

🤖 Assistant

以下是更详细的 ****端口扫描工具说明书****，旨在为不同背景和技能水平的用户提供全面的指导，确保他们能够轻松理解和使用该工具。

****端口扫描工具说明书****

****1. 工具简介****

本工具是一个基于 Python 的端口扫描程序，用于扫描指定主机的开放端口，并显示每个端口的作用。它支持多线程扫描，能够快速检测目标主机的端口状态，并将结果保存到文件中。无论是初学者、网络管理员、开发人员还是安全研究人员，都可以通过本工具轻松完成端口扫描任务。

****2. 适用人群****

- ****初学者****：无需编程经验，通过简单的命令行操作即可使用。
- ****网络管理员****：快速检测网络设备的开放端口，排查安全隐患。
- ****开发人员****：测试服务器端口状态，确保服务正常运行。
- ****安全研究人员****：分析目标主机的端口开放情况，评估安全风险。

****3. 功能特点****

- ****多线程扫描****：支持多线程并发扫描，提升扫描速度。
- ****端口作用说明****：自动识别常见端口的作用（如 HTTP、FTP 等），并提供详细说明。
- ****未知端口提示****：对于未知端口，提供进一步调查的建议。
- ****结果保存****：将扫描结果保存到文件中，方便后续分析。
- ****灵活配置****：支持自定义端口范围、线程数等参数。

****4. 使用步骤****

****4.1 安装依赖****

在运行工具之前，请确保已安装以下依赖：

****4.1.1 安装 Python****

1. 访问 [Python 官网](https://www.python.org/downloads/) 下载并安装 Python 3.x 版本。
2. 安装完成后，打开命令行（Windows: `cmd`；Linux/macOS: `终端`），输入以下命令验证安装：

```
```bash
python --version
```
```

如果显示 Python 3.x 版本号，则安装成功。

4.1.2 安装第三方库

1. 打开命令行，运行以下命令安装所需的 Python 库：

```
```bash
pip install python-nmap requests
```
```

4.1.3 安装 `nmap` 工具

1. 访问 [nmap 官网](https://nmap.org/download.html) 下载并安装 `nmap`。
2. 确保 `nmap` 已添加到系统环境变量 `PATH` 中：
 - **Windows**:
 1. 右键点击“此电脑” -> “属性” -> “高级系统设置” -> “环境变量”。
 2. 在“系统变量”中找到 `Path`，点击“编辑”。
 3. 点击“新建”，将 `nmap` 的安装路径（例如：`C:\Program Files (x86)\Nmap`）添加到 `Path` 中。
 4. 点击“确定”保存。

- **Linux/macOS**:

1. 打开终端，运行以下命令：

```
```bash
export PATH=$PATH:/path/to/nmap
```
```

将 `/path/to/nmap` 替换为 `nmap` 的实际安装路径。

3. 验证 `nmap` 是否安装成功：

```
```bash
nmap --version
```
```

如果显示 `nmap` 的版本信息，则安装成功。

4.2 运行工具

1. 将代码保存为 `port_scanner.py`。
2. 打开命令行（Windows: `cmd`；Linux/macOS: `终端`）。
3. 运行以下命令：

```
```bash
python port_scanner.py <主机地址> [选项]
```
```

****示例**:**

- 扫描 `www.163.com` 的 1 到 1024 端口，使用 10 个线程：

```
```bash
python port_scanner.py www.163.com -s 1 -e 1024 -t 10
```
```

- 扫描 `192.168.1.1` 的 1 到 1000 端口，使用默认线程数：

```
```bash
python port_scanner.py 192.168.1.1 -s 1 -e 1000
```
```

4.3 参数说明

| 参 数 | 说 明 |
|----------------------|---|
| ----- ----- | |
| ----- | |
| `<主机地址>` | 要扫描的主机地址（例如：`www.163.com` 或 `192.168.1.1`）。 |
| | |
| `-s`, `--start-port` | 起 始 端 口 号 （ 默 认 ： 1 ）。 |
| | |
| `-e`, `--end-port` | 结 束 端 口 号 （ 默 认 ： 1024 ）。 |
| | |
| `-t`, `--threads` | 最大线程数（默认：10）。线程数越多，扫描速度越快，但负载越大。 |

4.4 输出结果

- ****扫描进度****：实时显示当前扫描的端口号和进度百分比。
- ****扫描结果****：
 - 显示所有打开的端口及其作用。
 - 对于未知端口，提示进一步调查的建议。
- ****结果保存****：扫描结果将保存到当前目录下的 `port_scan_results.txt` 文件中。

****示例输出****：

```
```
```

正在扫描 www.163.com 的端口范围 1 到 1024，使用 10 个线程...

正在扫描端口 80... 进度：7.81%

端口 80 已打开 - HTTP（超文本传输协议）

正在扫描端口 443... 进度：43.36%

端口 443 已打开 - HTTPS（安全的超文本传输协议）

正在扫描端口 18156... 进度：99.90%

端口 18156 已打开 - 未知（此端口可能用于自定义或不常见的服务，建议进一步调查。）

扫描完成。

结果已保存到 port\_scan\_results.txt

``

----

## ## \*\*5. 注意事项\*\*

### 1. \*\*线程数设置\*\*:

- 线程数越多, 扫描速度越快, 但可能会对目标主机造成较大负载。
- 建议根据目标主机的性能和网络环境合理设置线程数。

### 2. \*\*未知端口\*\*:

- 对于未知端口, 工具会提示进一步调查的建议。可以通过访问 [IANA 端口注册表](<https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml>) 获取更多信息。

### 3. \*\*网络连接\*\*:

- 确保目标主机地址有效且网络连接正常。

### 4. \*\*权限问题\*\*:

- 在某些系统上, 扫描端口可能需要管理员权限。在 Linux/macOS 上, 可以使用 `sudo` 运行工具。

----

## ## \*\*6. 常见问题\*\*

### ### \*\*6.1 工具运行时报错: `nmap program was not found in path`\*\*

- \*\*原因\*\*：系统中未安装 `nmap` 或未正确配置环境变量。
- \*\*解决方法\*\*：
  1. 访问 [nmap 官网](<https://nmap.org/download.html>) 下载并安装 `nmap`。
  2. 将 `nmap` 的安装路径添加到系统环境变量 `PATH` 中。

### ### \*\*6.2 扫描速度过慢\*\*

- \*\*原因\*\*：线程数设置过低或网络延迟较高。
- \*\*解决方法\*\*：增加线程数 (例如: `-t 50`)。

### ### \*\*6.3 扫描结果不准确\*\*

- \*\*原因\*\*：目标主机可能启用了防火墙或端口过滤。
- \*\*解决方法\*\*：确保目标主机允许外部访问, 或使用更高级的扫描工具 (如 `nmap`)。

----

## ## \*\*7. 技术支持\*\*

如有任何问题或建议, 请联系:

- **\*\*邮箱\*\***: 无

- **\*\*GitHub\*\***:  
[https://github.com/duma520/port-scanner] (https://github.com/duma520/port-scanner)

----

### ## **\*\*8. 免责声明\*\***

本工具仅用于合法用途，禁止用于未经授权的网络扫描或攻击行为。使用者需自行承担因不当使用导致的任何法律责任。

----

通过本说明书，用户可以快速上手并使用端口扫描工具，满足不同场景下的需求！