

This Python script is a multithreaded TCP port scanner that scans a specified range of ports on a target IP address to identify which ports are open and what common services they correspond to. It uses argparse to handle command-line input, including the target IP, port range, timeout, and thread count. The script leverages socket for TCP connections and concurrent.futures.ThreadPoolExecutor for parallel port scanning, significantly improving speed. Results are printed to the console, showing each open port alongside its mapped service name, based on a predefined dictionary. The script includes robust input validation and error handling to ensure reliability and usability.

```
PowerShell 7.5.1
PS C:\Users\cole> python -m http.server 8080
Serving HTTP on :: port 8080 (http://[::]:8080/) ...
::ffff:127.0.0.1 - - [30/May/2025 20:31:19] "GET / HTTP/1.1" 200 -
::ffff:127.0.0.1 - - [30/May/2025 20:31:19] code 404, message File not found
::ffff:127.0.0.1 - - [30/May/2025 20:31:19] "GET /favicon.ico HTTP/1.1" 404 -
```

The local HTTP server on port 8080 is running successfully, as confirmed by the 200 status for the GET request. The 404 responses indicate that the requested files (/ and /favicon.ico) were not found, which is expected behavior if no index file exists in the directory.

```
PS C:\Projects\port_scanner> python port-scanner.py 127.0.0.1 -p 8080

Scanning 127.0.0.1 for open ports from 8080 to 8080...
Using 1 threads with 1.0s timeout
-----
Progress: 1/1 ports scanned
Scan completed in 0.03 seconds

Open ports:
-----
PORT      SERVICE
-----
8080      HTTP-ALT
PS C:\Projects\port_scanner> |
```

The port scanner successfully identified port 8080 as open on the localhost. It correctly recognized the associated service as HTTP-ALT, confirming accurate functionality.

```
Scanning 127.0.0.1 for open ports from 1 to 1024...
Using 100 threads with 1.0s timeout
-----
Progress: 1024/1024 ports scanned
Scan completed in 11.15 seconds

Open ports:
-----
PORT      SERVICE
-----
135       Unknown
445       SMB
PS C:\Projects\port_scanner> |
```

The port scanner detected two open ports on localhost: port 135 (service unknown) and port 445 (identified as SMB). This indicates that Windows networking services are active and being correctly recognized by the scanner.

```
Scanning 192.168.1.1 for open ports from 1 to 1024...
Using 100 threads with 1.0s timeout
-----
Progress: 1024/1024 ports scanned
Scan completed in 11.14 seconds

Open ports:
-----
PORT      SERVICE
-----
53        DNS
80        HTTP
443       HTTPS
PS C:\Projects\port_scanner> |
```

I tested the scanner on my local router. The scan of 192.168.1.1 revealed three open ports: 53 (DNS), 80 (HTTP), and 443 (HTTPS). The scan completed successfully in 11.14 seconds using 100 threads.