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

1. Portada

- **Título del Reporte**: Análisis de Vulnerabilidad y Explotación en el Sistema "PermX"
- **Fecha**: 21 de agosto 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 "PermX" de Hack The Box. A través de un análisis detallado, se descubrieron y explotaron vulnerabilidades en una plataforma web, lo que permitió obtener acceso inicial al sistema. Posteriormente, se realizó una escalada de privilegios, logrando acceso root y control total sobre la máquina. El informe concluye con recomendaciones para mitigar las vulnerabilidades identificadas.

3. Introducción

- **Contexto**: "PermX" es una máquina de Hack The Box diseñada para desafiar las habilidades de penetración en sistemas a través de la explotación de vulnerabilidades y la escalada de privilegios.
- **Propósito**: Evaluar la seguridad del sistema "PermX", identificar vulnerabilidades críticas y proponer medidas correctivas para fortalecer la seguridad del sistema.
- **Alcance**: Este informe cubre desde el reconocimiento inicial hasta la explotación de vulnerabilidades y la escalada de privilegios, que llevaron a obtener acceso root al sistema.
- **Metodología**: Se emplearon técnicas de reconocimiento, explotación de vulnerabilidades en aplicaciones web, y escalada de privilegios mediante el uso de configuraciones inseguras.

4. Estado Actual de la Ciberseguridad

- **Resumen de la Postura de Ciberseguridad**: El sistema "PermX" presentó varias vulnerabilidades críticas, desde la exposición de servicios web inseguros hasta configuraciones de sudo que permitieron la escalada de privilegios.
- **Sistemas y Datos Críticos**: Servicios web en el puerto 80, configuraciones de scripts, y permisos de sudo.

5. Evaluación de Vulnerabilidades y Explotación

- **Reconocimiento**:
    - **Escaneo de Puertos**: Se identificaron los puertos 22 (SSH) y 80 (HTTP) abiertos. El escaneo reveló que el dominio `permx.htb` estaba asociado a la dirección IP.

    - **Enumeración de Subdominios**: Se descubrió un subdominio `lms.permx.htb`, el cual alojaba la plataforma Chamilo.
- **Explotación**:
    - **Vulnerabilidad en Chamilo**: La plataforma Chamilo en su versión 1 fue identificada como vulnerable a una explotación de ejecución remota de comandos (RCE). Se utilizó un exploit público para obtener acceso inicial al sistema.
    - **Obtención de Acceso Shell**: Mediante la ejecución del exploit, se plantó una web shell, permitiendo la conexión al sistema y la obtención de una shell interactiva.
- **Escalada de Privilegios**:
    - **Reutilización de Credenciales**: Se descubrieron credenciales adicionales en archivos de configuración, las cuales fueron reutilizadas para acceder al sistema a través del puerto 22 (SSH) como el usuario `mtz`.
    - **Explotación de Sudo**: Se identificó que cualquier archivo ubicado en `/home/mtz` podía obtener permisos sudo. Se modificó el archivo `sudoers` para otorgar permisos de root sin contraseña, lo que permitió obtener acceso total al sistema.

6. Recomendaciones

- **Actualización de Software**: Mantener actualizadas todas las aplicaciones web, especialmente las plataformas como Chamilo, para evitar la explotación de vulnerabilidades conocidas.
- **Restricción de Permisos Sudo**: Revisar y limitar los permisos de sudo para evitar la escalada de privilegios no autorizada.
- **Seguridad de Subdominios**: Asegurar que todos los subdominios estén correctamente configurados y protegidos, y que no expongan servicios innecesarios o vulnerables.
- **Gestión Segura de Credenciales**: Evitar la reutilización de contraseñas y asegurar que todas las credenciales estén almacenadas de forma segura.

7. Conclusión

La evaluación del sistema "PermX" demostró que la explotación de vulnerabilidades web, junto con configuraciones inseguras de permisos, puede llevar a la completa toma de control del sistema. Es esencial implementar las recomendaciones mencionadas para mitigar estos riesgos y mejorar la seguridad general del sistema.

8. Anexos

- Detalles técnicos sobre la explotación de Chamilo y la escalada de privilegios.
- Resultados de escaneos de red y análisis de subdominios.
- Capturas de pantalla y comandos utilizados durante la explotación y la escalada de privilegios.