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

1. Portada

- **Título del Reporte**: Análisis de Vulnerabilidad y Explotación en el Sistema "Strong Jenkins"
- **Fecha**: 10 de abril 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 "Strong Jenkins", un entorno de práctica de DockerLabs. Se explotó una vulnerabilidad en el servicio Jenkins mediante un ataque de fuerza bruta para acceder a la interfaz web y posteriormente ejecutar comandos de forma remota. Finalmente, se logró una escalación de privilegios hasta obtener acceso root al sistema. Se proporcionan recomendaciones para mitigar estas vulnerabilidades y fortalecer la seguridad del sistema.

3. Introducción

- **Contexto**: El sistema "Strong Jenkins" expone un servicio Jenkins, ampliamente utilizado en la automatización de procesos de desarrollo, el cual se configuró con una seguridad insuficiente, haciendo posible la explotación de su autenticación web.
- **Propósito**: Evaluar la seguridad del servicio Jenkins y proponer mejoras para prevenir accesos no autorizados.
- **Alcance**: Incluye el reconocimiento de la infraestructura, la identificación de vulnerabilidades en Jenkins, la explotación mediante fuerza bruta y la escalación de privilegios.
- **Metodología**: Se utilizó Burp Suite para realizar un ataque de fuerza bruta en el formulario de inicio de sesión de Jenkins y luego se explotaron permisos SUID para escalar privilegios.

4. Estado Actual de la Ciberseguridad

- **Resumen de la Postura de Ciberseguridad**: El sistema "Strong Jenkins" presenta vulnerabilidades significativas que permiten el acceso no autorizado y la ejecución remota de comandos a través del servicio Jenkins.
- **Sistemas y Datos Críticos**: Jenkins, interfaz de administración del sistema y permisos de usuario.

5. Evaluación de Vulnerabilidades y Explotación

- **Reconocimiento**:

    - **Escaneo de Red**: Se realizó un escaneo Nmap que identificó el puerto 8080, utilizado por Jenkins.
    - **Análisis del Servicio Jenkins**: Se identificó una versión de Jenkins sin medidas de seguridad adecuadas para proteger la autenticación.
- **Explotación**:
    - **Ataque de Fuerza Bruta**: Se utilizó Burp Suite para realizar un ataque de fuerza bruta sobre el formulario de inicio de sesión de Jenkins.
    - **Acceso a Jenkins**: Después de romper la autenticación, se obtuvo acceso a la consola de Jenkins.
    - **Post-Explotación**:
        - Se usó la consola de Jenkins para ejecutar una reverse shell mediante un script Groovy.
    - **Escalación de Privilegios**:
        - **Análisis de Permisos SUID**: Se encontró que el binario `python3.10` tenía permisos SUID, lo que permitió escalar privilegios a root.
        - **Acceso Root**: Se confirmó el acceso root al ejecutar el comando `sudo python3.10`.

6. Recomendaciones

- **Fortalecimiento de la Configuración de Jenkins**: Configurar medidas de seguridad avanzadas en Jenkins, incluyendo autenticación fuerte y control de acceso basado en roles.
- **Implementación de Medidas Anti-Fuerza Bruta**: Implementar límites en los intentos de autenticación fallidos y utilizar herramientas como Fail2Ban.
- **Revisión de Permisos SUID**: Auditar y eliminar permisos SUID innecesarios o inseguros en binarios críticos.
- **Capacitación en Ciberseguridad**: Capacitar al personal sobre la gestión segura de servicios como Jenkins y la importancia de la revisión continua de configuraciones de seguridad.

7. Conclusión

El análisis del sistema "Strong Jenkins" reveló vulnerabilidades críticas que permitieron la explotación del servicio Jenkins y la escalación de privilegios. Las recomendaciones proporcionadas son cruciales para mitigar los riesgos y mejorar la postura de seguridad del sistema.

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.