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

1. Portada

- **Título del Reporte**: Análisis de Vulnerabilidad y Explotación en el Sistema "Asucar"
- **Fecha**: 14 de julio 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 "Asucar", un entorno práctico de DockerLabs. Se explotó una vulnerabilidad de Inclusión Local de Archivos (LFI) para acceder a archivos sensibles en el servidor. Posteriormente, se realizó un ataque de fuerza bruta en el servicio XML-RPC de WordPress para obtener credenciales y se utilizó el programa `puttygen` con privilegios root para generar una clave RSA que permitió el acceso como root al sistema. Se proporcionan recomendaciones para mitigar estas vulnerabilidades y fortalecer la seguridad del sistema.

3. Introducción

- **Contexto**: El sistema "Asucar" es un entorno vulnerable que presenta un LFI explotable y un servicio XML-RPC activo en WordPress, que permitió realizar un ataque de fuerza bruta para comprometer credenciales.
- **Propósito**: Evaluar la seguridad del sistema web basado en WordPress, identificar vulnerabilidades, y proponer medidas correctivas para reducir los riesgos de seguridad.
- **Alcance**: Incluye la explotación de LFI, ataques de fuerza bruta en XML-RPC, y la escalación de privilegios para obtener acceso root.
- **Metodología**: Se utilizó un enfoque sistemático que incluyó escaneos de red, explotación de LFI, 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 "Asucar" presenta vulnerabilidades críticas en su configuración de WordPress, específicamente un LFI explotable y la falta de protección contra ataques de fuerza bruta en XML-RPC, que fueron utilizados para comprometer el sistema y escalar privilegios a root.
- **Sistemas y Datos Críticos**: Servicios web (WordPress) y archivos sensibles del sistema.

5. Evaluación de Vulnerabilidades y Explotación

- **Reconocimiento**:
    - **Escaneo de Red**: Un escaneo de Nmap reveló los puertos 22 (SSH) y 80 (HTTP) abiertos.

    - **Enumeración de WordPress**: Con WPScan se detectó un servicio XML-RPC activo y un directorio `uploads` accesible.
- **Explotación**:
    - **Vulnerabilidad LFI**: Se identificó y explotó una vulnerabilidad de Inclusión Local de Archivos (LFI), lo que permitió acceder a archivos sensibles en el servidor.
    - **Ataque de Fuerza Bruta en XML-RPC**: Se realizó un ataque de fuerza bruta para descubrir la contraseña "password1" para el usuario "Curiosito".
- **Escalada de Privilegios**:
    - **Uso de Puttygen con Permisos Root**: Tras obtener acceso con las credenciales del usuario, se identificó que el comando `puttygen` podía ejecutarse con permisos root. Se utilizó este programa para generar una clave RSA y obtener acceso root al sistema.

6. Recomendaciones

- **Corrección de la Vulnerabilidad LFI**: Es crucial revisar y corregir la configuración del servidor para prevenir accesos no autorizados a través de LFI.
- **Fortalecimiento de la Seguridad de WordPress**: Implementar medidas de seguridad adicionales, como la desactivación del servicio XML-RPC si no es necesario, y aplicar límites de intentos de inicio de sesión para prevenir ataques de fuerza bruta.
- **Monitoreo de Actividades Sospechosas**: Implementar sistemas de detección de intrusiones (IDS) para identificar y responder a actividades no autorizadas en tiempo real.
- **Revisión de Permisos Root**: Revisar los comandos que pueden ejecutarse con permisos root para evitar posibles escalaciones de privilegios.

7. Conclusión

El análisis del sistema "Asucar" demostró que mediante la explotación de una vulnerabilidad LFI y la manipulación de permisos sudo, 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 LFI y el ataque de fuerza bruta en XML-RPC.
- Resultados de escaneos de red y análisis de servicios.
- Capturas de pantalla y comandos utilizados durante la explotación y la escalación de privilegios.