Reporte Ejecutivo de Ciberseguridad: Análisis de Vulnerabilidad y Explotación en el Sistema "WalkingCms"

1. Portada

- **Título del Reporte**: Análisis de Vulnerabilidad y Explotación en el Sistema "WalkingCms"
- **Fecha**: 28 de junio de 2024
- **Nombre de la Organización**: [N/A]
- **Autor(es)**: tellmefred

2. Resumen Ejecutivo

Este informe documenta la identificación y explotación de vulnerabilidades en el sistema "WalkingCms", un entorno práctico de DockerLabs. Se llevó a cabo un fuzzing web y una enumeración de WordPress para identificar usuarios. Posteriormente, se utilizó un ataque de fuerza bruta en el servicio XML-RPC para obtener acceso al panel de control de WordPress, donde se cargó una web shell para ejecutar comandos remotos. Finalmente, se logró una escalación de privilegios que permitió obtener acceso root al sistema. Se proporcionan recomendaciones para mitigar estas vulnerabilidades y fortalecer la seguridad del sistema.

3. Introducción

- **Contexto**: El sistema "WalkingCms" es un entorno WordPress que presentaba vulnerabilidades explotables a través de técnicas de fuzzing, enumeración de usuarios, y fuerza bruta en el servicio XML-RPC.
- **Propósito**: Evaluar la seguridad del sistema WordPress, identificar vulnerabilidades, y proponer medidas correctivas para reducir los riesgos de seguridad.
- **Alcance**: Incluye la exploración de servicios web, la enumeración de usuarios en WordPress, el uso de fuerza bruta para obtener acceso, y la escalación de privilegios para obtener acceso root.
- **Metodología**: Se utilizó un enfoque sistemático que incluyó escaneos de red, fuzzing web, ataques de fuerza bruta, y técnicas de post-explotación para obtener acceso privilegiado al sistema.

4. Estado Actual de la Ciberseguridad

- **Resumen de la Postura de Ciberseguridad**: El sistema "WalkingCms" presenta vulnerabilidades críticas en WordPress que permitieron comprometer el sistema y escalar privilegios a root.
- **Sistemas y Datos Críticos**: Servicios web y archivos del sistema.

5. Evaluación de Vulnerabilidades y Explotación

- **Reconocimiento**:

    - **Escaneo de Red**: Un escaneo de Nmap reveló el puerto 80 (HTTP) abierto con un sitio web de WordPress accesible.
    - **Fuzzing y Enumeración**: Utilizando Gobuster, se identificó la ruta `http://172.17.0.2/wordpress`, y a través de la herramienta WPScan se descubrió el usuario "Mario".
- **Explotación**:
    - **Fuerza Bruta en XML-RPC**: Se realizó un ataque de fuerza bruta utilizando el diccionario `rockyou.txt`, lo que permitió descubrir la contraseña "love" para el usuario "Mario".
    - **Acceso al Panel de Control**: Con las credenciales obtenidas, se accedió al panel de administración de WordPress, donde se cargó una web shell mediante la edición de un archivo de tema.
- **Escalada de Privilegios**:
    - **Ejecución de SUID en 'env'**: Se identificó el binario `env` con permisos SUID, lo que permitió ejecutar `/bin/sh -p` y obtener acceso root al sistema.

6. Recomendaciones

- **Fortalecimiento de la Seguridad de WordPress**: Implementar medidas de seguridad adicionales como la eliminación de usuarios predeterminados y la restricción de acceso a archivos sensibles.
- **Monitoreo de Actividades Sospechosas**: Implementar sistemas de detección de intrusiones para identificar y responder a actividades no autorizadas en tiempo real.
- **Revisión y Restricción de Permisos SUID**: Realizar auditorías periódicas de permisos SUID en el sistema para evitar escalaciones de privilegios similares.
- **Capacitación en Ciberseguridad**: Entrenar al personal en la administración segura de sistemas WordPress y en la importancia de mantener los sistemas actualizados.

7. Conclusión

El análisis del sistema "WalkingCms" demostró que, mediante la explotación de vulnerabilidades en WordPress y el uso de permisos SUID mal configurados, un atacante puede comprometer gravemente la seguridad del sistema. Es crucial implementar las recomendaciones propuestas para mitigar estos riesgos y mejorar la postura de seguridad del sistema.

8. Anexos

- Detalles técnicos sobre la explotación de WordPress y la carga de la web shell.
- Resultados de escaneos de red y análisis de servicios.
- Capturas de pantalla y comandos utilizados durante la explotación y la escalación de privilegios.