Mai Quốc Việt – 21IT595 – 21NS

Code Python : myString.py

import string

import sys

import os

def extract\_strings(filename, min\_length=4):

    fstring = ""

    try:

        with open(filename, "rb") as f:

            result = ""

            for c in f.read().decode(errors="ignore"):

                if c in string.printable:

                    result += c

                    continue

                if len(result) >= min\_length:

                    fstring += result + '\n'

                result = ""

    except FileNotFoundError:

        print(f"Error: File '{filename}' not found!")

        sys.exit(1)

    except Exception as e:

        print(f"Error: {e}")

        sys.exit(1)

    return fstring

def extract\_indicators(strings):

    host\_indicators = []

    network\_indicators = []

    for line in strings.split("\n"):

        if "\\" in line or "/" in line:

            host\_indicators.append(line)

        if any(proto in line for proto in ["http", "https", "ftp", "tcp", "udp"]):

            network\_indicators.append(line)

    return host\_indicators, network\_indicators

def main():

    if len(sys.argv) > 1:

        fname = sys.argv[1]

    else:

        fname = input("Enter filename: ")

    if not fname:

        print("Pls enter a file name")

        sys.exit()

    strings = extract\_strings(fname)

    print("Extracted Strings:\n", strings)

    host\_indicators, network\_indicators = extract\_indicators(strings)

    print("\nHost-based Indicators:")

    print("\n".join(host\_indicators) if host\_indicators else "None found")

    print("\nNetwork-based Indicators:")

    print("\n".join(network\_indicators) if network\_indicators else "None found")

if \_\_name\_\_ == "\_\_main\_\_":

    main()

Kết quả sau khi chạy lệnh





