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

1. Portada

- **Título del Reporte**: Análisis de Vulnerabilidad y Explotación en el Sistema "Summer Vibes"
- **Fecha**: 20 de junio de 2024
- **Nombre de la Organización**: [Nombre de la Organización]
- **Autor(es)**: tellmefred

2. Resumen Ejecutivo

Este informe documenta la identificación y explotación de vulnerabilidades en el sistema "Summer Vibes" de Docker Labs. Se explotaron varias debilidades, incluyendo la identificación de rutas críticas a través de fuzzing web y un ataque de fuerza bruta en un panel de login vulnerable. Estas vulnerabilidades permitieron ejecutar código remoto (RCE) y finalmente escalar privilegios para obtener acceso root en el sistema. Se incluyen recomendaciones para mitigar estas vulnerabilidades.

3. Introducción

- **Contexto**: "Summer Vibes" es una máquina de Docker Labs diseñada para desafiar las habilidades de penetración en un entorno controlado, poniendo énfasis en técnicas como fuzzing web y ataques de fuerza bruta.
- **Propósito**: Evaluar la seguridad del sistema web, identificar puntos críticos de vulnerabilidad, y proponer soluciones para mejorar la seguridad del sistema.
- **Alcance**: El informe cubre desde el reconocimiento inicial hasta la explotación de vulnerabilidades y la escalada de privilegios que llevaron a obtener acceso root.
- **Metodología**: Se utilizó un enfoque que combina técnicas de enumeración, explotación de debilidades en el sistema de autenticación, y la posterior escalada de privilegios utilizando herramientas estándar de penetración.

4. Estado Actual de la Ciberseguridad

- **Resumen de la Postura de Ciberseguridad**: El sistema "Summer Vibes" presentó múltiples vulnerabilidades explotables, principalmente en la seguridad del login y la administración del CMS, lo que permitió comprometer completamente el sistema.
- **Sistemas y Datos Críticos**: Panel de administración web, sistema de gestión de contenido (CMS), y archivos de configuración críticos.

5. Evaluación de Vulnerabilidades y Explotación

- **Reconocimiento**:
    - **Escaneo Inicial**: Se identificaron los puertos 80 (HTTP) y 22 (SSH) abiertos. El puerto 80 alojaba una página web por defecto.

    - **Enumeración de Rutas Web**: Mediante el uso de `Gobuster`, se identificaron directorios ocultos en la aplicación web, incluyendo `/admin`, lo que facilitó la identificación del punto de entrada.
- **Explotación**:
    - **Ataque de Fuerza Bruta**: Se realizó un ataque de fuerza bruta utilizando `Hydra` contra el panel de login, lo que permitió descubrir credenciales débiles y acceder al sistema de gestión de contenido (CMS).
    - **Ejecución de Código Remoto (RCE)**: Al acceder al CMS, se explotó una vulnerabilidad en la versión 2.2.19 de CMS Made Simple para ejecutar comandos en el servidor, logrando cargar una shell web maliciosa.
- **Escalada de Privilegios**:
    - **Explotación de SUID**: Aunque se exploraron varias rutas de escalada utilizando permisos SUID, la escalada de privilegios se logró reutilizando la contraseña descubierta en el CMS para obtener acceso root.

6. Recomendaciones

- **Fortalecimiento de Contraseñas**: Implementar políticas estrictas de contraseñas seguras y cambiar las credenciales predeterminadas de inmediato.
- **Actualización de CMS**: Mantener todas las aplicaciones, especialmente los sistemas de gestión de contenido, actualizadas a la última versión para evitar vulnerabilidades conocidas.
- **Seguridad en la Configuración**: Revisar y asegurar configuraciones críticas del sistema, como permisos SUID, para evitar escaladas de privilegios no autorizadas.
- **Monitorización y Alerta**: Implementar sistemas de detección y alerta temprana para identificar intentos de fuerza bruta y otras actividades maliciosas.

7. Conclusión

La evaluación del sistema "Summer Vibes" demostró que, mediante la explotación de credenciales débiles y vulnerabilidades en el CMS, un atacante puede comprometer completamente la seguridad del sistema. Es crucial aplicar las recomendaciones propuestas para mitigar estos riesgos y fortalecer la postura de seguridad del sistema.

8. Anexos

- Detalles técnicos sobre el ataque de fuerza bruta y la explotación del RCE.
- Resultados de escaneos de red y análisis de directorios web.
- Capturas de pantalla y comandos utilizados durante la explotación y la escalada de privilegios.