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

1. Portada

- **Título del Reporte**: Análisis de Vulnerabilidad y Explotación en el Sistema "Eclipse"
- **Fecha**: 17 de Junio 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 "Eclipse" basado en Dockerlabs. Se descubrió una vulnerabilidad en el servicio Solr que permitió la ejecución remota de comandos (RCE) y, finalmente, la 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 "Eclipse" es un entorno que permite la explotación de vulnerabilidades en servicios web y aplicaciones. Este análisis se centró en la identificación de fallas en los servicios activos en la máquina.
- **Propósito**: Evaluar la seguridad del sistema y proponer medidas correctivas para reducir los riesgos.
- **Alcance**: El análisis incluyó el reconocimiento de servicios activos, la identificación de vulnerabilidades, la explotación de RCE, y la escalación de privilegios.
- **Metodología**: Se utilizó un enfoque basado en la exploración de puertos y la búsqueda de vulnerabilidades conocidas en las versiones específicas de los servicios encontrados.

4. Estado Actual de la Ciberseguridad

- **Resumen de la Postura de Ciberseguridad**: El sistema "Eclipse" presenta una vulnerabilidad crítica en el servicio Solr, que fue explotada para ejecutar comandos en el sistema de forma remota y escalar privilegios hasta obtener acceso root.
- **Sistemas y Datos Críticos**: Servicios web (HTTP y Solr) y permisos de usuario.

5. Evaluación de Vulnerabilidades y Explotación

- **Reconocimiento**:
  - **Escaneo de Red**: Se realizó un escaneo Nmap que identificó los puertos 80 (HTTP) y 8983 (Solr) abiertos.
  - **Análisis del Servicio Solr**: Se detectó una instancia de Apache Solr vulnerable, lo que permitió identificar un exploit de ejecución remota de comandos (RCE).
- **Explotación**:

- **Ejecución Remota de Comandos (RCE)**: Se descargó y ejecutó un exploit RCE en la versión específica de Solr, permitiendo la ejecución de comandos en la máquina víctima.
- **Post-Explotación**:
  - Se estableció una reverse shell para obtener acceso continuo al sistema.
- **Escalación de Privilegios**:
  - **Análisis de Permisos SUID**: Se identificó un binario SUID vulnerable (`dosbox`), que fue explotado para escalar privilegios a root.
  - **Acceso Root**: Se verificó el acceso root mediante el comando `sudo su`, confirmando la obtención de privilegios máximos en el sistema.

6. Recomendaciones

- **Actualización de Software**: Actualizar Apache Solr a la versión más reciente para evitar la explotación de vulnerabilidades conocidas.
- **Revisión de Permisos SUID**: Auditar y eliminar configuraciones de permisos SUID innecesarios o vulnerables en el sistema.
- **Implementación de Medidas de Seguridad**: Fortalecer la configuración de seguridad del sistema, incluyendo firewalls y mecanismos de detección de intrusiones.
- **Capacitación en Ciberseguridad**: Capacitar al personal en la gestión segura de servicios web y en la identificación de vulnerabilidades comunes.

7. Conclusión

El análisis del sistema "Eclipse" reveló vulnerabilidades críticas en el servicio Solr que permitieron la ejecución remota de comandos y la escalación de privilegios. Las recomendaciones proporcionadas son esenciales para mitigar 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.