Lấy thông tin website

import requests

def geoip(domain):

headers = {

"Content-Type": "application/json"

}

response = requests.get('http://freegeoip.app/json/' + domain,headers=headers)

return(response.text)

print(geoip('python.org'))

**Tạo webserver (chạy cùng với test server)**

import socket

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

mySocket.bind(('localhost', 8080))

mySocket.listen(5)

while True:

print('Waiting for connections')

(recvSocket, address) = mySocket.accept()

print('HTTP request received:')

print(recvSocket.recv(1024))

recvSocket.send(bytes("HTTP/1.1 200 OK\r\n\r\n <html><body><h1>Hello world!</h1></body></html> \r\n",'utf-8'))

recvSocket.close()

**Test server**

import socket

webhost = 'localhost'

webport = 8080

print("Contacting %s on port %d ..." % (webhost, webport))

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

webclient.connect((webhost, webport))

webclient.send(bytes("GET / HTTP/1.1\r\nHost: localhost\r\n\r\n".encode('utf-8')))

reply = webclient.recv(4096)

print("Response from %s:" % webhost)

print(reply.decode())

**Một số hàm socket**

import socket

try:

print("gethostname:",socket.gethostname())

print("gethostbyname",socket.gethostbyname('www.google.com'))

print("gethostbyname\_ex",socket.gethostbyname\_ex('www.google.com'))

print("gethostbyaddr",socket.gethostbyaddr('8.8.8.8'))

print("getfqdn",socket.getfqdn('www.google.com'))

print("getaddrinfo",socket.getaddrinfo("www.google.com",None,0,socket.SOCK\_STREAM))

except socket.error as error:

print (str(error))

print ("Connection error")

**Phân giải địa chỉ**

import socket

try :

result = socket.gethostbyaddr("8.8.8.8")

print("The host name is:",result[0])

print("Ip addresses:")

for item in result[2]:

print(" "+item)

except socket.error as e:

print("Error for resolving ip address:",e)

**Scan cổng**

import optparse

from socket import \*

from threading import \*

def socketScan(host, port):

try:

socket\_connect = socket(AF\_INET, SOCK\_STREAM)

socket\_connect.settimeout(5)

result = socket\_connect.connect((host, port))

print('[+] %d/tcp open' % port)

except Exception as exception:

print('[-] %d/tcp closed' % port)

print('[-] Reason:%s' % str(exception))

finally:

socket\_connect.close()

def portScanning(host, ports):

try:

ip = gethostbyname(host)

print('[+] Scan Results for: ' + ip)

except:

print("[-] Cannot resolve '%s': Unknown host" %host)

return

for port in ports:

t = Thread(target=socketScan,args=(ip,int(port)))

t.start()

def main():

host = 'www.google.com'

ports = 80,81,21,22,443

portScanning(host, ports)

if \_\_name\_\_ == '\_\_main\_\_':

main()