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

1. Portada

- **Título del Reporte**: Análisis de Vulnerabilidad y Explotación en el Sistema "Chemistry"
- **Fecha**: 12 de diciembre de 2024
- **Nombre de la Organización**: (N/A) - Proyecto Educativo
- **Autor(es)**: tellmefred

2. Resumen Ejecutivo

Este informe describe el análisis y explotación de la máquina "Chemistry" de Hack The Box, diseñada para evaluar habilidades en ciberseguridad. A través de técnicas de reconocimiento, explotación de servicios vulnerables y escalada de privilegios, se logró comprometer el sistema, obteniendo acceso root. Este ejercicio refuerza conceptos clave en ethical hacking y seguridad de sistemas.

3. Introducción

- **Contexto**: "Chemistry" es una máquina diseñada para desafiar habilidades técnicas en un entorno seguro. Permite a los profesionales explorar vulnerabilidades comunes en servicios y configuraciones.
- **Propósito**: Evaluar la seguridad del sistema mediante la identificación y explotación de vulnerabilidades críticas.
- **Alcance**: Incluye reconocimiento inicial, explotación de servicios vulnerables y escalada de privilegios hasta obtener acceso root.
- **Metodología**: Uso de herramientas de escaneo, explotación de vulnerabilidades mediante pruebas de concepto (PoC) y análisis de configuraciones locales.

4. Estado Actual de la Ciberseguridad

- **Resumen de la Postura de Ciberseguridad**: Se identificaron varias vulnerabilidades críticas, incluyendo exposición de servicios web, contraseñas débiles y configuraciones locales inseguras.
- **Sistemas y Datos Críticos**: Servicios web en el puerto 5000, base de datos expuesta y claves SSH.

5. Evaluación de Vulnerabilidades y Explotación

- **Reconocimiento**:
    - Se utilizó un escaneo `ping` y `nmap` para identificar el puerto 5000 abierto, que alojaba un dashboard con un archivo `.cif`.
    - El archivo y su ejemplo sugerían una posible vulnerabilidad que fue verificada mediante un PoC.

- **Explotación**:
  - Se explotó la vulnerabilidad para ejecutar una shell reversa y obtener acceso inicial al sistema.
  - Mediante herramientas de análisis como `linpeas`, se identificó una base de datos expuesta que contenía un hash. El hash fue descifrado para obtener la contraseña del usuario.
  - Se obtuvo la bandera `USER.txt` con estas credenciales.
- **Escalada de Privilegios**:
  - Se detectó un servicio de monitoreo en un puerto local. Usando port forwarding, se accedió al servicio desde la máquina atacante.
  - El servicio presentó una vulnerabilidad de Inclusión Local de Archivos (LFI), que permitió leer el archivo `id_rsa` del usuario root.
  - Con la clave SSH recuperada, se logró acceso root al sistema, obteniendo la bandera `ROOT.txt`.

6. Recomendaciones

- **Seguridad de Servicios Web**:
  - Implementar medidas de autenticación y autorización para proteger dashboards y archivos sensibles.
- **Gestión de Contraseñas**:
  - Evitar el uso de contraseñas débiles y almacenar hashes utilizando algoritmos robustos.
- **Monitorización y Alerta**:
  - Implementar sistemas que detecten intentos de explotación de vulnerabilidades conocidas como LFI.
- **Segmentación de Servicios**:
  - Asegurar que los servicios críticos solo sean accesibles desde redes internas o mediante VPN.

7. Conclusión

El análisis de la máquina "Chemistry" evidenció vulnerabilidades críticas en la configuración de servicios y el manejo de credenciales, que permitieron comprometer completamente el sistema. La implementación de las recomendaciones propuestas es esencial para mitigar riesgos similares y fortalecer la seguridad del sistema.

8. Anexos

- Detalles técnicos sobre la explotación de PoC y LFI.
- Resultados de escaneos de red y configuraciones detectadas.
- Capturas de pantalla y comandos utilizados durante la explotación y la escalada de privilegios.