Informe de Incidente de Seguridad

- Viviana Mendoza
- 4Geeks

1. Resumen del incidente

Se nos entrega máquina virtual Debian hackeada y se solicita que se realice el análisis forense de la misma. Se nos pide corregir las vulnerabilidades explotadas y garantizar un funcionamiento optimo

2. Detalles del incidente

- **Activo afectado:** Servidor web principal (Debian 12).
- **IP del servidor comprometido:** 192.168.1.90
- **Impacto:**
    - Posible acceso no autorizado a archivos críticos del servidor.

3. Análisis Forense

Mediante el uso del programa Autopsy se ha analizado una copia RAW de la imagen virtual hackeada.
Autopsy nos ha devuelto los archivos encontrados dentro de la máquina virtual y toda la información de interés.
Se ha realizado un análisis exhaustivo en el que se han encontrado posibles indicios de actividad maliciosa.

- Múltiples intentos de acceso al sistema, lo que lleva a una revisión de logs relacionados.
- Credenciales débiles, vulnerables y que podrían permitir que se produjera una infiltración.
- Malas configuraciones que permitirían accesos inseguros.
- Intento de ejecutar comandos con privilegios elevados, con numerosos intentos fallidos. **Faillog.**
- Intentos de modificar registros de inicio en **lastlog.**
- Posibles archivos eliminados en las fechas sospechosas.
- Contraseñas y credenciales débiles en Wordpress que podrían ser explotadas.
- Archivos de configuración de servicios con permisos inadecuados.
- Falta de firewall

A continuación, se ha utilizado Kali Linux para analizar la maquina hackeada. Se ha ejecutado nmap con exploits para poder averiguar los puertos abiertos de la maquina Debian.
Lo que nos ha permitido confirmar algunas de las vulnerabilidades halladas y encontrar otras susceptibles de solucionarse.

3.1. Identificación del ataque:

A nuestro entender no se ha podido identificar claramente el ataque, aunque lo más probable, por el puerto sospechosamente anormal utilizado, es que se haya producido el 8/10/2024 mediante un acceso del puerto 45623 ssh2.
Puesto que Nmap nos revela que ssh es un servicio desactualizado y poco seguro, creemos que es bastante posible que la infiltración se haya llevado acabo ese día.

Sin embargo no podemos descartar indicios de que el día 31/07/2024 también hubo actividad sospecho, varios intentos de ingresar al sistema y también del uso de root.

3.2. Posible Impacto:

Un ingreso no autorizado en el sistema puede tener consecuencias graves para una organización, tanto a nivel de seguridad, operatividad, reputación y cumplimiento normativo.
Podría suponer pérdida de datos sensibles (como datos personales, credenciales de acceso, información financiera o propiedad intelectual) todos datos que pueden tener un alto valor/coste.

El impacto también puede ser económico, como el robo de información financiera, datos bancarios, manipulación contable... y no es solo la información sustraída o secuestrada, sino que la recuperación del daño puede tener un impacto grave en la economía de la empresa, puesto que puede requerir una gran inversión.

Interrupción de servicios, credenciales débiles, accesos no autorizados, podrían poner en jaque la operatividad del sistema, ya que podría permitir al intruso deshabilitar sistemas clave, como servidores, bases de datos, apps críticas, realizar taques que dejen accesibles sitios web o servicios internos o eliminar archivos esenciales para el día a día.

Todo esto puede tener un impacto reputacional e incluso legal dependiendo de la normativa y la gravedad.

En este caso, en la que la mayoría de los servicios estaban desactualizados, la empresa podría tener que asumir gran parte de la culpa de la perdida de datos ya que no estaba utilizando los medios necesarios para proteger su información.

4. Acciones tomadas

Tras el análisis del sistema, se han tomado las siguientes medidas:

- Actualización del sistema al completo.
- Actualización de los servicios clave:
    - Apache
    - SSH
    - FTP
    - Wordpress
- Configuración correcta de los servicios, modificación de archivos de configuración.
- Modificación de permisos de archivos clave, como wp-config.php.
- Cambio de credenciales sensibles, como MariaDB.
- Modificación de políticas de contraseñas.
- Instalación de firewall (ufw)
- Cierre de puertos innecesarios o recomendación de cierre en caso de que no se estén utilizando.

Todas las medidas están detalladas en el informe de Pentesting.

5. Medidas inmediatas: Acciones que se tomaron inmediatamente después de detectar el incidente

Puesto que el punto de intrusión más probable era el puerto no habitual para el servicio ssh2, se concluyó que lo primero que debía hacerse es suspender el servicio de manera momentánea.
Se procedió a la actualización y configuración de este, para hacerlo más seguro y que no vuelva a repetirse.

6. Medidas futuras:

Se recomienda el uso de programas de monitorización, como wazuh.

Se recomienda implementar alertas ante intrusiones.

Se recomienda implementar alertas de cambio de contraseñas

Se recomienda deshabilitar puertos que no se use e implementar políticas de uso solo en caso de necesidad.

Se recomienda la creación de formación orientada al usuario, concienciar en seguridad.

7. Conclusión

La falta de actualización del sistema, las configuraciones por defecto o mal configuradas, hacen del sistema uno vulnerable. Es imprescindible mantener el sistema y los servicios actualizados a la última versión. En este caso puede haber sido precisamente un sistema obsoleto y una configuración vulnerable lo que haya facilitado el ataque.

Por lo que también es recomendable revisar las configuraciones existentes de manera regular.

El cierre de puertos no utilizados también sería una buena práctica, aplicar reglas para mantener los mínimos puertos necesarios abiertos. Se pueden crear listas blancas o listas negras de puertos, lo que haga el sistema más seguro, sin dejar de ser funcional.

Dada la evidencia de credenciales extremadamente débiles, es imprescindible que se realice una campaña de concienciación al personal, para que esto no vuelva a ocurrir. Así como implantar una política de contraseñas seguras, que incluya avisos, recordatorios e incluso la petición de cambio obligatorio.