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

1. Portada

- **Título del Reporte**: Análisis de Vulnerabilidad y Explotación en el Sistema "Anonymouspingu FTP"
- **Fecha**: 21 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 "Anonymouspingu FTP" de Docker Labs. Se explotaron configuraciones incorrectas en el servicio FTP, lo que permitió la carga de un archivo malicioso que condujo a la obtención de acceso al sistema. A través de técnicas de escalada de privilegios, se logró acceso root. Se detallan los procedimientos utilizados y se ofrecen recomendaciones para mitigar las vulnerabilidades identificadas.

3. Introducción

- **Contexto**: "Anonymouspingu FTP" es una máquina de Docker Labs diseñada para probar la seguridad de configuraciones de FTP y la capacidad de escalar privilegios dentro de un sistema comprometido.
- **Propósito**: Evaluar la seguridad del servicio FTP, identificar configuraciones inseguras, y proponer medidas correctivas para reducir los riesgos.
- **Alcance**: Incluye la enumeración inicial, explotación de vulnerabilidades FTP, y la escalada de privilegios para obtener acceso root al sistema.
- **Metodología**: Se utilizó un enfoque basado en la explotación de configuraciones inseguras de FTP, seguida de la ejecución de técnicas de escalada de privilegios mediante comandos y herramientas comunes.

4. Estado Actual de la Ciberseguridad

- **Resumen de la Postura de Ciberseguridad**: El sistema "Anonymouspingu FTP" presentó una configuración FTP vulnerable que fue explotada para comprometer el sistema, seguido por una escalada de privilegios hasta obtener acceso root.
- **Sistemas y Datos Críticos**: Servicio FTP, archivos sensibles del sistema, y el acceso root.

5. Evaluación de Vulnerabilidades y Explotación

- **Reconocimiento**:
    - **Escaneo Inicial**: Se realizó un escaneo de puertos utilizando `nmap`, que reveló un servicio FTP accesible públicamente en el puerto 21.

    - **Enumeración de Servicios**: Se descubrió que el servicio FTP permitía la carga de archivos sin autenticación.
- **Explotación**:
    - **Carga de Web Shell**: Se subió un archivo PHP malicioso a través del servicio FTP. Este archivo proporcionó una shell web que permitió ejecutar comandos en el servidor.
    - **Acceso Inicial**: La ejecución de la shell web condujo a la ejecución remota de comandos, permitiendo obtener una shell reversa en el sistema.
- **Escalada de Privilegios**:
    - **Usuario "pingu"**: A través del comando `sudo -l`, se identificó que el usuario "pingu" tenía permisos para ejecutar el comando `man` con privilegios elevados, lo que fue explotado para obtener acceso como "pingu".
    - **Usuario "gladys"**: Posteriormente, se utilizó una técnica similar para escalar privilegios al usuario "gladys".
    - **Acceso root**: Finalmente, se explotó el binario `chown` para modificar el archivo `/etc/passwd`, eliminando la contraseña del usuario root, lo que permitió obtener acceso total al sistema.

6. Recomendaciones

- **Configuración Segura de FTP**: Deshabilitar la carga de archivos sin autenticación y restringir el acceso a usuarios autorizados.
- **Actualización de Software**: Asegurar que todos los servicios FTP estén actualizados y configurados con las mejores prácticas de seguridad.
- **Revisión de Permisos de Sudo**: Auditar y restringir los permisos de sudo para evitar escaladas de privilegios no autorizadas.
- **Gestión de Contraseñas**: Implementar políticas de contraseñas seguras y asegurar que los archivos de configuración críticos, como `/etc/passwd`, no sean vulnerables a modificaciones no autorizadas.

7. Conclusión

La evaluación del sistema "Anonymouspingu FTP" demostró que, a través de la explotación de configuraciones FTP inseguras y la manipulación de permisos de sudo, un atacante puede comprometer completamente el sistema. Es crucial implementar las recomendaciones propuestas para mitigar estos riesgos y mejorar la seguridad del sistema.

8. Anexos

- Detalles técnicos sobre la carga de archivos maliciosos 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.