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

1. Portada

- **Título del Reporte**: Análisis de Vulnerabilidad y Explotación en el Sistema "**Alert**"
- **Fecha**: 03 de Diciembre del 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 "Alert" de Hack The Box. A través de técnicas como la manipulación de peticiones HTTP, el descifrado de contraseñas y el uso de una reverse shell, se logró comprometer el sistema y obtener acceso root. Este análisis proporciona una visión detallada del enfoque utilizado y recomendaciones para mitigar riesgos similares.

3. Introducción

- **Contexto**: "Alert" es una máquina de Hack The Box diseñada para evaluar habilidades clave en el análisis de servicios web y la escalada de privilegios.
- **Propósito**: Evaluar la seguridad del sistema mediante la identificación de vulnerabilidades explotables y la implementación de técnicas avanzadas de penetración.
- **Alcance**: El análisis abarca desde el reconocimiento inicial hasta la escalada de privilegios para obtener acceso root.
- **Metodología**: Escaneo de red con Nmap, manipulación de peticiones HTTP, explotación de contraseñas y escalada de privilegios mediante puertos abiertos.

4. Estado Actual de la Ciberseguridad

- **Resumen de la Postura de Ciberseguridad**: El sistema presentó vulnerabilidades en su manejo de peticiones HTTP y en la exposición de contraseñas, lo que permitió la explotación y el acceso no autorizado.
- **Sistemas y Datos Críticos**: Servicio web con un visualizador `.md`, credenciales de usuario y configuraciones del sistema.

5. Evaluación de Vulnerabilidades y Explotación

- **Reconocimiento**:
  - **Escaneo Inicial**: Se utilizó `nmap` para identificar servicios activos. Fue necesario añadir el dominio al archivo `/etc/hosts` para acceder al sistema.
  - **Identificación de Visualizador `.md`**: Se detectó un visualizador web que permitió el envío de un payload malicioso.

- **Explotación**:
  - **Envío de Payload**: Se utilizó un enlace codificado para explotar el sistema, logrando obtener el archivo `/etc/passwd` y una contraseña en texto plano.
  - **Acceso por SSH**: Con las credenciales obtenidas, se accedió al sistema y se capturó la bandera `user.txt`.
- **Escalada de Privilegios**:
  - **Exploración de Puertos**: Se identificó el puerto 8080, lo que permitió redirigir el tráfico al localhost y ejecutar una reverse shell.
  - **Acceso Root**: Finalmente, se capturó la bandera `root.txt` al obtener privilegios root en el sistema.

6. Recomendaciones

- **Validación de Entradas y Seguridad Web**:
  - Implementar validaciones estrictas para las peticiones HTTP y evitar la ejecución de comandos maliciosos en el servidor.
- **Gestión Segura de Contraseñas**:
  - Proteger contraseñas y hashes mediante el uso de cifrado seguro y almacenarlas en ubicaciones no accesibles desde aplicaciones web.
- **Monitoreo y Respuesta**:
  - Implementar herramientas de monitoreo para detectar actividad anómala en servicios web y posibles intentos de explotación.
- **Segmentación de Puertos**:
  - Restringir el acceso a puertos sensibles y asegurar servicios internos con autenticación fuerte.

7. Conclusión

La evaluación del sistema "Alert" muestra que una mala gestión de entradas web y la exposición de contraseñas son riesgos críticos. Es esencial implementar las recomendaciones propuestas para proteger el sistema contra ataques similares.

8. Anexos

- Detalles técnicos sobre la explotación de peticiones HTTP y el uso de reverse shell.
- Resultados de escaneos de red y análisis de servicios.
- Capturas de pantalla y comandos utilizados durante la explotación y la escalada de privilegios.