Reporte Ejecutivo de Ciberseguridad: Análisis de Vulnerabilidad y Explotación en el Sistema "Where is My Web Shell"

1. Portada

- **Título del Reporte**: Análisis de Vulnerabilidad y Explotación en el Sistema "Where is My Web Shell"
- **Fecha**: 19 de julio de 2024
- **Nombre de la Organización**: [N/A]
- **Autor(es)**: tellmefred

2. Resumen Ejecutivo

Este informe documenta la identificación y explotación de una vulnerabilidad en el sistema "Where is My Web Shell", un entorno práctico de Docker Labs. Se exploraron técnicas avanzadas de fuzzing web para descubrir una web shell oculta en el sistema. Posteriormente, se utilizó la web shell para ejecutar comandos y, finalmente, escalar privilegios hasta obtener acceso root. Se proporcionan recomendaciones para mitigar estas vulnerabilidades y fortalecer la seguridad del sistema.

3. Introducción

- **Contexto**: El sistema "Where is My Web Shell" está diseñado para desafiar a los usuarios a encontrar y explotar una web shell oculta en un servidor web. Este análisis se centró en el reconocimiento, la explotación de la web shell y la escalación de privilegios.
- **Propósito**: Evaluar la seguridad del servidor web, identificar y eliminar cualquier web shell oculta y proponer medidas de mejora en la seguridad.
- **Alcance**: Incluye el reconocimiento de servicios web, la búsqueda de archivos ocultos y la escalación de privilegios mediante la explotación de la web shell.
- **Metodología**: Se utilizó un enfoque sistemático que incluyó escaneos de red, fuzzing de directorios web 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 "Where is My Web Shell" presenta una vulnerabilidad que permite la ejecución remota de comandos a través de una web shell oculta, lo que facilita la escalación de privilegios a root.
- **Sistemas y Datos Críticos**: Servidor web y archivos del sistema.

5. Evaluación de Vulnerabilidades y Explotación

- **Reconocimiento**:
    - **Escaneo de Red**: Se realizó un escaneo con Nmap que identificó el puerto 80 (HTTP) como el único puerto abierto.

    - **Fuzzing Web**: Utilizando la herramienta Gobuster, se realizó un fuzzing que reveló la existencia de un archivo `warning.html` que albergaba una web shell oculta.
- **Explotación**:
    - **Ejecución de Comandos a través de la Web Shell**: Se identificó que la web shell requería un parámetro específico para ejecutar comandos. Se utilizó este parámetro para ejecutar comandos en el servidor, comenzando con el comando `id` para verificar los privilegios del usuario.
    - **Acceso Shell Reversa**: Se estableció una conexión de shell reversa desde la web shell hacia el atacante, permitiendo un acceso interactivo al sistema.
- **Escalada de Privilegios**:
    - **Búsqueda de Archivos Ocultos en /tmp**: Se descubrió un archivo oculto en el directorio `/tmp` llamado `.secret.txt`, que contenía la clave para obtener acceso root.
    - **Acceso Root**: Con la clave obtenida, se obtuvo acceso root al sistema, lo que permitió el control total del mismo.

6. Recomendaciones

- **Eliminación de Web Shells Ocultas**: Realizar auditorías exhaustivas en los servidores para detectar y eliminar cualquier web shell oculta.
- **Fortalecimiento de la Seguridad del Servidor Web**: Implementar medidas de seguridad para prevenir la carga y ejecución de archivos maliciosos en el servidor web.
- **Monitoreo de Actividades Sospechosas**: Implementar sistemas de detección de intrusiones para identificar actividades sospechosas como la creación de archivos ocultos o la ejecución de comandos no autorizados.
- **Capacitación en Seguridad Web**: Entrenar al personal en la identificación y mitigación de vulnerabilidades web, así como en la importancia de mantener sistemas actualizados y seguros.

7. Conclusión

El análisis del sistema "Where is My Web Shell" demostró que la presencia de una web shell oculta puede comprometer gravemente la seguridad del sistema, permitiendo la escalación de privilegios a root. Es crucial implementar las recomendaciones propuestas para mitigar los riesgos y mejorar la postura de seguridad del sistema.

8. Anexos

- Detalles técnicos sobre el fuzzing web y la identificación de la web shell.
- Resultados de escaneos de red y análisis de archivos ocultos.
- Capturas de pantalla y comandos utilizados durante la explotación y la escalación de privilegios.