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

1. Portada

- **Título del Reporte**: Análisis de Vulnerabilidad y Explotación en el Sistema "Secret Jenkins"
- **Fecha**: 16 de julio 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 "Secret Jenkins", una máquina práctica de DockerLabs. Se explotó una vulnerabilidad conocida en Jenkins (CVE-2024-23897) y se realizaron ataques de fuerza bruta en el servicio SSH para obtener acceso no autorizado. Posteriormente, se logró una escalación de privilegios mediante la manipulación de un script ejecutado con permisos root. Se proporcionan recomendaciones para mitigar estas vulnerabilidades y fortalecer la seguridad del sistema.

3. Introducción

- **Contexto**: El sistema "Secret Jenkins" expone un Jenkins vulnerable, lo que permitió explotar la vulnerabilidad CVE-2024-23897. Además, se identificó un servicio SSH accesible que permitió ataques de fuerza bruta.
- **Propósito**: Evaluar la seguridad del sistema Jenkins y el servicio SSH, identificar vulnerabilidades, y proponer medidas correctivas para reducir los riesgos de seguridad.
- **Alcance**: Incluye la explotación de Jenkins, ataques de fuerza bruta en SSH, y la escalación de privilegios para obtener acceso root.
- **Metodología**: Se utilizó un enfoque sistemático que incluyó escaneos de red, explotación de Jenkins, ataques de fuerza bruta, y técnicas de post-explotación para obtener acceso privilegiado al sistema.

4. Estado Actual de la Ciberseguridad

- **Resumen de la Postura de Ciberseguridad**: El sistema "Secret Jenkins" presenta vulnerabilidades críticas en Jenkins y en el servicio SSH, que fueron explotadas para comprometer el sistema y escalar privilegios a root.
- **Sistemas y Datos Críticos**: Servicios Jenkins, SSH y archivos del sistema.

5. Evaluación de Vulnerabilidades y Explotación

- **Reconocimiento**:
    - **Escaneo de Red**: Un escaneo de Nmap reveló los puertos 22 (SSH) y 8080 (Jenkins) abiertos.

    - **Identificación de Vulnerabilidad en Jenkins**: Se identificó la versión de Jenkins 2.441 como vulnerable a CVE-2024-23897. Un POC (Prueba de Concepto) permitió obtener acceso a archivos sensibles (`/etc/passwd`).
- **Explotación**:
    - **Ataque de Fuerza Bruta en SSH**: Se utilizó Hydra para realizar un ataque de fuerza bruta en el puerto 22. Se descubrió la contraseña "chocolate" para el usuario "Bobby", lo que permitió el acceso al sistema.
- **Escalada de Privilegios**:
    - **Manipulación de Script con Permisos Root**: Al verificar los permisos sudo, se encontró que el usuario "pinguinito" podía ejecutar Python3. A través de GTFObins, se escaló a este usuario y se manipuló un script ejecutado como root, logrando así acceso total al sistema.

6. Recomendaciones

- **Actualización de Jenkins**: Es crucial actualizar Jenkins a una versión que no esté afectada por la vulnerabilidad CVE-2024-23897.
- **Fortalecimiento de la Seguridad de SSH**: Implementar políticas de contraseñas robustas y limitar los intentos de inicio de sesión fallidos en SSH.
- **Monitoreo de Actividades Sospechosas**: Implementar sistemas de detección de intrusiones para identificar y responder a actividades no autorizadas en tiempo real.
- **Revisión de Permisos Sudo y Scripts Críticos**: Revisar y restringir el uso de sudo para ejecutar comandos peligrosos y scripts con permisos root.

7. Conclusión

El análisis del sistema "Secret Jenkins" demostró que, mediante la explotación de una vulnerabilidad en Jenkins y la manipulación de permisos sudo, un atacante puede comprometer gravemente la seguridad del sistema. Es crucial implementar las recomendaciones propuestas para mitigar estos riesgos y mejorar la postura de seguridad del sistema.

8. Anexos

- Detalles técnicos sobre la explotación de Jenkins y el ataque de fuerza bruta en SSH.
- Resultados de escaneos de red y análisis de servicios.
- Capturas de pantalla y comandos utilizados durante la explotación y la escalación de privilegios.