Tel.: +1 (809) 286 1009
Web: www.ogtic.gob.do
RNC: 430-01950-1
ogticrd

# Programa de escanear de puertos

## Objetivo General

Desarrollar una herramienta en Python que permita escanear los puertos de un equipo, ya sea de manera personalizada o utilizando una lista predefinida de puertos, con el fin de identificar qué servicios están activos y potencialmente vulnerables.

## Objetivos Específicos

- **Interfaz de usuario:** Crear una interfaz sencilla que permita al usuario ingresar la dirección IP a escanear y seleccionar el modo de escaneo (lista de puertos predefinida o personalizada).
- **Módulo de escaneo:** Implementar un módulo que utilice la librería socket de Python para intentar establecer conexiones en cada uno de los puertos especificados.
- **Gestión de resultados:** Almacenar los resultados del escaneo en una estructura de datos adecuada (por ejemplo, un diccionario) y generar un archivo de texto con los puertos abiertos y sus respectivos servicios (si es posible identificarlos).
- **Flexibilidad:** Permitir al usuario configurar el rango de puertos a escanear, así como personalizar la lista de puertos a verificar.

## Alcance del Proyecto

- **Tipos de escaneo:** Se implementarán escaneos TCP y UDP, aunque se priorizará TCP por ser el protocolo más común.
- **Sistemas operativos:** Se buscará compatibilidad con los sistemas operativos más utilizados (Windows, Linux, macOS).
- **Servicios identificados:** Se intentará identificar los servicios asociados a cada puerto abierto utilizando bases de datos de servicios conocidos (por ejemplo, nmap-services).
    - Si el puerto identificado es el 21 indique que es el puerto FTP.
    - Si identifica el puerto 80 indique que es HTTP.
- **Generación de reportes:** Se generará un archivo de texto con los resultados del escaneo, incluyendo la dirección IP, el puerto, el estado (abierto/cerrado) y, si es posible, el servicio asociado.

Tel.: +1 (809) 286 1009
Web: www.ogtic.gob.do
RNC: 430-01950-1
ogticrd

## Justificación

Un escáner de puertos es una herramienta fundamental en la evaluación de la seguridad de un sistema. Automatizar este proceso permite realizar análisis de vulnerabilidad de forma más eficiente y precisa, facilitando la identificación de posibles puntos de entrada para ataques.

## Diagrama de Flujo General

[Diagrama de flujo que muestre los siguientes pasos:

1. Ingreso de la dirección IP
2. Selección del modo de escaneo
3. Escaneo de puertos
4. Almacenamiento de resultados
5. Generación de reporte]

## Evaluación

Se evaluará el sistema en función de los siguientes criterios:

- **Precisión:** Porcentaje de puertos correctamente identificados como abiertos o cerrados.
- **Rendimiento:** Tiempo de ejecución para diferentes rangos de puertos y direcciones IP.
- **Usabilidad:** Facilidad de uso de la herramienta.