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

1. Portada

- **Título del Reporte**: Análisis de Vulnerabilidad y Explotación en el Sistema "Cicada"
- **Fecha**: 20 de Noviembre de 2024
- **Nombre de la Organización**: [N/A]
- **Autor(es)**: tellmefred

2. Resumen Ejecutivo

Este informe documenta la identificación y explotación de vulnerabilidades en la máquina "Cicada" de Hack The Box. Se utilizaron técnicas como la enumeración de recursos SMB, la manipulación de credenciales y la extracción de hashes para comprometer el sistema y obtener acceso root. Este análisis incluye un enfoque sistemático desde el reconocimiento hasta la escalada de privilegios, junto con recomendaciones para mitigar riesgos similares.

3. Introducción

- **Contexto**: "Cicada" es una máquina de Hack The Box orientada a la práctica en la explotación de sistemas Windows mediante técnicas de enumeración de servicios compartidos y análisis de contraseñas.
- **Propósito**: Evaluar la seguridad del sistema "Cicada" identificando vulnerabilidades críticas y aplicando metodologías propias del ethical hacking.
- **Alcance**: Desde el reconocimiento inicial hasta la obtención de acceso root, pasando por la explotación de recursos SMB y escalada de privilegios.
- **Metodología**: Escaneo de red, fuerza bruta sobre usuarios, enumeración LDAP y extracción de hashes.

4. Estado Actual de la Ciberseguridad

- **Resumen de la Postura de Ciberseguridad**: El sistema presentó configuraciones inseguras en recursos compartidos SMB y manejo de contraseñas, lo que permitió la explotación completa.
- **Sistemas y Datos Críticos**: Recursos compartidos (HR, DEV), contraseñas de usuarios (Michael, David) y hashes de administrador.

5. Evaluación de Vulnerabilidades y Explotación

- **Reconocimiento**:
    - **Ping y Escaneo de Red**: Verificación inicial de conectividad y descubrimiento de servicios activos mediante `nmap`.
    - **Enumeración SMB**: Identificación del recurso compartido HR accesible sin autenticación.

- **Explotación**:
  - **Obtención de Contraseñas**: Descarga de archivos desde el recurso HR, identificación de una contraseña, y fuerza bruta para asociarla al usuario "Michael".
  - **Acceso al Recurso DEV**: Con credenciales obtenidas, se accede al recurso DEV y se recupera un archivo de respaldo que contiene otra contraseña, ahora asociada al usuario "David".
  - **Acceso al Usuario Final**: Utilizando las credenciales de "David", se accede al sistema y se captura la `user.txt`.
- **Escalada de Privilegios**:
  - **Extracción de Hashes**: Mediante el uso de herramientas como `pypykatz`, se combinaron claves SAM y SYSTEM para descifrar el hash del administrador.
  - **Pass the Hash**: Se utilizó el hash del administrador para acceder como root y capturar la `root.txt`.

6. Recomendaciones

- **Reforzar la Seguridad de SMB**:
  - Restringir el acceso anónimo y auditar permisos en recursos compartidos.
- **Gestión Segura de Contraseñas**:
  - Implementar políticas de contraseñas robustas y evitar almacenar credenciales en texto claro.
- **Protección de Hashes de Contraseñas**:
  - Asegurar que los archivos SAM y SYSTEM no sean accesibles por usuarios no autorizados.
- **Monitorización y Respuesta**:
  - Implementar sistemas de monitoreo para detectar intentos de explotación de servicios compartidos y manipulación de hashes.

7. Conclusión

El análisis de la máquina "Cicada" evidenció vulnerabilidades críticas en la gestión de recursos compartidos y credenciales, que permitieron comprometer completamente el sistema. La implementación de las recomendaciones propuestas es esencial para mitigar riesgos similares y fortalecer la postura de seguridad del sistema.

8. Anexos

- Detalles técnicos sobre la enumeración SMB y la explotación de hashes.
- Resultados de escaneos de red y análisis de recursos compartidos.
- Capturas de pantalla y comandos utilizados durante el proceso de explotación.