Asniff

Innovación en Análisis y Seguridad de Dispositivos Cercanos

Github del proyecto:

https://github.com/pablo-972/Asniff

Componentes del equipo:

Pablo Miguel Aguilar Blanco

Antonio Salvador Gámez Zafra

En un mundo cada vez más interconectado, garantizar la seguridad y el control sobre los dispositivos cercanos es una necesidad. **Asniff** se presenta como la solución definitiva para identificar, analizar y asegurar dispositivos cercanos mediante tecnologías de vanguardia.

¿Qué es Asniff?

Asniff es una innovadora aplicación móvil diseñada para escanear dispositivos cercanos utilizando WiFi y Bluetooth. Esta herramienta no solo detecta dispositivos, sino que permite a los usuarios recopilar, gestionar y analizar información clave en tiempo real.

Características clave:

1. **Detección Avanzada:**
    1.1. Escanea redes WiFi y conexiones Bluetooth cercanas.
    1.2. Identifica dispositivos de manera rápida y precisa.
2. **Gestión de Dispositivos:**
    2.1. Opción para almacenar dispositivos encontrados en una base de datos remota, manteniendo un registro accesible y seguro.
3. **Información Detallada:**
    3.1. Obtén información relevante del dispositivo utilizando su dirección MAC, proporcionando datos valiosos para un análisis más profundo, mediante un api MACVendor.
4. **Integración con la API NVD:**
    4.1. Conexión directa a la **National Vulnerability Database (NVD)** para obtener información actualizada sobre posibles vulnerabilidades de los dispositivos detectados.

¿Por qué elegir Asniff?

1. **Seguridad Proactiva:** Permite a empresas y usuarios particulares identificar posibles riesgos antes de que se conviertan en amenazas.
2. **Eficiencia:** La interfaz intuitiva y las funcionalidades automatizadas optimizan el proceso de escaneo y análisis.

3. **Conectividad Global:** Con la integración de bases de datos remotas y la API NVD, Asniff opera como una herramienta de seguridad global en tiempo real.

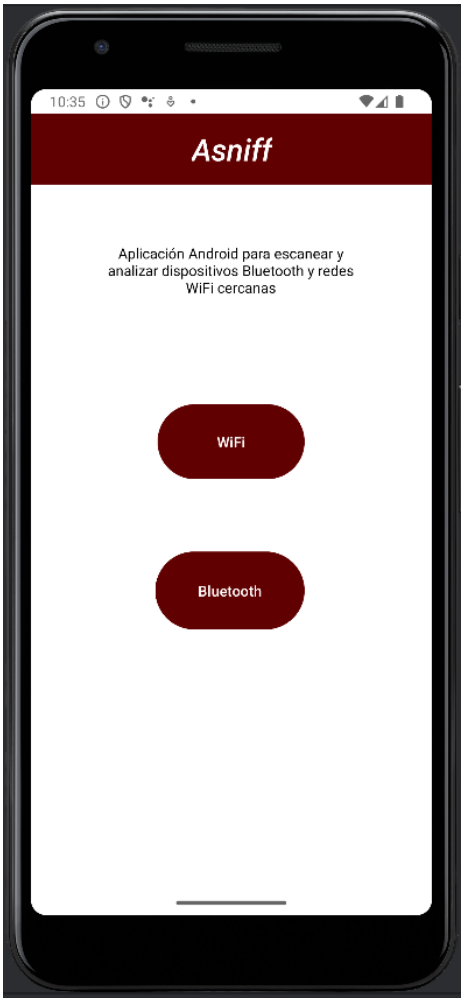
Aplicaciones de Asniff:

1. Auditorías de seguridad y análisis de vulnerabilidades en redes corporativas.
2. Evaluación de dispositivos desconocidos en ubicaciones públicas o privadas.
3. Investigaciones en ciberseguridad para profesionales y entusiastas de la tecnología.

Manual de Usuario

Ventana Principal

Desde esta pantalla, puedes seleccionar entre dos opciones principales: Scanner WiFi o Scanner Bluetooth.



Scanner

Puedes visualizar la red Wifi a la que estás conectado y detectar dispositivos Wifi cercanos. Si seleccionas un dispositivo se almacena en la base de datos.

Si seleccionas el botón Ver Registros, accederás a la lista de dispositivos previamente guardados.

Registros

Aquí encontrarás un listado con todos los dispositivos registrados:

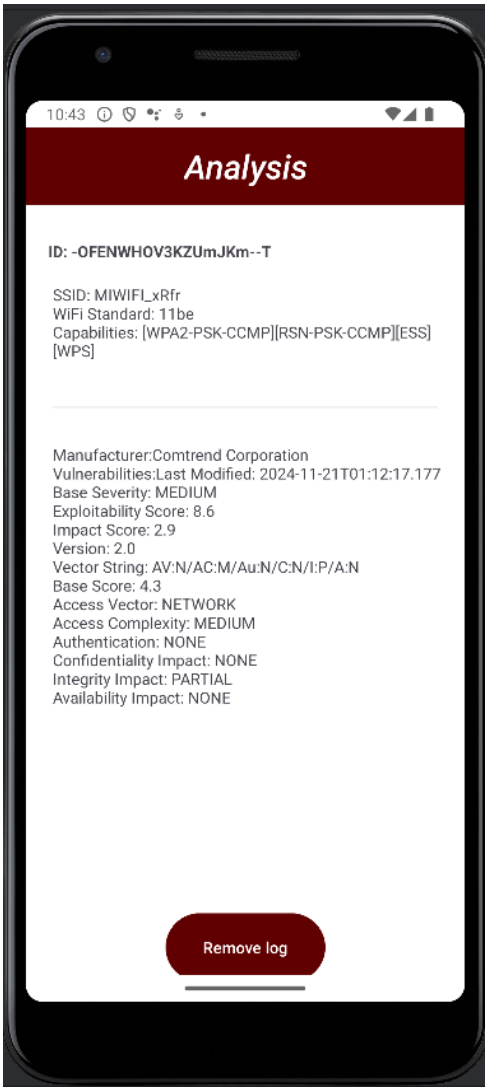
- Al seleccionar una entrada específica, puedes analizarla.

Análisis

Esta funcionalidad permite:

Consultar la información almacenada del dispositivo seleccionado.

Acceder a datos adicionales obtenidos desde la base de datos NVD (National Vulnerability Database).



El análisis realiza dos consultas principales:

1. **Consulta de información del dispositivo:** Realiza una llamada a una API utilizando la dirección MAC identificada para obtener datos adicionales sobre el dispositivo.

2. **Consulta a la API de la base de datos NVD:** Con la información obtenida en la primera consulta, se accede a la API de la National Vulnerability Database, gestionada por el gobierno de los Estados Unidos, que contiene detalles sobre todas las vulnerabilidades detectadas en dispositivos de hardware.

Detalles explicados a continuación.

Descripción datos NVD:

Sección Superior: Información General

1. **ID:** 0FETfi8KwiDpTLGdi91
   1.1. Identificador único asignado al dispositivo escaneado.
2. **SSID:** MOVISTAR_PLUS_9DC0
   2.1. Nombre de la red Wifi a la que pertenece el dispositivo.
3. **WiFi Standard:** 11be
   3.1. Especifica la norma Wifi que utiliza el dispositivo.
4. **Capabilities:** [WPA2-PSK-CCMP][RSN-PSK-CCMP][ESS][WPS]
   4.1. Indica las capacidades de seguridad y autenticación de la red:
      4.1.1. **WPA2-PSK-CCMP:** Modo de seguridad WPA2 con cifrado CCMP.
      4.1.2. **RSN-PSK-CCMP:** Red segura compatible con WPA2-PSK y CCMP.
      4.1.3. **ESS:** Sistema de red extendido (Extended Service Set).
      4.1.4. **WPS:** Configuración protegida WiFi (WiFi Protected Setup).
5. **Manufacturer:** ASKEY COMPUTER CORP
   5.1. Fabricante del dispositivo detectado.
6. **Vulnerabilities:**
   6.1. **Last Modified:** 2024-11-21T04:22:57.283
      6.1.1. Última actualización de la base de datos de vulnerabilidades.
   6.2. Base Severity: HIGH
      6.2.1. Nivel de severidad clasificado como bajo, medio o alto.
   6.3. Exploitability Score: 10.0

6.3.1. Puntuación (0-10) que indica la probabilidad de ser explotado.

6.4. **Impact Score:** 10.0

6.4.1. Nivel de impacto (0-10) clasificado como inofensivo o crítico.

6.5. **Version:** 2.0

6.5.1. Versión del reporte o estándar utilizado para clasificar las vulnerabilidades.

Detalles Técnicos:

1. **Vector String:**

1.1. AV:N/AC:L/Au:N/C:C/I:C/A:C

1.2. Código que describe el vector de ataque:

1.2.1. **AV:N:** Ataque remoto posible a través de la red.

1.2.2. **AC:L:** Complejidad baja para realizar el ataque.

1.2.3. **Au:N:** No se requiere autenticación para explotar la vulnerabilidad.

1.2.4. C:C, I:C, A:C: Impacto completo en la Confidencialidad (C), Integridad (I) y Disponibilidad (A) del sistema afectado.

2. **Base Score:** 10.0

2.1. Puntuación general máxima, indica un riesgo crítico.

3. **Access Vector:** NETWORK

3.1. Ataque se realiza a través de la red.

4. **Access Complexity:** LOW

4.1. Nivel bajo de dificultad para explotar la vulnerabilidad.

5. **Authentication:** NONE

5.1. No se requiere autenticación para acceder.

6. **Confidentiality Impact:** COMPLETE

6.1. Impacto total en la confidencialidad.

7. **Integrity Impact:** COMPLETE

7.1. Impacto total en la integridad.

8. **Availability Impact:** COMPLETE

8.1. Impacto total en la disponibilidad.

Adicionalmente es posible eliminar el registro mediante el botón situado en el inferior de la pantalla.

Lo explicado anteriormente para el caso del WiFi sería aplicable de igual manera al caso del Bluetooth.