Informe de Incidente de Seguridad

Fecha: 9 de enero de 2026

Nombre del Autor: Javi

Proyecto: Análisis y respuesta ante incidente de seguridad

2. Descripción del Incidente

El incidente de seguridad se originó cuando un atacante explotó vulnerabilidades en los servicios expuestos de un servidor.

El atacante aprovechó configuraciones incorrectas en varios servicios para obtener acceso no autorizado al sistema.

A continuación, se describen las principales vulnerabilidades que facilitaron el ataque:

- Acceso no autorizado a directorios web listables
- Acceso anónimo habilitado en FTP
- Contraseña débil en base de datos MySQL
- Configuración insegura de SSH

3. Análisis Forense

3.1. Identificación de la Brecha de Seguridad

- Revisión de Logs: Se revisaron los logs del servidor web, FTP y MySQL para identificar los momentos en que el atacante logró acceder al sistema.
- Análisis de Archivos Comprometidos: Se identificaron archivos modificados o cargados por el

atacante. Esto incluyó scripts maliciosos subidos a directorios accesibles públicamente.

- Escaneo de Puertos y Servicios Expuestos: Se utilizó nmap para escanear los puertos abiertos en el servidor, identificando servicios expuestos que no estaban protegidos adecuadamente.

3.2. Determinación del Alcance del Ataque

- Acceso a la Base de Datos: El atacante logró acceder a la base de datos de MySQL a través de credenciales débiles y pudo extraer datos sensibles de la empresa.
- Exploit de Servicios FTP: Al aprovechar el acceso anónimo en el servicio FTP, el atacante pudo cargar scripts maliciosos que se ejecutaron en el servidor.
- Escalada de Privilegios: Mediante SSH, el atacante escaló privilegios al acceder al servidor como usuario root, lo que le otorgó control total.

4. Acciones Correctivas Implementadas

4.1. Fortalecimiento de Configuraciones de Servicio

- FTP: Se deshabilitó el acceso anónimo en el archivo vsftpd.conf, cambiando la configuración a anonymous_enable=NO y restringiendo el acceso a usuarios autenticados.
- SSH: Se configuró el archivo sshd_config para deshabilitar el acceso como root (PermitRootLogin no) y se implementó autenticación mediante claves SSH, deshabilitando la autenticación por contraseña.
- MySQL: Se restablecieron las contraseñas de las cuentas de usuario con contraseñas fuertes y se configuró MySQL para que solo escuche en 127.0.0.1, evitando conexiones externas.

4.2. Actualización de Software y Parcheo

- Parches de Seguridad: Se aplicaron los parches más recientes a todos los servicios expuestos (Apache, MySQL, FTP, SSH) para corregir vulnerabilidades conocidas.
- Auditoría de Dependencias: Se revisaron todas las dependencias del sistema y se actualizó cualquier software que pudiera estar desactualizado y ser susceptible a vulnerabilidades.

4.3. Remoción de Archivos Maliciosos

- Se eliminaron todos los archivos maliciosos subidos al servidor, incluidos los scripts y herramientas utilizadas por el atacante.
- Se realizó un escaneo exhaustivo de malware en el servidor utilizando ClamAV y herramientas específicas para asegurarse de que el servidor estuviera limpio.

5. Medidas Preventivas Aplicadas

5.1. Reforzamiento de Políticas de Seguridad

- Control de Acceso: Se implementaron políticas más estrictas de control de acceso tanto a nivel de red como de servicios, restringiendo las conexiones solo a direcciones IP confiables.
- Monitoreo y Alerta: Se implementaron soluciones de monitoreo (como fail2ban) para detectar intentos de acceso no autorizado y prevenir ataques de fuerza bruta.
- Auditoría Continua: Se estableció un sistema de auditoría continua para realizar revisiones periódicas de logs y configuraciones de seguridad.

5.2. Seguridad en la Red

- Firewall: Se configuró un firewall a nivel de red utilizando ufw para bloquear puertos innecesarios y restringir el acceso solo a los puertos necesarios.
- Segmentación de la Red: Se implementó una red segmentada para aislar los servicios críticos y limitar el impacto de cualquier brecha futura.

5.3. Entrenamiento y Concienciación

- Se implementaron sesiones de capacitación periódicas para el equipo sobre buenas prácticas de seguridad, incluyendo el uso de contraseñas fuertes y el manejo adecuado de los servicios críticos.

6. Conclusiones

El incidente de seguridad fue mitigado con éxito mediante la implementación de una serie de acciones correctivas y preventivas. Se lograron restablecer las configuraciones seguras de los servicios comprometidos, se eliminaron los archivos maliciosos y se tomaron medidas para prevenir futuros incidentes similares. A pesar de la brecha, la rápida respuesta del equipo permitió minimizar los daños y evitar la exfiltración de datos sensibles.

Es fundamental continuar con las auditorías de seguridad y fortalecer las configuraciones de todos los sistemas expuestos a Internet para reducir la superficie de ataque y proteger los activos de la organización.

Firma:

Javi

Empresa: Javi