

campañas de simulación de phishing para evaluar la efectividad. El seguimiento de la finalización será mandatorio.

- **6.3. Hardening Específico de SSH:**
    - Mantener la configuración segura establecida post-incidente: PermitRootLogin no, PasswordAuthentication no.
    - Implementar fail2ban o herramientas similares para bloquear automáticamente direcciones IP que realicen múltiples intentos fallidos de autenticación SSH.
    - Considerar el uso de puertos no estándar para SSH (opcional).
    - Limitar el acceso SSH a través del firewall únicamente a direcciones IP o rangos de red autorizados y necesarios.
- **6.4. Gestión de Permisos Estricta:**
    - Auditoría periódica de permisos en sistemas de archivos críticos, especialmente directorios web y de aplicaciones, para asegurar la aplicación del principio de mínimo privilegio.
- **6.5. Implementación y Mantenimiento de Firewall:**
    - Asegurar que **todos** los servidores conectados a la red tengan un firewall de host configurado y activo con políticas restrictivas por defecto. Revisar y auditar las reglas periódicamente.
- **6.6. Proceso Formal de Gestión de Vulnerabilidades y Parches:**
    - Establecer un ciclo regular (ej. mensual) para escanear sistemas en busca de vulnerabilidades.
    - Priorizar y aplicar parches críticos de seguridad de manera oportuna, con un proceso definido para pruebas y despliegue.
- **6.7. Monitorización, Auditoría y Alerta:**
    - Centralizar y revisar regularmente logs críticos (autenticación (/var/log/auth.log), sistema, firewall, aplicaciones). Considerar la implementación de un SIEM.
    - Configurar alertas para eventos de alta sospecha (ej. múltiples logins fallidos con fail2ban, cambios en cuentas privilegiadas, etc.).
- **6.8. Segmentación de Red:**
    - Evaluar la arquitectura de red y, si es posible, implementar segmentación para aislar servidores críticos.

- **6.9. Autenticación Multifactor (MFA):**
    - Implementar MFA (ej. TOTP, llaves de seguridad) como capa adicional obligatoria para todas las cuentas con privilegios administrativos (incluyendo SSH si es posible con configuración adicional) y para accesos remotos VPN/aplicaciones críticas.

Lecciones Aprendidas Clave: Este incidente subraya que la seguridad es un proceso continuo y que las configuraciones por defecto rara vez son seguras. La falta de atención a aspectos básicos como contraseñas fuertes, permisos correctos y defensas básicas (firewall, hardening) crea vulnerabilidades críticas. La formación y concienciación del personal son tan importantes como las herramientas tecnológicas. La reutilización de contraseñas multiplica exponencialmente el riesgo.

1.7. Estado Actual

- **Incidente Cerrado.** (Asumiendo que todas las acciones correctivas principales se han aplicado según las instrucciones). Se mantiene monitorización activa.

1.8. Apéndices

- Referencia: Informe de Pentesting - Máquina Debian (10.0.2.11) - Fecha: 03/04/2025.