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

1. Portada

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

2. Resumen Ejecutivo

Este informe describe la identificación y explotación de vulnerabilidades en la máquina "Editorial" de Hack The Box. La máquina es un reto de nivel fácil, que ilustra cómo las vulnerabilidades de carga de archivos y la falta de control de acceso pueden ser explotadas para obtener acceso inicial y escalar privilegios hasta obtener control total del sistema. Se presentan recomendaciones clave para mitigar estos riesgos en entornos reales.

3. Introducción

- **Contexto**: "Editorial" es una máquina diseñada para desafiar a los profesionales de la ciberseguridad a través de la identificación y explotación de vulnerabilidades en un entorno controlado. La máquina se centra en la explotación de un Servicio Web mal configurado.
- **Propósito**: Evaluar la seguridad del sistema "Editorial", identificar vulnerabilidades críticas y proponer medidas correctivas para mejorar la seguridad del sistema.
- **Alcance**: El análisis cubre el reconocimiento inicial, la explotación de vulnerabilidades de carga de archivos y de Server-Side Request Forgery (SSRF), así como la escalada de privilegios mediante la explotación de scripts inseguros.
- **Metodología**: Se emplearon técnicas de escaneo de red, enumeración de servicios, y explotación de vulnerabilidades conocidas para acceder al sistema y obtener privilegios de root.

4. Estado Actual de la Ciberseguridad

- **Resumen de la Postura de Ciberseguridad**: El sistema "Editorial" presentó múltiples vulnerabilidades explotables, particularmente en la funcionalidad de carga de archivos y en configuraciones inseguras de scripts de desarrollo, lo que permitió a un atacante comprometer completamente el sistema.
- **Sistemas y Datos Críticos**: Servicios web en el puerto 80, configuraciones de scripts de desarrollo y credenciales de usuarios.

5. Evaluación de Vulnerabilidades y Explotación

- **Reconocimiento**:

    - **Escaneo de Puertos**: El escaneo inicial con `nmap` reveló que los puertos 22 (SSH) y 80 (HTTP) estaban abiertos.
    - **Modificación del Archivo Hosts**: Se añadió el dominio del servidor en el archivo `/etc/hosts` para facilitar el acceso a la web en el puerto 80.
- **Explotación**:
    - **Carga de Archivos y SSRF**: Se intentó subir un archivo PHP malicioso, pero la funcionalidad estaba limitada. Se aprovechó una vulnerabilidad de SSRF mediante la manipulación de URLs dentro de la aplicación para acceder a otros servicios internos protegidos, como el puerto 5000, que no fue detectado inicialmente.
    - **Obtención de Credenciales**: A través de la explotación de la API descubierta en el puerto 5000, se lograron extraer credenciales de usuario, permitiendo el acceso al sistema.
- **Escalada de Privilegios**:
    - **Análisis de Repositorio Git**: Se encontró un archivo `.git` en el directorio de un desarrollador, lo que permitió acceder a credenciales adicionales y hacer un pivoting a otro usuario del sistema.
    - **Explotación de Scripts con Permisos Sudo**: Se detectó que el usuario `prod` tenía permisos sudo para ejecutar un script Python vulnerable, permitiendo modificar su funcionamiento para obtener acceso root y extraer la `flag` del usuario root.

6. Recomendaciones

- **Validación y Saneamiento de Entradas**: Implementar validaciones estrictas en la carga de archivos y asegurar que cualquier entrada sea adecuadamente saneada para prevenir vulnerabilidades de SSRF.
- **Protección de APIs Internas**: Restringir el acceso a APIs internas y asegurarse de que no sean accesibles a través de manipulaciones como SSRF.
- **Gestión Segura de Credenciales**: Evitar almacenar credenciales en repositorios públicos o inseguros y asegurar que los scripts no expongan datos sensibles.
- **Revisión de Permisos Sudo**: Limitar los permisos sudo a lo estrictamente necesario y revisar regularmente la configuración de scripts que se ejecutan con estos permisos.

7. Conclusión

La evaluación del sistema "Editorial" demuestra que la falta de validación en la carga de archivos y la configuración insegura de scripts pueden ser explotadas para comprometer completamente un sistema. Es crucial implementar las recomendaciones mencionadas para mitigar estos riesgos y mejorar la postura de seguridad del sistema.

8. Anexos

- Detalles técnicos sobre la explotación de SSRF y el análisis de scripts.
- Resultados de escaneos de red y detalles de la explotación del puerto 5000.
- Capturas de pantalla y comandos utilizados durante la explotación y la escalada de privilegios.