#!/bin/python3

import socket # Socket Library

from IPy import IP # IP Library

# Scan the Ip address and print out the port that are open

# It collects the translated IP address for check ip function and scans it against a range of ports

def scan(target): # Function that scan the target and returns the opened ports on the target.

converted\_ip = check\_ip(target) # output of the check\_ip is assigned to the variable converted\_ip

print('\n' + '[-\_ 0 scanning Target]' + str(target))

for port in range(1, 500): # A forloop for scanning in the range between 1 & 50

scan\_port(converted\_ip, port) # Calling the scan\_port function with the converted IP address and port as it arguments

def check\_ip(ip): # function creates from IP Library to map webhostname to ip address.

try:

try:

IP(ip)

return(ip)

except ValueError:

return socket.gethostbyname(ip) # maps hostname to it IP address

except: #(socket.gaierror) as err:

pass

def get\_banner(s): # Banner grabbing using socket function

return s.recv(1024)

def scan\_port(ipaddress, port): # scan\_port function with ipaddress and port as it parameter

try:

sock = socket.socket() # creates the socket object sock for other content manangement

sock.settimeout(0.5) # a socket object that set the amount of time used to scan each port

sock.connect ((ipaddress, port)) # socket object that is use for establishing connection to internet

try:

banner = get\_banner(sock)

print(' [+] Open port ' + str(port) + ' : ' + str(banner.decode().strip('\n')))

except:

print(' [+] Open Port ' + str(port))

except: