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

1. Portada

- **Título del Reporte**: Análisis de Vulnerabilidad y Explotación en el Sistema "Sightless"
- **Fecha**: 26 de septiembre de 2024
- **Nombre de la Organización**: [N/A]
- **Autor(es)**: tellmefred

2. Resumen Ejecutivo

Este informe describe la identificación y explotación de vulnerabilidades en el sistema "Sightless" de Hack The Box. A través de técnicas como la explotación de un servicio SQLpad y la escalada de privilegios mediante el uso de herramientas de port forwarding, se logró comprometer completamente el sistema y obtener acceso root. El análisis concluye con recomendaciones específicas para mitigar los riesgos identificados.

3. Introducción

- **Contexto**: "Sightless" es una máquina de Hack The Box diseñada para explorar vulnerabilidades en servicios públicos y utilizar técnicas como port forwarding y explotación de vulnerabilidades en contenedores Docker.
- **Propósito**: Evaluar la seguridad del sistema "Sightless" mediante la identificación de vulnerabilidades críticas y técnicas de escalada de privilegios.
- **Alcance**: El análisis cubre desde el reconocimiento inicial, la explotación de SQLpad, hasta la escalada de privilegios mediante la utilización de port forwarding.
- **Metodología**: Se emplearon técnicas de escaneo de red, explotación de servicios vulnerables, uso de herramientas de descifrado de contraseñas y escalada de privilegios mediante la explotación de puertos locales.

4. Estado Actual de la Ciberseguridad

- **Resumen de la Postura de Ciberseguridad**: El sistema "Sightless" presentó múltiples vulnerabilidades explotables, incluyendo la exposición de un servicio SQLpad vulnerable y la reutilización de contraseñas, lo que facilitó la explotación y el acceso no autorizado.
- **Sistemas y Datos Críticos**: Servicios SQLpad, credenciales de usuario y configuración de Docker.

5. Evaluación de Vulnerabilidades y Explotación

- **Reconocimiento**:
    - **Escaneo de Puertos**: Se realizó un escaneo inicial con `nmap`, que reveló una redirección en el puerto 80 a `sightless.htb`, y un servicio SQLpad en un subdominio.

    - **Identificación de Servicio Vulnerable**: SQLpad corriendo en el subdominio fue identificado como vulnerable a una ejecución remota de comandos (RCE).
- **Explotación**:
    - **Reverse Shell**: Al ejecutar un comando en SQLpad, se obtuvo una shell reversa. Sin embargo, se detectó que la shell se ejecutaba dentro de un contenedor Docker.
    - **Hash de Michael**: Se extrajo el archivo `/etc/shadow` desde el contenedor y se descifró el hash del usuario Michael utilizando la herramienta John the Ripper, lo que permitió obtener su contraseña.
- **Escalada de Privilegios**:
    - **Port Forwarding**: Utilizando port forwarding, se accedió a servicios adicionales corriendo en la máquina local, incluyendo Froxlor.
    - **Captura de Credenciales Admin**: Se utilizó una herramienta de desarrollo en Chrome para interceptar y capturar la contraseña y el usuario `admin` desde el tráfico web.
    - **Modificación de PHP-FPM**: Se modificaron procesos en PHP-FPM para capturar la clave SSH RSA del usuario root, lo que permitió obtener acceso root completo al sistema.

6. Recomendaciones

- **Actualización y Protección de Servicios Públicos**: Actualizar SQLpad a una versión más segura y configurar adecuadamente los servicios públicos para evitar la exposición de vulnerabilidades críticas.
- **Revisión de Configuración de Contenedores Docker**: Implementar mejores prácticas de seguridad en Docker para evitar que los contenedores puedan ser utilizados como puntos de entrada para la escalada de privilegios.
- **Gestión Segura de Contraseñas**: Evitar la reutilización de contraseñas y asegurar que las credenciales no sean expuestas en archivos accesibles o en tráfico no cifrado.
- **Monitorización y Alerta**: Implementar sistemas de detección de intrusiones (IDS) para identificar y alertar sobre actividades sospechosas, como el uso de herramientas de port forwarding o la modificación de procesos PHP-FPM.

7. Conclusión

La evaluación del sistema "Sightless" demostró que la explotación de un servicio vulnerable como SQLpad, junto con la reutilización de contraseñas y la configuración insegura de contenedores, pueden comprometer completamente un sistema. Se recomienda aplicar las medidas correctivas propuestas para mitigar estos riesgos y mejorar la postura de seguridad general del sistema.

8. Anexos

- Detalles técnicos sobre la explotación de SQLpad y la escalada de privilegios mediante port forwarding.
- Resultados de escaneos de red y análisis de servicios.
- Capturas de pantalla y comandos utilizados durante la explotación y la escalada de privilegios