**NTKH**

**Chỉnh sửa code trên để có thể chạy và nhập file như là một tham số khi gọi chương trình**

import string

import sys

def process\_file(fname):

fstring = ""

min\_length = 4

try:

with open(fname, errors="ignore") as f:

print("File opened successfully.")

result = ""

for c in f.read():

if c in string.printable:

result += c

continue

if len(result) >= min\_length:

fstring += result + '\n'

result = ""

except Exception as e:

print(f"Error opening file: {e}")

return ""

print(f"Processed string:\n{fstring}")

return fstring

# Lab03-01.exe đã được tải lên Google Colab

filename = 'Lab03-01.exe'

output = process\_file(filename)

print(f"Output:\n{output}")

**Xác định host-based indicators, network-based indicators từ các strings**

**Host-Based Indicators (Chỉ số dựa trên máy chủ)**

* File Paths và Registry Keys:
  + SOFTWARE\Classes\http\shell\open\commandV
  + Software\Microsoft\Active Setup\Installed Components\
  + SOFTWARE\Microsoft\Windows\CurrentVersion\Run
  + SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders
* Tập tin liên quan:
  + vmx32to64.exe
* Các tên thư mục:
  + AppData
* Các hàm và thư viện hệ thống:
  + ExitProcess
  + kernel32.dll
  + ws2\_32
  + advapi32
  + ntdll
  + user32
* Tên tiến trình và các từ khoá:
  + VideoDriver
  + WinVMX32-
  + admin

**Network-Based Indicators (Chỉ số dựa trên mạng)**

* HTTP Request:
  + CONNECT %s:%i HTTP/1.0
  + Đây là một mẫu yêu cầu HTTP cho thấy malware có thể thực hiện các kết nối mạng.
* Địa chỉ Website:
  + www.practicalmalwareanalysis.com
  + Đây có thể là một địa chỉ mà malware cố gắng kết nối tới.
* Các chỉ báo khác:
  + Các chuỗi như 0cks=, 0ttp= có thể chỉ định thông tin về kết nối mạng hoặc dữ liệu mà malware sử dụng.