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

1. Portada

- **Título del Reporte**: Análisis de Vulnerabilidad y Explotación en el Sistema "Fileception"
- **Fecha**: 20 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 "Fileception" de Docker Labs. La máquina "Fileception" está diseñada para demostrar cómo las técnicas de esteganografía pueden ser utilizadas por atacantes para ocultar información dentro de archivos. Se explotaron varios vectores de ataque, incluyendo la recuperación de datos ocultos mediante técnicas esteganográficas, la descodificación de contraseñas y la escalada de privilegios a través de configuraciones inseguras en sudo. El informe proporciona recomendaciones para mitigar estas vulnerabilidades.

3. Introducción

- **Contexto**: "Fileception" es una máquina de Docker Labs creada para explorar las técnicas de esteganografía y la seguridad en la transferencia y almacenamiento de archivos dentro de un entorno de TI.
- **Propósito**: Evaluar la seguridad del sistema "Fileception" mediante la identificación y explotación de técnicas de ocultación de información y escalada de privilegios.
- **Alcance**: El análisis cubre desde el reconocimiento inicial, la extracción de datos ocultos, hasta la escalada de privilegios que llevó al acceso root del sistema.
- **Metodología**: Se empleó un enfoque sistemático que incluyó escaneos de puertos, análisis de archivos FTP, descodificación de contraseñas y escalada de privilegios mediante el uso de sudo.

4. Estado Actual de la Ciberseguridad

- **Resumen de la Postura de Ciberseguridad**: El sistema "Fileception" presentó múltiples vulnerabilidades, incluyendo un servicio FTP con acceso anónimo, datos sensibles ocultos mediante esteganografía y configuraciones inseguras de sudo que facilitaron la obtención de acceso root.
- **Sistemas y Datos Críticos**: Archivos FTP, credenciales de usuario, y la configuración de permisos sudo.

5. Evaluación de Vulnerabilidades y Explotación

- **Reconocimiento**:

    - **Escaneo Inicial**: Se realizó un escaneo con `nmap` que reveló los puertos 21 (FTP), 22 (SSH) y 80 (HTTP) abiertos.
    - **Acceso a FTP**: Se accedió al servicio FTP utilizando el usuario "anonymous", y se descargó un archivo de imagen.
- **Explotación**:
    - **Esteganografía**: Se descubrió que la imagen descargada contenía información oculta, la cual fue extraída utilizando una frase clave encontrada en el código fuente de la página web alojada en el puerto 80.
    - **Decodificación y Acceso**: Tras decodificar el archivo oculto y extraer una contraseña, se logró acceso al sistema mediante SSH con el usuario "peter".
- **Escalada de Privilegios**:
    - **Conversión de Archivos**: Un archivo adicional descubierto en el sistema fue modificado y convertido en un archivo comprimido `.zip`, permitiendo extraer más información confidencial.
    - **Decodificación Base64**: Se descodificó una contraseña utilizando Base64, lo que permitió iniciar sesión como el usuario "octopus".
    - **Configuración Insegura de Sudo**: Se descubrió que el usuario "octopus" tenía permisos para ejecutar todos los comandos como root, lo que permitió escalar privilegios y obtener acceso root utilizando el comando `bash -p`.

6. Recomendaciones

- **Mejorar la Seguridad del Servicio FTP**: Deshabilitar el acceso anónimo y asegurar que todos los archivos sensibles estén protegidos mediante autenticación robusta.
- **Revisar y Auditar Permisos de Sudo**: Restringir los permisos sudo a los mínimos necesarios para evitar escaladas de privilegios no autorizadas.
- **Protección Contra Esteganografía**: Implementar herramientas de detección de esteganografía en archivos críticos y monitorizar el tráfico de archivos sospechosos.
- **Gestión de Contraseñas**: Asegurar que todas las contraseñas sean fuertes y almacenadas de manera segura, evitando su codificación simple como Base64.

7. Conclusión

La evaluación del sistema "Fileception" demostró que, mediante la explotación de configuraciones inseguras y técnicas esteganográficas, un atacante puede comprometer completamente la seguridad del sistema. Es crucial implementar las recomendaciones propuestas para mitigar estos riesgos y mejorar la postura de seguridad general del sistema.

8. Anexos

- Detalles técnicos sobre la extracción de datos ocultos mediante esteganografía.
- Resultados de escaneos de red y análisis de archivos.
- Capturas de pantalla y comandos utilizados durante la explotación y la escalada de privilegios.