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

1. Portada

- **Título del Reporte**: Análisis de Vulnerabilidad y Explotación en el Sistema "Trust"
- **Fecha**: 7 de agosto de 2024
- **Nombre de la Organización**: [N/A]
- **Autor(es)**: tellmefred

2. Resumen Ejecutivo

Este informe presenta el análisis de la vulnerabilidad y explotación del sistema "Trust", una máquina virtual creada por DockerLabs. Se identificaron servicios vulnerables en el servidor web, se realizó un ataque de fuerza bruta sobre el servicio SSH, y finalmente se escaló privilegios hasta obtener acceso root. Se proporcionan recomendaciones para mitigar estas vulnerabilidades y fortalecer la seguridad del sistema.

3. Introducción

- **Contexto**: El sistema "Trust" es una máquina virtual que simula un servidor web vulnerable. El objetivo del análisis fue obtener acceso privilegiado al sistema mediante la identificación y explotación de vulnerabilidades.
- **Propósito**: Evaluar la seguridad del servidor web y del servicio SSH del sistema "Trust", y proponer medidas correctivas para reducir los riesgos de seguridad.
- **Alcance**: Incluye el reconocimiento de servicios, la identificación de vulnerabilidades en el servicio SSH, y la escalación de privilegios mediante herramientas de administración.
- **Metodología**: Se utilizó un enfoque combinado de escaneo de puertos, fuzzing de directorios web, fuerza bruta en SSH, y técnicas de escalación de privilegios.

4. Estado Actual de la Ciberseguridad

- **Resumen de la Postura de Ciberseguridad**: El sistema "Trust" presenta vulnerabilidades críticas en el servicio SSH que permiten la obtención de acceso no autorizado mediante ataques de fuerza bruta.
- **Sistemas y Datos Críticos**: Servicios SSH y aplicaciones web vulnerables.

5. Evaluación de Vulnerabilidades y Explotación

- **Reconocimiento**:
  - **Escaneo de Red**: Se realizó un escaneo Nmap que identificó los puertos 22 (SSH) y 80 (HTTP) como abiertos.
  - **Análisis del Sitio Web**: Se utilizaron herramientas de fuzzing web que revelaron la existencia de un archivo oculto (`secret.php`), lo que ayudó a identificar un usuario potencial para el ataque de fuerza bruta.
- **Explotación**:

    - **Ataque de Fuerza Bruta en SSH**: Utilizando el usuario identificado, "mario", se realizó un ataque de fuerza bruta en el servicio SSH, logrando encontrar la contraseña "CHOCOLATE".
    - **Acceso SSH**: Con las credenciales obtenidas, se accedió al sistema a través de SSH como el usuario "mario".
- **Escalada de Privilegios**:
    - **Uso de Sudo**: Se verificaron los permisos sudo para el usuario "mario" y se identificó la posibilidad de ejecutar el editor de texto `vim` con privilegios root.
    - **Escalada Mediante Vim**: Utilizando el comando `sudo vim -c '!/bin/sh'`, se obtuvo acceso root al sistema.

6. Recomendaciones

- **Fortalecimiento de Seguridad en SSH**: Implementar políticas de contraseñas más robustas y limitar los intentos de inicio de sesión fallidos para prevenir ataques de fuerza bruta.
- **Auditoría de Permisos Sudo**: Revisar y restringir los permisos sudo, especialmente para comandos que pueden ser usados para escalación de privilegios.
- **Monitoreo de Actividades Sospechosas**: Implementar sistemas de monitoreo y alerta para detectar y responder a intentos de acceso no autorizados en tiempo real.
- **Capacitación en Ciberseguridad**: Asegurar que el personal esté entrenado en las mejores prácticas de administración de servidores y seguridad informática.

7. Conclusión

El análisis del sistema "Trust" demostró que, mediante la explotación de servicios mal configurados, un atacante puede obtener acceso root. Las recomendaciones proporcionadas son esenciales 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.