# Marc Pierrot

# February 28, 2022,

# analyze a network for vulnerabilities

# write a Python program that should test the given host, and it should generate a list of

# all the TCP Open ports within the range of 1 to 1025.

import socket

import datetime

name = input("Please enter your full name: ")

print("Hello!" + name)

print("\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*Welcome to our Port Scanner\*\*\*\*\*\*\*\*\*\*\*\*\*")

fl\_tpt = open("port's scan file.txt", "w")

fl\_tpt.write("Welcome to the scanner-dome.--..--..--..--..-\*-.\n\n")

target\_name = input("Enter the host that you want to scan please: ")

target\_ip = socket.gethostbyname(target\_name)

"""just\_checking = socket.gethostbyaddr(target\_ip)

print(str(target\_ip) + " : " + str(just\_checking))"""

print(target\_ip)

fl\_tpt.write("Scanning the target: {}\n\n".format(target\_name))

starttime = datetime.datetime.now()

fl\_tpt.write(str(starttime) + "\n")

print(starttime)

openports = []

count = 0

i = 1

while i <= 1025:

s = socket.socket(socket.AF\_INET, socket.SOCK\_STREAM)

status = s.connect\_ex((target\_ip, i))

if status == 0:

print("{}:{} is open to check!".format(target\_ip, i))

fl\_tpt.write(str(target\_ip) + " : " + str(i) + " is open")

fl\_tpt.write("{}:{} is open to check!\n".format(target\_ip, i))

openports.append(i)

count += 1

elif status == 10060:

print("{}:{} is closed - Status code: {} This is the reason this port is closed".format(target\_ip, i,

status))

fl\_tpt.write("{}:{} is closed - Status code: {} This is the reason this port is closed".format(target\_ip, i,

status))

elif status == 10061:

print("{}:{} is closed - Status code: {} This is the other reason this port is closed".format(target\_ip, i,

status))

elif status == 6660:

print("{}:{} is closed - Status code: {} This is the other reason this port is closed".format(target\_ip, i,

status))

elif status == 6669:

print("{}:{} is closed - Status code: {} This is the other reason this port is closed".format(target\_ip, i,

status))

else:

print("{}:{} is closed - Status code: {}".format(target\_ip, i, status))

i += 1

endtime = datetime.datetime.now()

fl\_tpt.write("\n" + str(endtime) + "\n")

print(endtime)

total\_time = endtime - starttime

fl\_tpt.write("This is the total time taken for the scan: " + str(total\_time) + " The total number of open ports wa s: "

+ str(count))

print(total\_time)

fl\_tpt.close()

print("thank you" + name + "for using our port's scan bye!")