Herramienta de Inventariado y Monitoreo de Red

Esta aplicación permite escanear dispositivos en una red local, detectar sus servicios activos, analizar riesgos de seguridad y monitorear la red en tiempo real. Cuenta con una interfaz gráfica intuitiva que facilita la visualización y gestión de los resultados, incluyendo representación de topología de red y generación de informes detallados.

Características

Escaneo y Detección

- **Escaneo de red**: Detecta dispositivos en un rango de red especificado con optimización para redes grandes.
- **Identificación de servicios**: Detecta servicios como HTTP, HTTPS, SSH, RDP, SNMP, WMI y muchos más.
- **Recopilación de información**: Obtiene IP, hostname, MAC, fabricante, sistema operativo, hardware y más.
- **Detección automática de red**: Identifica automáticamente la red local para facilitar el escaneo.

Análisis de Seguridad

- **Auditoría de seguridad**: Detecta puertos y servicios inseguros como Telnet, FTP sin cifrar, SMB v1, etc.
- **Análisis de riesgos**: Sistema de puntuación tipo semáforo (verde, naranja, rojo) para clasificar dispositivos.
- **Recomendaciones de seguridad**: Genera automáticamente recomendaciones específicas para cada vulnerabilidad.
- **Informes de seguridad**: Crea informes detallados con estadísticas y recomendaciones globales.

Monitoreo en Tiempo Real

- **Detección de nuevos dispositivos**: Monitorea la red para detectar dispositivos que se conectan.
- **Sistema de alertas**: Notificaciones configurables cuando se detectan eventos importantes.
- **Reglas personalizables**: Permite definir condiciones específicas para generar alertas.
- **Múltiples canales de notificación**: Notificaciones en la aplicación, logs y soporte para canales personalizados.

Visualización y Topología

- **Mapa de red interactivo**: Visualización gráfica de la red con nodos y conexiones.
- **Clasificación automática**: Identifica automáticamente el tipo de dispositivo (router, switch, servidor, etc.).
- **Interfaz interactiva**: Zoom, arrastre y menú contextual para cada nodo del mapa.
- **Exportación de topología**: Guarda el mapa de red en formato HTML interactivo.

Gestión de Inventario

- **Base de datos SQLite**: Almacena el historial de escaneos y la información de dispositivos.
- **Seguimiento de cambios**: Registra modificaciones en los dispositivos a lo largo del tiempo.
- **Etiquetado y categorización**: Permite organizar dispositivos con etiquetas y categorías.
- **Búsqueda y filtrado**: Localiza rápidamente dispositivos específicos en el inventario.

Exportación e Informes

- **Múltiples formatos**: Exporta resultados a CSV, JSON, HTML y PDF.
- **Informes personalizables**: Genera informes con diferentes niveles de detalle.
- **Estadísticas y gráficos**: Visualiza tendencias y distribución de dispositivos.
- **Informes de seguridad**: Documentación detallada de vulnerabilidades y recomendaciones.

Interfaz y Usabilidad

- **Interfaz moderna**: Diseño con ttkbootstrap para una experiencia visual mejorada.
- **Operaciones en segundo plano**: Escaneos y monitoreo sin bloquear la interfaz.
- **Conexión directa**: Abre interfaces web, conexiones SSH o RDP directamente desde la aplicación.
- **Gestión segura de credenciales**: Almacenamiento cifrado de contraseñas y claves.

Requisitos

- Python 3.6 o superior
- Nmap instalado en el sistema
- Bibliotecas Python (ver requirements.txt)

Instalación

1. Asegúrate de tener instalado Python 3.6 o superior.

2. Instala Nmap en tu sistema:

    - Windows: Descarga e instala desde nmap.org
    - Linux: `sudo apt-get install nmap` (Ubuntu/Debian) o `sudo yum install nmap` (CentOS/RHEL)
    - macOS: `brew install nmap` (usando Homebrew)

3. Clona o descarga este repositorio.

4. Instala las dependencias de Python:

```
pip install -r requirements.txt
```

Uso

Para iniciar la aplicación, ejecuta:

```
python main.py
```

Configuración del escaneo

1. Ingresa el rango de red a escanear (por ejemplo, 192.168.1.0/24) o utiliza la detección automática.
2. Opcionalmente, configura credenciales para obtener información adicional:
    - SSH: Usuario y contraseña o archivo de clave privada
    - SNMP: Comunidad
    - Windows (WMI): Usuario y contraseña
3. Activa el análisis de riesgos si deseas una evaluación de seguridad.
4. Haz clic en "Iniciar Escaneo".

Monitoreo de red

1. Después de un escaneo, puedes activar el monitoreo en tiempo real.
2. Configura las reglas de alerta según tus necesidades.
3. El sistema te notificará cuando se detecten nuevos dispositivos o cambios importantes.

Análisis de seguridad

1. Revisa el informe de seguridad generado tras el escaneo.
2. Consulta las vulnerabilidades detectadas y su nivel de riesgo (crítico, alto, medio, bajo).
3. Implementa las recomendaciones sugeridas para mejorar la seguridad de tu red.

Visualización de topología

1. Accede a la vista de topología para visualizar gráficamente tu red.
2. Interactúa con el mapa para explorar las conexiones entre dispositivos.
3. Exporta la topología para compartirla o documentarla.

Interacción con los resultados

- **Doble clic** en un dispositivo para ver sus detalles completos.
- **Clic derecho** en un dispositivo para acceder al menú contextual con opciones como:
    - Abrir interfaz web (HTTP/HTTPS)
    - Conectar por SSH
    - Conectar por RDP
    - Ver historial de cambios
    - Analizar riesgos de seguridad
- Utiliza las opciones de exportación para guardar los resultados en diferentes formatos.

Estructura del proyecto

- `main.py`: Punto de entrada de la aplicación.
- `ui/gui.py`: Implementación de la interfaz gráfica con ttkbootstrap.
- `core/scanner.py`: Lógica de escaneo de red usando python-nmap.
- `core/monitor.py`: Monitoreo en tiempo real con scapy.
- `core/risk_analyzer.py`: Análisis de riesgos de seguridad.
- `core/security.py`: Auditoría de seguridad y detección de vulnerabilidades.
- `core/topology.py`: Gestión de topología de red.
- `core/network_visualizer.py`: Visualización interactiva de red.
- `core/inventory.py`: Gestión de inventario con SQLite.

- `core/exporter.py`: Exportación de datos a diferentes formatos.
- `core/alert_system.py`: Sistema de alertas configurable.
- `core/ai_analyzer.py`: Análisis con reglas predefinidas.
- `utils/network_utils.py`: Funciones auxiliares de red y gestión de credenciales.

Notas de seguridad

- Esta herramienta debe utilizarse únicamente en redes sobre las que tengas autorización para realizar escaneos.
- El escaneo de puertos puede ser detectado por sistemas de seguridad y considerado como actividad sospechosa.
- Almacena las credenciales de forma segura y no las compartas.
- Las credenciales se almacenan cifradas utilizando Fernet para mayor seguridad.

Licencia