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

1. Portada

- **Título del Reporte**: Análisis de Vulnerabilidad y Explotación en el Sistema "Uploads"
- **Fecha**: 25 de Mayo de 2024
- **Nombre de la Organización**: [N/A]
- **Autor(es)**: Tellmefred

2. Resumen Ejecutivo

Este informe detalla el proceso de identificación y explotación de una vulnerabilidad en el sistema "Uploads" basado en Docker Labs. Se descubrió una vulnerabilidad de subida de archivos sin filtros de seguridad, lo que permitió la ejecución remota de comandos y escalación de privilegios hasta obtener control completo del sistema. Se proporcionan recomendaciones para mitigar estas vulnerabilidades y fortalecer la seguridad del sistema.

3. Introducción

- **Contexto**: El sistema "Uploads" permite la subida de archivos sin los filtros de seguridad adecuados, lo que puede ser explotado para ejecutar comandos remotos en el servidor.
- **Propósito**: Evaluar la seguridad del sistema y proponer mejoras.
- **Alcance**: Incluye el análisis de la funcionalidad de subida de archivos, identificación de vulnerabilidades, explotación y escalación de privilegios.
- **Metodología**: Se utilizó una combinación de herramientas de escaneo de red, creación de web shells y técnicas de hacking ético.

4. Estado Actual de la Ciberseguridad

- **Resumen de la Postura de Ciberseguridad**: El sistema "Uploads" presenta una grave vulnerabilidad en la funcionalidad de subida de archivos, que permite la ejecución remota de comandos y escalación de privilegios.
- **Sistemas y Datos Críticos**: Servicios web y datos de usuario críticos.

5. Evaluación de Vulnerabilidades y Explotación

- **Reconocimiento**:
  - **Escaneo de Red**: Se realizó un escaneo Nmap para identificar los servicios abiertos.
  - **Análisis del Sitio Web**: Se identificó la funcionalidad de subida de archivos sin filtros de seguridad.
- **Explotación**:
  - **Subida de Web Shell**: Se subió una web shell en PHP para probar la seguridad de la funcionalidad de subida.

- **Ejecución de Comandos**: Se verificó la ejecución de comandos remotos mediante la web shell.
- **Post-Explotación**:
  - Se estableció una reverse shell para obtener acceso remoto completo al sistema.
- **Escalación de Privilegios**:
  - **Análisis de Permisos**: Se utilizó el comando `sudo -l` para identificar permisos de escalación de privilegios.
  - **Elevación a Root**: Se explotó el permiso de ejecución de `/usr/bin/env` para obtener acceso root mediante `sudo env /bin/sh`.

6. Recomendaciones

- **Implementación de Filtros de Seguridad**: Configurar filtros de seguridad para la funcionalidad de subida de archivos.
- **Validación y Sanitización de Archivos**: Implementar validación y sanitización estricta de los archivos subidos.
- **Monitoreo y Auditoría**: Implementar un sistema de monitoreo continuo y auditoría de logs para detectar actividades sospechosas.
- **Seguridad de Contraseñas**: Implementar políticas de contraseñas robustas y almacenamiento seguro de las mismas.
- **Capacitación en Ciberseguridad**: Capacitar al personal en buenas prácticas de seguridad y manejo de incidentes.

7. Conclusión

El análisis del sistema "Uploads" reveló una grave vulnerabilidad en la funcionalidad de subida de archivos que fue explotada para obtener acceso completo al sistema. Se han proporcionado recomendaciones específicas para mejorar la seguridad del sistema y protegerlo contra futuras amenazas.

8. Anexos

- Detalles técnicos de los exploits utilizados.
- Resultados de escaneos de red y análisis de servicios.
- Capturas de pantalla y comandos utilizados durante el proceso de explotación.