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

1. Portada

- **Título del Reporte**: Análisis de Vulnerabilidad y Explotación en el Sistema "Surveillance"
- **Fecha**: 7 de agosto 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 de vigilancia "Surveillance" basado en la plataforma HTB (Hack The Box). Se descubrió una vulnerabilidad en Craft CMS que permitió acceso no autorizado 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**: La máquina "Surveillance" simula un sistema de vigilancia empresarial con el objetivo de obtener acceso como usuario root. Este informe documenta el proceso de reconocimiento, explotación y post-explotación de vulnerabilidades.
- **Propósito**: Evaluar la seguridad del sistema y proponer mejoras.
- **Alcance**: Incluye el análisis de puertos abiertos, identificación de servicios vulnerables, explotación de vulnerabilidades y escalación de privilegios.
- **Metodología**: Se utilizó una combinación de herramientas de escaneo de red, búsqueda de exploits conocidos y técnicas de hacking ético.

4. Estado Actual de la Ciberseguridad

- **Resumen de la Postura de Ciberseguridad**: El sistema "Surveillance" presenta varias vulnerabilidades explotables que permiten el acceso no autorizado y la escalación de privilegios.
- **Sistemas y Datos Críticos**: Servicios de vigilancia y datos de usuario críticos.

5. Evaluación de Vulnerabilidades y Explotación

- **Reconocimiento**:
  - **Escaneo de Red**: Se identificaron los puertos 22 (SSH) y 80 (HTTP) abiertos.
  - **Análisis del Sitio Web**: Utilizando Wappalyzer, se identificó que el sitio web utilizaba Craft CMS versión 4.4.14.
- **Explotación**:
  - **Craft CMS RCE**: Se utilizó un exploit de ejecución remota de comandos (RCE) para obtener una consola interactiva.

- **Acceso Inicial**: Obtención de acceso al sistema mediante el exploit.
- **Post-Explotación**:
  - Identificación de usuarios y archivos relevantes.
  - Descarga y análisis de un archivo ZIP de backups, obteniendo información de usuarios y hashes de contraseñas.
- **Escalación de Privilegios**:
  - **Acceso SSH**: Se rompió el hash de una contraseña y se utilizó para acceder vía SSH.
  - **Elevación de Privilegios a Root**: Utilizando un exploit en ZoneMinder, se obtuvo acceso root mediante un bypass de seguridad en scripts de sistema.

6. Recomendaciones

- **Actualización de Software**: Actualizar Craft CMS a la última versión para mitigar vulnerabilidades conocidas.
- **Seguridad de Contraseñas**: Implementar políticas de contraseñas robustas y almacenamiento seguro de las mismas.
- **Monitoreo y Auditoría**: Implementar un sistema de monitoreo continuo y auditoría de logs para detectar accesos no autorizados.
- **Segmentación de Red**: Aislar servicios críticos en segmentos de red seguros.
- **Capacitación en Ciberseguridad**: Capacitar al personal en buenas prácticas de seguridad y manejo de incidentes.

7. Conclusión

El análisis del sistema "Surveillance" reveló múltiples vulnerabilidades que fueron explotadas 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.