|  |  |
| --- | --- |
| Portfolio Task 4 - Python | |
|  | |
| 24/09/2022COIT11241 | 12195171 DILSHA KEERTHI KUMARACYBER SECURITY TECHNOLOGIES |

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  |  |
|  | PRIVATE GIT REPOSITORY | |  |
|  | <https://github.com/DilshaWe/ePortfolio.git> CODE import os  import subprocess  import requests  import re  response = requests.get('http://dev.virtualearth.net/REST/v1/Imagery/Map/Road/-16.9206560000013,145.777730700002/15?mapSize=500,500&key=AlYOKsYd2-Kn51Hnnws3Ua\_3TMbDjlO85lMbpdi9aT92DZe8NRyteXVvhzJOlViG' )  print( response.raw )  with open('bingmap.png', 'wb') as out\_file:  out\_file.write( response.content )  del response  # to create the list  def Q2CreateL() :  subprocess.check\_output(" > ftpRepo.txt ", shell=True)  output = subprocess.check\_output(" ip a | grep -E '([0-9]{1,3}[\.]){3}[0-9]{1,3}' ", shell=True)  output = output.decode().split("\n")  list =[]  for i in range( len(output)) :  if i > 0 and i < len(output) -1 :  #print(output[i].split("inet ")[1].split(" ")[0] )  try:  var = output[i].split("inet ")[1].split(" ")[0]  strng = "nmap -sn "+ var + " | grep -E '([0-9]{1,3}[\.]){3}[0-9]{1,3}' "  out2 = subprocess.check\_output( strng , shell=True)  out2 = out2.split("\n")  for j in range ( len( out2)) :  if j > 0 and j < len( out2 )- 1 :  var2 = out2[j].split(" ")[4]  #print(var2)  strng2 = " nmap -sV -O "+ var2 + " |grep ftp ; exit 0 "  out3 = subprocess.check\_output( strng2 , stderr=subprocess.STDOUT, shell=True )  if out3 != "" :  out3 = out3.split("\n")  for k in range( len( out3)):  if k < len((out3)) -1 :  #print( out3 )  text = var2 + " : " + out3[0]  #print( text )  subprocess.check\_output("echo '"+ text + "' >> ftpRepo.txt ; exit 0 ", stderr=subprocess.STDOUT , shell=True )  except:  continue  def Q2CheckL():  lines = []  with open("ftpRepo.txt") as file:  for line in file:  #print(line.rstrip())  lines.append(line.rstrip())  output = subprocess.check\_output(" ip a | grep -E '([0-9]{1,3}[\.]){3}[0-9]{1,3}' ", shell=True)  output = output.decode().split("\n")  for i in range( len(output)) :  if i > 0 and i < len(output) -1 :  #print(output[i].split("inet ")[1].split(" ")[0] )  try:  var = output[i].split("inet ")[1].split(" ")[0]  strng = "nmap -sn "+ var + " | grep -E '([0-9]{1,3}[\.]){3}[0-9]{1,3}' "  out2 = subprocess.check\_output( strng , shell=True)  out2 = out2.split("\n")  for j in range ( len( out2)) :  if j > 0 and j < len( out2 )- 1 :  var2 = out2[j].split(" ")[4]  #print(var2)  strng2 = " nmap -sV -O "+ var2 + " |grep ftp ; exit 0 "  out3 = subprocess.check\_output( strng2 , stderr=subprocess.STDOUT, shell=True )  if out3 != "" :  out3 = out3.split("\n")  for k in range( len( out3)):  if k < len((out3)) -1 :  #print( out3 )  text = var2 + " : " + out3[0]  #print( text )  if text not in lines :  print( text +" is not an allowed ftp server")  if out3[0].split(" ")[-1] == "2.3.4" :  print( "\*\*\*\*\*\*\*\*\*\*\*The server " + var2 + " has a ftp server version 2.3.4\*\*\*\*\*\*\*\*\*\*\* " )  except:  continue  yes = { '1' }  no = { '2' }  print(" please enter 1 to make the input ftp inventory file . press 2 to check the network with the ftp file ")  choice = input().lower()  if choice in yes:  print("please wait for a few minutes")  Q2CreateL()  elif choice in no:  print("please wait for a few minutes")  Q2CheckL()  else:  print("please provide valid input")  def Q3CreateL() :  subprocess.check\_output(" > httpRepo.txt ", shell=True)  output = subprocess.check\_output(" ip a | grep -E '([0-9]{1,3}[\.]){3}[0-9]{1,3}' ", shell=True)  output = output.decode().split("\n")  list =[]  for i in range( len(output)) :  if i > 0 and i < len(output) -1 :  #print(output[i].split("inet ")[1].split(" ")[0] )  try:  var = output[i].split("inet ")[1].split(" ")[0]  strng = "nmap -sn "+ var + " | grep -E '([0-9]{1,3}[\.]){3}[0-9]{1,3}' "  out2 = subprocess.check\_output( strng , shell=True)  out2 = out2.split("\n")  for j in range ( len( out2)) :  if j > 0 and j < len( out2 )- 1 :  var2 = out2[j].split(" ")[4]  #print(var2)  strng2 = " nmap -sV -O "+ var2 + " |grep 'open http' ; exit 0 "  out3 = subprocess.check\_output( strng2 , stderr=subprocess.STDOUT, shell=True )  if out3 != "" :  out3 = out3.split("\n")  for k in range( len( out3)):    if k < len((out3)) -1 :  #print( out3 )  text = var2 + " : " + out3[0]  #print( text )  subprocess.check\_output("echo '"+ text + "' >> httpRepo.txt ; exit 0 ", stderr=subprocess.STDOUT , shell=True )  except:  continue  def Q3CheckL():  lines = []  with open("httpRepo.txt") as file:  for line in file:  #print(line.rstrip())  lines.append(line.rstrip())  output = subprocess.check\_output(" ip a | grep -E '([0-9]{1,3}[\.]){3}[0-9]{1,3}' ", shell=True)  output = output.decode().split("\n")  for i in range( len(output)) :  if i > 0 and i < len(output) -1 :  #print(output[i].split("inet ")[1].split(" ")[0] )  try:  var = output[i].split("inet ")[1].split(" ")[0]  strng = "nmap -sn "+ var + " | grep -E '([0-9]{1,3}[\.]){3}[0-9]{1,3}' "  out2 = subprocess.check\_output( strng , shell=True)  out2 = out2.split("\n")  for j in range ( len( out2)) :  if j > 0 and j < len( out2 )- 1 :  var2 = out2[j].split(" ")[4]  #print(var2)  strng2 = " nmap -sV -O "+ var2 + " |grep 'open http' ; exit 0 "  out3 = subprocess.check\_output( strng2 , stderr=subprocess.STDOUT, shell=True )  if out3 != "" :  out3 = out3.split("\n")  for k in range( len( out3)):  if k < len((out3)) -1 :  #print( out3 )  text = var2 + " : " + out3[0]  #print( text )  if text not in lines :  print( text +" is not an allowed http server")  # servers with no idle workers  str = "ssh root@"+var2+" apachectl status |grep Status"  output = subprocess.check\_output(str , shell=True )  if output.split("requests/sec: ")[1].split("; Current")[0] == "0" :  print( "The host " + var2 + " has no idle workers")    # trying to login to dvwa  url = 'http://'+ var2 +'/DVWA/login.php'  s = requests.Session()  x = s.post(url)  if x.status\_code == 200:  print("THe server " + var2 + " has a running DVWA. Trying to login to it with admin:password ")  pattern = r'\b\w{32}\b'  result = re.findall( pattern , x.text )  myobj = {'username': 'admin' , 'password': 'password', 'user\_token': result[0] , 'Login': 'Login' }  m = s.post( url , data = myobj )  try:  re.search( 'sqli/">SQL Injection</a></li>', m.text).group(0)  print("Login was successful")  except AttributeError:  print("Login was failed")  except:  continue  yes = { '1' }  no = { '2' }  print(" please enter 1 to make the input http inventory file . press 2 to check the network with the http file ")  choice = input().lower()  if choice in yes:  print("please wait for a few minutes")  Q3CreateL()  elif choice in no:  print("please wait for a few minutes")  Q3CheckL()  else:  print("please provide valid input") EVIDENCE OF OUTPUT | |  |
|  | E:\Dilsha\CQ\Cyber\Python\PHOTO-2022-09-25-00-00-59.jpg | |  |

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  |  |