Reporte Ejecutivo de Ciberseguridad: Análisis de Vulnerabilidad y Explotación en el Sistema "Break My SSH"

1. Portada

- **Título del Reporte**: Análisis de Vulnerabilidad y Explotación en el Sistema "Break My SSH"
- **Fecha**: 30 de mayo 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 "Break My SSH" basado en DockerLabs. Se exploraron técnicas de fuerza bruta sobre el servicio SSH, lo que permitió obtener acceso root al sistema. Se proporcionan recomendaciones para mitigar estas vulnerabilidades y fortalecer la seguridad del sistema.

3. Introducción

- **Contexto**: El sistema "Break My SSH" permite a los usuarios explorar vulnerabilidades relacionadas con el servicio SSH, en particular las relacionadas con ataques de fuerza bruta.
- **Propósito**: Evaluar la seguridad del servicio SSH en el sistema y proponer mejoras.
- **Alcance**: Incluye el análisis del servicio SSH, identificación de vulnerabilidades, y explotación mediante técnicas de fuerza bruta.
- **Metodología**: Se utilizó un enfoque basado en fuerza bruta para intentar adivinar credenciales y obtener acceso no autorizado.

4. Estado Actual de la Ciberseguridad

- **Resumen de la Postura de Ciberseguridad**: El sistema "Break My SSH" presenta una vulnerabilidad significativa en el servicio SSH que permite la explotación mediante ataques de fuerza bruta.
- **Sistemas y Datos Críticos**: Servicio SSH y credenciales de usuario.

5. Evaluación de Vulnerabilidades y Explotación

- **Reconocimiento**:
  - **Escaneo de Red**: Se realizó un escaneo Nmap que reveló el puerto 22 (SSH) como el único puerto abierto.
  - **Análisis del Servicio SSH**: Se identificó una versión vulnerable del servicio SSH que permite la enumeración de usuarios.
- **Explotación**:
  - **Ataque de Fuerza Bruta**: Se realizó un ataque de fuerza bruta sobre el servicio SSH para adivinar la contraseña del usuario root.

- **Ejecución de Comandos**: Tras el ataque de fuerza bruta exitoso, se obtuvo acceso root directo al sistema.
- **Post-Explotación**:
  - Se solucionó un problema con la identificación del host remoto utilizando `ssh-keygen -R [IP]`.

6. Recomendaciones

- **Fortalecimiento de la Configuración SSH**: Configurar el servicio SSH para limitar los intentos de inicio de sesión fallidos y utilizar autenticación basada en clave pública.
- **Implementación de Medidas Anti-Fuerza Bruta**: Implementar herramientas como Fail2Ban para bloquear intentos de fuerza bruta.
- **Auditoría de Seguridad**: Realizar auditorías regulares del servicio SSH para identificar y mitigar vulnerabilidades.
- **Capacitación en Ciberseguridad**: Capacitar al personal en buenas prácticas de seguridad, incluyendo la gestión segura del servicio SSH.

7. Conclusión

El análisis del sistema "Break My SSH" reveló una vulnerabilidad crítica en el servicio SSH que fue explotada con éxito mediante un ataque de fuerza bruta. Se han proporcionado recomendaciones específicas para mejorar la seguridad del sistema y protegerlo contra futuras amenazas.

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.