Port Scan Program

CSC 4610

By Ben Finkelstein
& Farzad Mohammadi

Background

- commonly used to identify open ports on a network
- knowledge of ports can maximize security and data transmission rates
- port scan begins by host identification via IP address
- utilizes both TCP and UDP protocols to scan for open ports

Ports

- Port status: open, closed, filtered
- Common ports:
  - Port 20 (UDP) FTP file transfer
  - Port 53 (UDP) DNS for web IP addresses
  - Port 80 (TCP) World Wide Web HTTP

- 0 to 65,536, with 0 to 1023 being common ports for internet use

Security

- port scans are commonly used to identify points of infiltration for cyber-crime
- can establish connection over a network and send packets through open ports
- common ports usually safe
- firewalls are not 100% effective
- port scanning can identify these “risky” ports before a hacker

Program Procedure

- It begins with setting up a socket connection to send network data to a port.
  - Purpose: Determine current status of port.

- The action is completed over a large pool of ports and repeated utilizing loops.

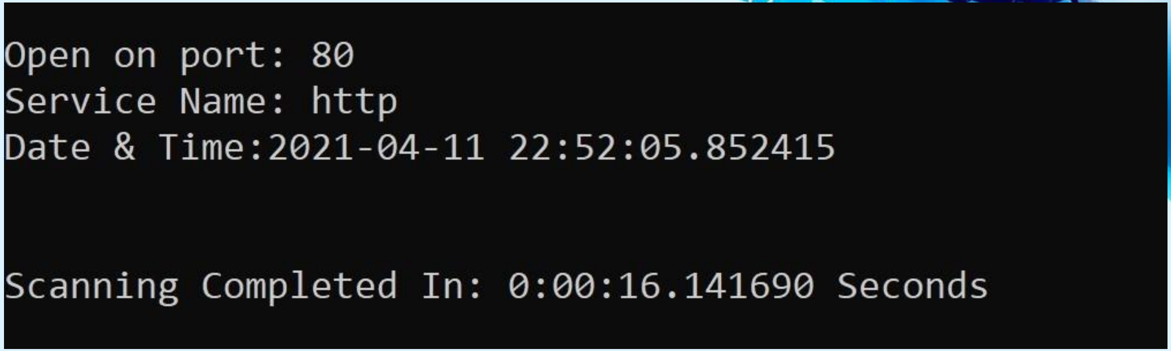
- The procedure of scanning multiple ports is executed asynchronously using concurrent.futures.

- Concurrent.futures: a python module that provides a high-level interface which interacts with pools of threads and processes.

Program Details

Prints Five Different Details:

- Open Port w/
  - Service Name
  - Date & Time



```
Open on port: 80
Service Name: http
Date & Time:2021-04-11 22:52:05.852415


Scanning Completed In: 0:00:16.141690 Seconds
```

- The duration of the entire scan is revealed at the end

- No other details for the intended purposes of the program

Ports

- The number of registered ports and well-known ports are 49,151 which were learned through class lectures.
- The large number of ports took time and testing to decrease the value.
- We tested our localhosts, web hosts, and other hosts to discover our highest values with timeout values set between 1 and 5.
- This assisted in breaking down the number of analyzed ports to 30,000 since the open ports were in proximity.

Service Name

- One of the details of the scanned ports was the ports’ service name.

- The getservbyport() python function from the socket module was employed to acquire the service names.

- Acquired Mainly Known Ports Like:
  - Port 80: HTML
  - Port 135: epmap
  - Port 445: microsoft-dns

- Reasoning: A name is not available for every port

Simple Moments

- It was simple to execute a socket connection and scan a single open port as socket connections have been completed throughout the semester.

- We researched and found the python module, concurrent.futures, to simplify the implementation of loops and the large pool of ports to analyze.

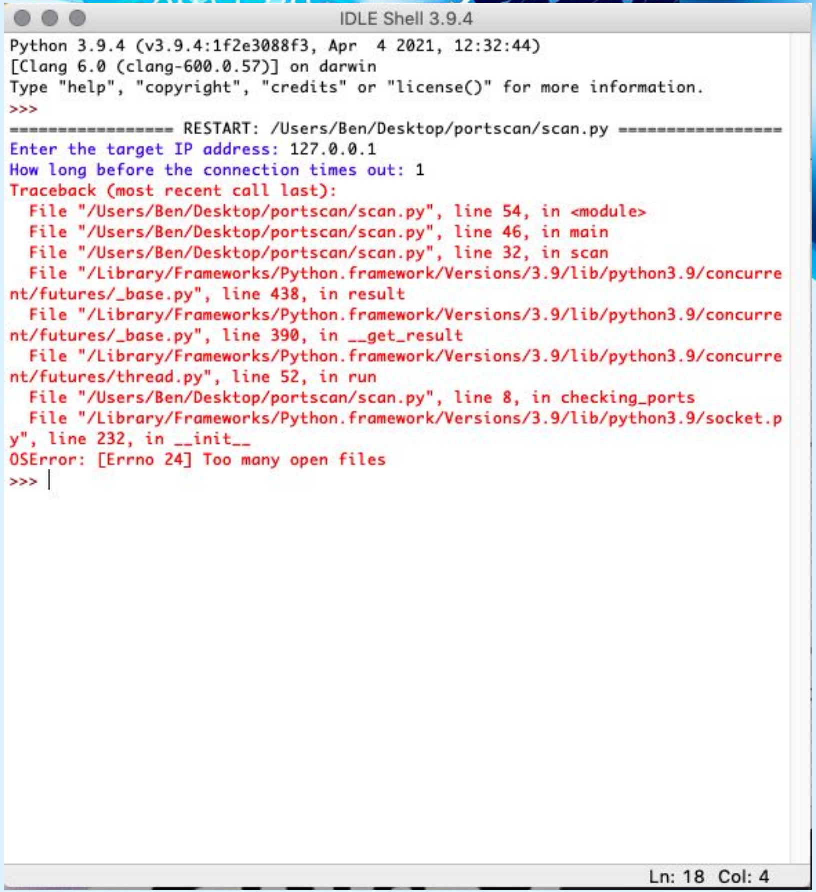
- Concurrent.futures also significantly speeded up the process of looking through all of the ports.

Challenging Moment

- A challenge which occurred was running the program on Apple Macbook where there would be a error due to the threadpoolsize.

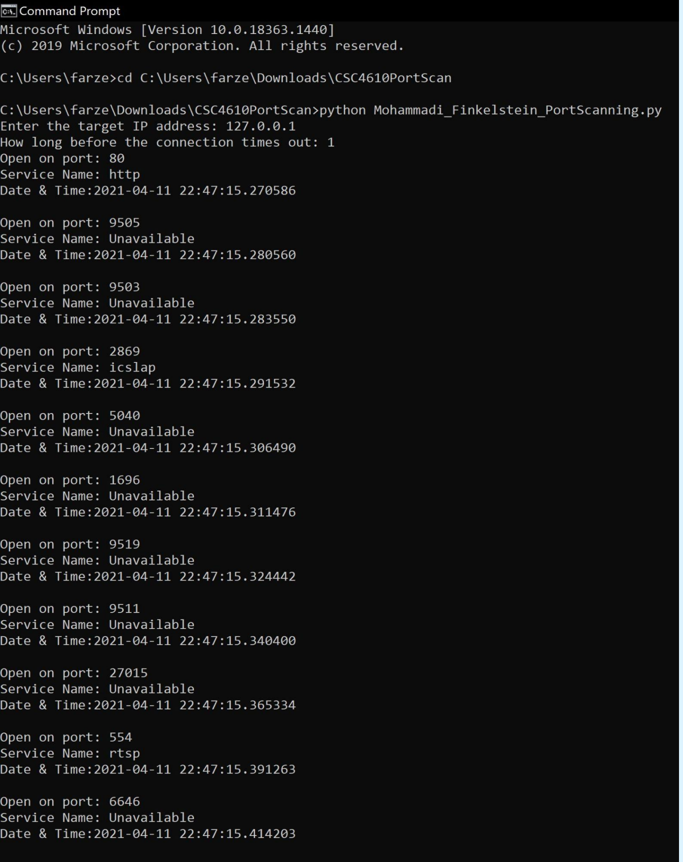
- The error was “OSError: [Errno 24] Too many open files”

- We could not solve this problem and figure out the reason for the error in time so we left it be.

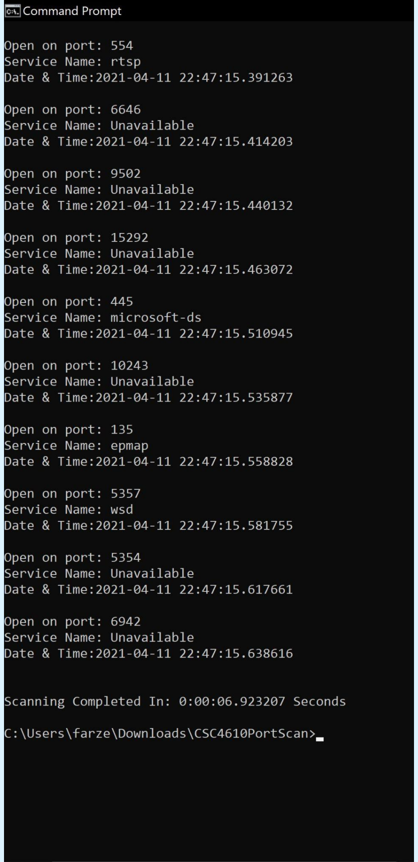


```
Python 3.9.4 (v3.9.4:1f2e3088f3, Apr  4 2021, 12:32:44)
[Clang 6.0 (clang-600.0.57)] on darwin
Type "help", "copyright", "credits" or "license()" for more information.
>>>
================= RESTART: /Users/Ben/Desktop/portscan/scan.py =================
Enter the target IP address: 127.0.0.1
How long before the connection times out: 1
Traceback (most recent call last):
  File "/Users/Ben/Desktop/portscan/scan.py", line 54, in <module>
  File "/Users/Ben/Desktop/portscan/scan.py", line 46, in main
  File "/Users/Ben/Desktop/portscan/scan.py", line 32, in scan
  File "/Library/Frameworks/Python.framework/Versions/3.9/lib/python3.9/concurre
nt/futures/_base.py", line 438, in result
  File "/Library/Frameworks/Python.framework/Versions/3.9/lib/python3.9/concurre
nt/futures/_base.py", line 390, in __get_result
  File "/Library/Frameworks/Python.framework/Versions/3.9/lib/python3.9/concurre
nt/futures/thread.py", line 52, in run
  File "/Users/Ben/Desktop/portscan/scan.py", line 8, in checking_ports
  File "/Library/Frameworks/Python.framework/Versions/3.9/lib/python3.9/socket.p
y", line 232, in __init__
OSError: [Errno 24] Too many open files
>>> |
```

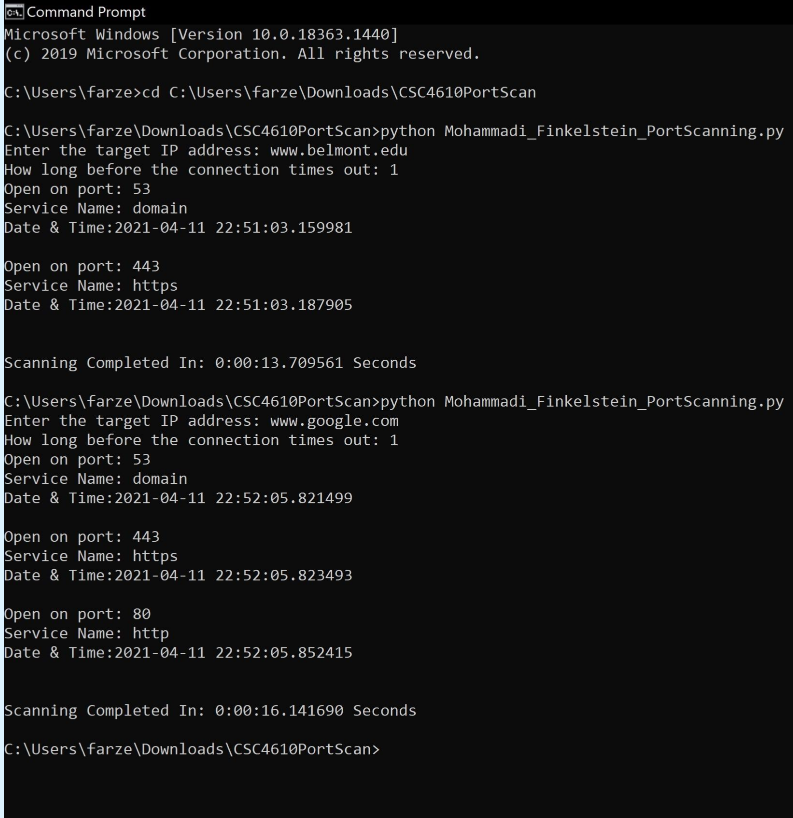
Results (Screenshots)



```
Microsoft Windows [Version 10.0.18363.1440]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\farze>cd C:\Users\farze\Downloads\CSC4610PortScan

C:\Users\farze\Downloads\CSC4610PortScan>python Mohammadi_Finkelstein_PortScanning.py
Enter the target IP address: 127.0.0.1
How long before the connection times out: 1
Open on port: 80
Service Name: http
Date & Time:2021-04-11 22:47:15.270586

Open on port: 9505
Service Name: Unavailable
Date & Time:2021-04-11 22:47:15.280560

Open on port: 9503
Service Name: Unavailable
Date & Time:2021-04-11 22:47:15.283550

Open on port: 2869
Service Name: icslap
Date & Time:2021-04-11 22:47:15.291532

Open on port: 5040
Service Name: Unavailable
Date & Time:2021-04-11 22:47:15.306490

Open on port: 1696
Service Name: Unavailable
Date & Time:2021-04-11 22:47:15.311476

Open on port: 9519
Service Name: Unavailable
Date & Time:2021-04-11 22:47:15.324442

Open on port: 9511
Service Name: Unavailable
Date & Time:2021-04-11 22:47:15.340400

Open on port: 27015
Service Name: Unavailable
Date & Time:2021-04-11 22:47:15.365334

Open on port: 554
Service Name: rtsp
Date & Time:2021-04-11 22:47:15.391263

Open on port: 6646
Service Name: Unavailable
Date & Time:2021-04-11 22:47:15.414203
```



```
Open on port: 554
Service Name: rtsp
Date & Time:2021-04-11 22:47:15.391263

Open on port: 6646
Service Name: Unavailable
Date & Time:2021-04-11 22:47:15.414203

Open on port: 9502
Service Name: Unavailable
Date & Time:2021-04-11 22:47:15.440132

Open on port: 15292
Service Name: Unavailable
Date & Time:2021-04-11 22:47:15.463072

Open on port: 445
Service Name: microsoft-ds
Date & Time:2021-04-11 22:47:15.510945

Open on port: 10243
Service Name: Unavailable
Date & Time:2021-04-11 22:47:15.535877

Open on port: 135
Service Name: epmap
Date & Time:2021-04-11 22:47:15.558828

Open on port: 5357
Service Name: wsd
Date & Time:2021-04-11 22:47:15.581755

Open on port: 5354
Service Name: Unavailable
Date & Time:2021-04-11 22:47:15.617661

Open on port: 6942
Service Name: Unavailable
Date & Time:2021-04-11 22:47:15.638616


Scanning Completed In: 0:00:06.923207 Seconds

C:\Users\farze\Downloads\CSC4610PortScan>
```



```
Microsoft Windows [Version 10.0.18363.1440]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\farze>cd C:\Users\farze\Downloads\CSC4610PortScan

C:\Users\farze\Downloads\CSC4610PortScan>python Mohammadi_Finkelstein_PortScanning.py
Enter the target IP address: www.belmont.edu
How long before the connection times out: 1
Open on port: 53
Service Name: domain
Date & Time:2021-04-11 22:51:03.159981

Open on port: 443
Service Name: https
Date & Time:2021-04-11 22:51:03.187905


Scanning Completed In: 0:00:13.709561 Seconds

C:\Users\farze\Downloads\CSC4610PortScan>python Mohammadi_Finkelstein_PortScanning.py
Enter the target IP address: www.google.com
How long before the connection times out: 1
Open on port: 53
Service Name: domain
Date & Time:2021-04-11 22:52:05.821499

Open on port: 443
Service Name: https
Date & Time:2021-04-11 22:52:05.823493

Open on port: 80
Service Name: http
Date & Time:2021-04-11 22:52:05.852415


Scanning Completed In: 0:00:16.141690 Seconds

C:\Users\farze\Downloads\CSC4610PortScan>
```

Conclusion

- Port scanning will most likely remain relevant and more advanced as we progress as a more technologically advanced and interconnected society.

- However, as port scans and firewall protections get more advanced, so too will the cyber-criminals’ techniques to identify open ports.

- It will be up to IT professionals and computer scientists to develop better methods to identify and protect open and at-risk ports beyond a basic port scan.