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

1. Portada

- **Título del Reporte**: Análisis de Vulnerabilidad y Explotación en el Sistema "Instant"
- **Fecha**: 25 de noviembre de 2024
- **Nombre de la Organización**: [N/A]
- **Autor(es)**: tellmefred

2. Resumen Ejecutivo

Este informe documenta el proceso de ataque y explotación del sistema "Instant" de Hack The Box. A través de la identificación de múltiples dominios, la extracción de claves desde un archivo APK y el descifrado de archivos de sesión, se logró comprometer el sistema y obtener acceso root. Se presentan recomendaciones para mitigar los riesgos detectados.

3. Introducción

- **Contexto**: "Instant" es una máquina diseñada para desafiar habilidades de ciberseguridad, con un enfoque en la explotación de aplicaciones web y análisis de archivos móviles (APK).
- **Propósito**: Evaluar la seguridad del sistema mediante la identificación de vulnerabilidades críticas y su explotación.
- **Alcance**: Desde el reconocimiento inicial hasta la escalada de privilegios y la obtención de acceso root.
- **Metodología**: Escaneo de red, análisis de aplicaciones móviles, explotación de APIs y descifrado de archivos de sesión.

4. Estado Actual de la Ciberseguridad

- **Resumen de la Postura de Ciberseguridad**: Se identificaron múltiples debilidades en la configuración del sistema, incluyendo claves incrustadas en un APK, APIs vulnerables y almacenamiento inseguro de datos de sesión.
- **Sistemas y Datos Críticos**: Clave SSH `id_rsa`, archivos de sesión Solar-Putty y credenciales root.

5. Evaluación de Vulnerabilidades y Explotación

- **Reconocimiento**:
  - Escaneo de puertos reveló servicios web y APIs activos.
  - Descarga y análisis de un APK que contenía claves de autenticación y dominios adicionales.
- **Explotación**:
  - Uso de claves para autenticarse en la API y leer archivos críticos.
  - Obtención de la clave SSH privada `id_rsa` y acceso al sistema vía SSH.

- **Escalada de Privilegios**:
    - Descifrado de hashes y extracción de credenciales desde un archivo de sesión Solar-Putty.
    - Uso de estas credenciales para obtener acceso root.

6. Recomendaciones

- **Seguridad en el Desarrollo de Aplicaciones**:
    - Evitar incluir claves o datos sensibles en archivos APK.
- **Protección de APIs**:
    - Implementar autenticación fuerte y validar todas las solicitudes.
- **Gestión Segura de Credenciales**:
    - Utilizar cifrado robusto y proteger archivos de sesión con contraseñas fuertes.
- **Monitorización y Respuesta**:
    - Implementar sistemas de detección de intrusiones para identificar accesos no autorizados.

7. Conclusión

La evaluación de "Instant" muestra que vulnerabilidades en el manejo de datos sensibles y configuraciones inseguras pueden comprometer la seguridad del sistema. Las recomendaciones propuestas son fundamentales para mejorar la postura de seguridad.

8. Anexos

- Detalles técnicos sobre el análisis del APK y la explotación de APIs.
- Resultados de escaneos de red y análisis de servicios.
- Capturas de pantalla y comandos utilizados durante la explotación.