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

1. Portada

- **Título del Reporte**: Análisis de Vulnerabilidad y Explotación en el Sistema "BoardLight"
- **Fecha**: 27 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 "BoardLight" de la plataforma Hack The Box. Se descubrieron y explotaron vulnerabilidades que permitieron obtener acceso inicial al sistema a través de credenciales predefinidas y posteriormente escalar privilegios hasta obtener control total (root) sobre el sistema. Se detallan los pasos seguidos y se ofrecen recomendaciones para mitigar estas vulnerabilidades.

3. Introducción

- **Contexto**: "BoardLight" es una máquina de Hack The Box diseñada para probar habilidades en ciberseguridad, específicamente en la identificación y explotación de vulnerabilidades conocidas, así como en la escalada de privilegios.
- **Propósito**: Evaluar la seguridad del sistema web, identificar vulnerabilidades críticas, y proponer medidas correctivas para reducir los riesgos de seguridad.
- **Alcance**: Incluye la enumeración inicial, explotación de vulnerabilidades, y la escalada de privilegios para obtener acceso root al sistema.
- **Metodología**: Se utilizó un enfoque basado en técnicas de enumeración, explotación de vulnerabilidades conocidas, y escalada de privilegios, apoyándose en herramientas comunes de penetración y scripts específicos.

4. Estado Actual de la Ciberseguridad

- **Resumen de la Postura de Ciberseguridad**: El sistema "BoardLight" presentó varias vulnerabilidades que fueron explotadas para comprometer completamente el sistema, incluyendo el uso de credenciales predefinidas y la ejecución de exploits para escalar privilegios.
- **Sistemas y Datos Críticos**: Aplicaciones web (Dolibarr CRM), archivos de configuración sensibles, y el acceso root al sistema.

5. Evaluación de Vulnerabilidades y Explotación

- **Reconocimiento**:
  - **Escaneo Inicial**: Se realizó un escaneo de puertos que reveló los puertos 22 (SSH) y 80 (HTTP) abiertos. Además, se descubrió el dominio `crm.board.htb`.

    - **Enumeración de Servicios**: Se identificó la aplicación Dolibarr CRM en el dominio `crm.board.htb`, con una versión vulnerable documentada.
- **Explotación**:
    - **Credenciales Predefinidas**: Se utilizaron credenciales predefinidas para acceder al sistema, lo que permitió explotar un PoC conocido para la versión específica de Dolibarr.
    - **Shell Reversa**: Se ejecutó un exploit que generó una shell reversa, proporcionando acceso inicial al sistema.
- **Escalada de Privilegios**:
    - **Búsqueda de Configuraciones**: Se encontraron credenciales en un archivo `conf.php`, que permitieron intentar acceso con privilegios más altos.
    - **Explotación de SUID**: Se identificó un binario con permisos SUID que se explotó para escalar los privilegios hasta obtener acceso root.

6. Recomendaciones

- **Gestión de Credenciales**: Cambiar todas las credenciales predeterminadas inmediatamente después de la instalación del software y usar contraseñas seguras.
- **Actualización de Software**: Asegurarse de que todas las aplicaciones, especialmente aquellas accesibles públicamente, estén actualizadas a la última versión para evitar la explotación de vulnerabilidades conocidas.
- **Revisión de Permisos de Archivos**: Auditar y restringir los permisos en archivos de configuración para evitar la exposición de credenciales sensibles.
- **Revisión de Permisos SUID**: Revisar y limitar el uso de binarios con permisos SUID para evitar posibles escaladas de privilegios.

7. Conclusión

La evaluación del sistema "BoardLight" demostró que, mediante la explotación de vulnerabilidades conocidas y la manipulación de permisos SUID, un atacante puede comprometer gravemente la seguridad del sistema. Es fundamental implementar las recomendaciones propuestas para mitigar estos riesgos y fortalecer la postura de seguridad del sistema.

8. Anexos

- Detalles técnicos sobre la explotación de credenciales predefinidas y la escalada de privilegios.
- Resultados de escaneos de red y análisis de servicios.
- Capturas de pantalla y comandos utilizados durante la explotación y la escalada de privilegios.