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

1. Portada

- **Título del Reporte**: Análisis de Vulnerabilidad y Explotación en el Sistema "CapyPenguin"
- **Fecha**: 20 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 el sistema "CapyPenguin" de DockerLabs. La máquina se enfoca en la explotación de un servicio MySQL vulnerable mediante técnicas de fuerza bruta, lo que permitió obtener acceso a la base de datos y, finalmente, escalar privilegios para obtener acceso root al sistema. Se proporcionan recomendaciones para mitigar las vulnerabilidades identificadas.

3. Introducción

- **Contexto**: "CapyPenguin" es una máquina diseñada por DockerLabs para poner a prueba habilidades de ciberseguridad, específicamente en la explotación de bases de datos MySQL y la escalada de privilegios en un entorno controlado.
- **Propósito**: Evaluar la seguridad del sistema "CapyPenguin", identificar vulnerabilidades críticas y proponer medidas correctivas para mejorar la seguridad del sistema.
- **Alcance**: Este informe cubre desde el reconocimiento inicial hasta la explotación de vulnerabilidades en MySQL y la escalada de privilegios que llevaron a obtener acceso root al sistema.
- **Metodología**: Se utilizaron técnicas de escaneo de puertos, fuerza bruta contra MySQL y explotación de configuraciones inseguras de sudo para obtener acceso privilegiado al sistema.

4. Estado Actual de la Ciberseguridad

- **Resumen de la Postura de Ciberseguridad**: El sistema "CapyPenguin" presentó varias vulnerabilidades críticas, incluyendo la exposición de un servicio MySQL vulnerable a ataques de fuerza bruta y la configuración insegura de sudo, que permitieron comprometer completamente el sistema.
- **Sistemas y Datos Críticos**: Servicio MySQL, credenciales de usuario y permisos de sudo.

5. Evaluación de Vulnerabilidades y Explotación

- **Reconocimiento**:

    - **Escaneo de Puertos**: Se realizó un escaneo inicial con `nmap`, que reveló los puertos 22 (SSH), 80 (HTTP) y 3306 (MySQL) abiertos.
    - **Enumeración de Servicios**: A través de la exploración del puerto 80, se descubrió información sobre un usuario (`capybarauser`) y un comando (`tac`) en el código fuente del sitio web.
- **Explotación**:
    - **Ataque de Fuerza Bruta a MySQL**: Utilizando `Medusa`, se realizó un ataque de fuerza bruta exitoso contra el servicio MySQL, lo que permitió obtener la contraseña para el usuario `capybarauser`.
    - **Acceso a MySQL**: Con las credenciales obtenidas, se accedió a la base de datos MySQL, lo que permitió extraer información de la base de datos `pinguinasio_db`, incluyendo credenciales adicionales.
- **Escalada de Privilegios**:
    - **Explotación de Sudo en Nano**: Se descubrió que el binario `nano` tenía permisos sudo, lo que permitió escalar privilegios y obtener acceso root al sistema mediante la explotación de vulnerabilidades conocidas en `nano`.

6. Recomendaciones

- **Fortalecimiento de la Seguridad de MySQL**: Implementar políticas de contraseñas más seguras y limitar los intentos de inicio de sesión fallidos para proteger contra ataques de fuerza bruta.
- **Revisión de Permisos de Sudo**: Auditar y restringir los permisos de sudo para evitar la explotación de binarios con configuraciones inseguras como `nano`.
- **Monitorización y Alerta**: Implementar sistemas de detección de intrusiones (IDS) para identificar y alertar sobre intentos de acceso no autorizado, especialmente en servicios críticos como MySQL.
- **Revisión y Seguridad del Código Fuente**: Evitar la exposición de información sensible en el código fuente de páginas web accesibles públicamente.

7. Conclusión

La evaluación del sistema "CapyPenguin" demostró que la explotación de un servicio MySQL mal configurado y la utilización de configuraciones inseguras de sudo pueden comprometer seriamente la seguridad del sistema. Es esencial implementar las recomendaciones propuestas para mitigar estos riesgos y mejorar la seguridad general del sistema.

8. Anexos

- Detalles técnicos sobre el ataque de fuerza bruta a MySQL y la escalada de privilegios mediante `nano`.
- Resultados de escaneos de red y análisis de servicios.
- Capturas de pantalla y comandos utilizados durante la explotación y la escalada de privilegios.