BÁO CÁO BÀI TẬP

Môn học: Cơ chế hoạt động của mã độc

Tên chủ đề: Mã độc lẫn trốn

GVHD: Phạm Văn Hậu – Phan Thế Duy

1. THÔNG TIN CHUNG:

(Liệt kê tất cả các thành viên trong nhóm)

Lớp: NT230.N21.ANTN

STT	Họ và tên	MSSV	Email
1	Võ Anh Kiệt	20520605	20520605@gm.uit.edu.vn
2	Nguyễn Bùi Kim Ngân	20520648	20520648@gm.uit.edu.vn
3	Nguyễn Bình Thục Trâm	20520815	20520815@gm.uit.edu.vn

2. NỘI DUNG THỰC HIỆN:[1]

STT	Công việc	Kết quả tự đánh giá
1	Yêu cầu 1	60%
2	Yêu cầu 2	60%

Phần bên dưới của báo cáo này là tài liệu báo cáo chi tiết của nhóm thực hiện.

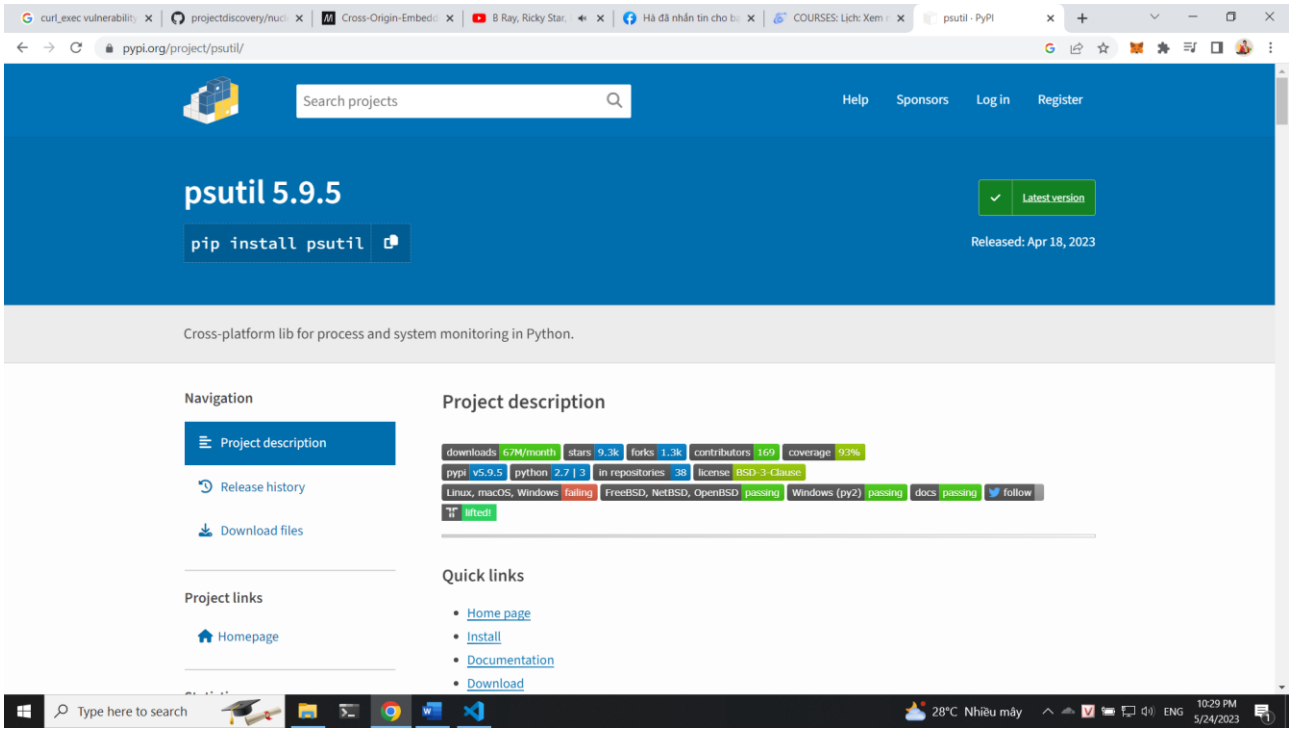
[1] Ghi nội dung công việc, các kịch bản trong bài Thực hành

BÁO CÁO CHI TIẾT

1. Yêu cầu 1

Đầu tiên ta cần phải chú ý đến việc đặc điểm của môi trường máy ảo và môi trường sandbox

Để kiểm tra các thông tin này thì ta cần kiểm tra các thông tin liên quan đến bộ nhớ ảo (virtual memory) và thông tin liên quan đến CPU (cpu count). Ở đây để thực hiện kiểm tra các thông tin này ta cần sử dụng đến một thư viện của python là psutil:



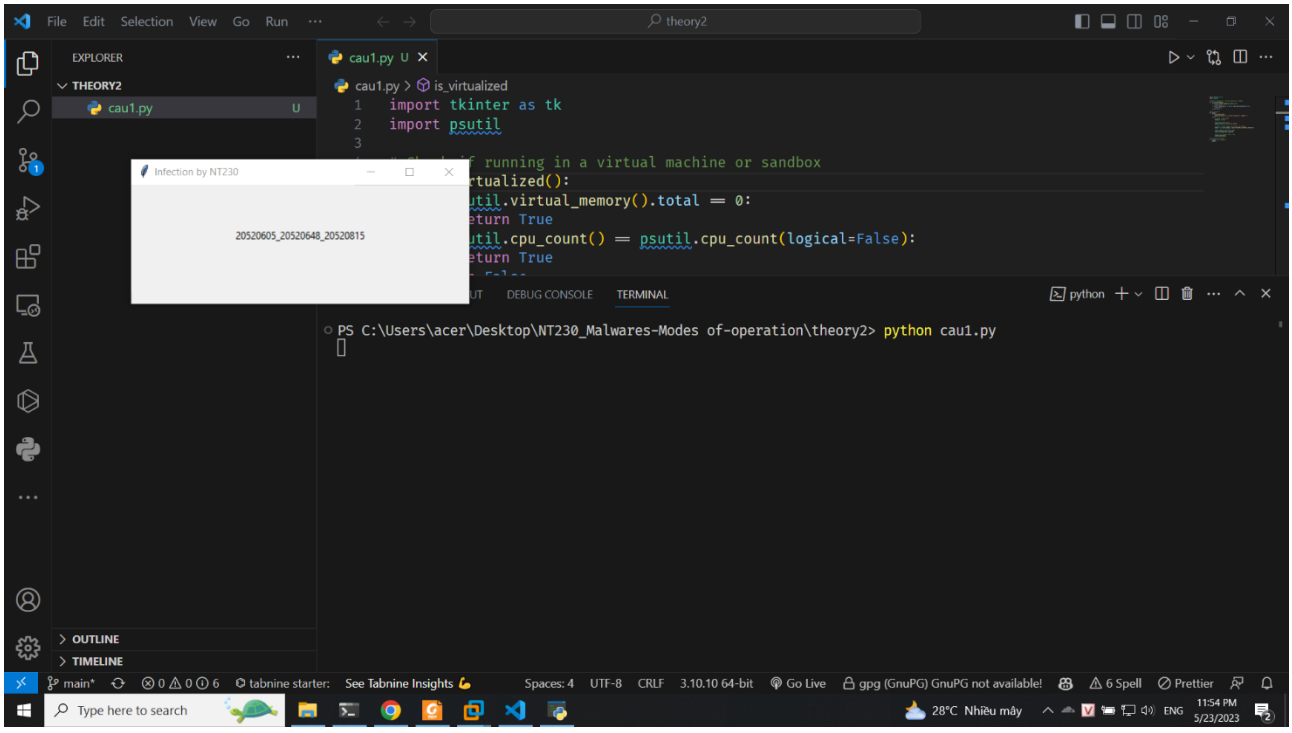
Tiếp theo ta sẽ viết một chương trình python thực hiện việc pop up cửa sổ lên nếu trong môi trường thường và không thực hiện nếu ở trong môi trường máy ảo hay sandbox (comment giải thích chi tiết trong code)

```
import tkinter as tk
import psutil

# Check if running in a virtual machine or sandbox
def is_virtualized():
    if psutil.virtual_memory().total == 0:
        return True
    if psutil.cpu_count() == psutil.cpu_count(logical=False):
        return True
    return False

# Main function
```

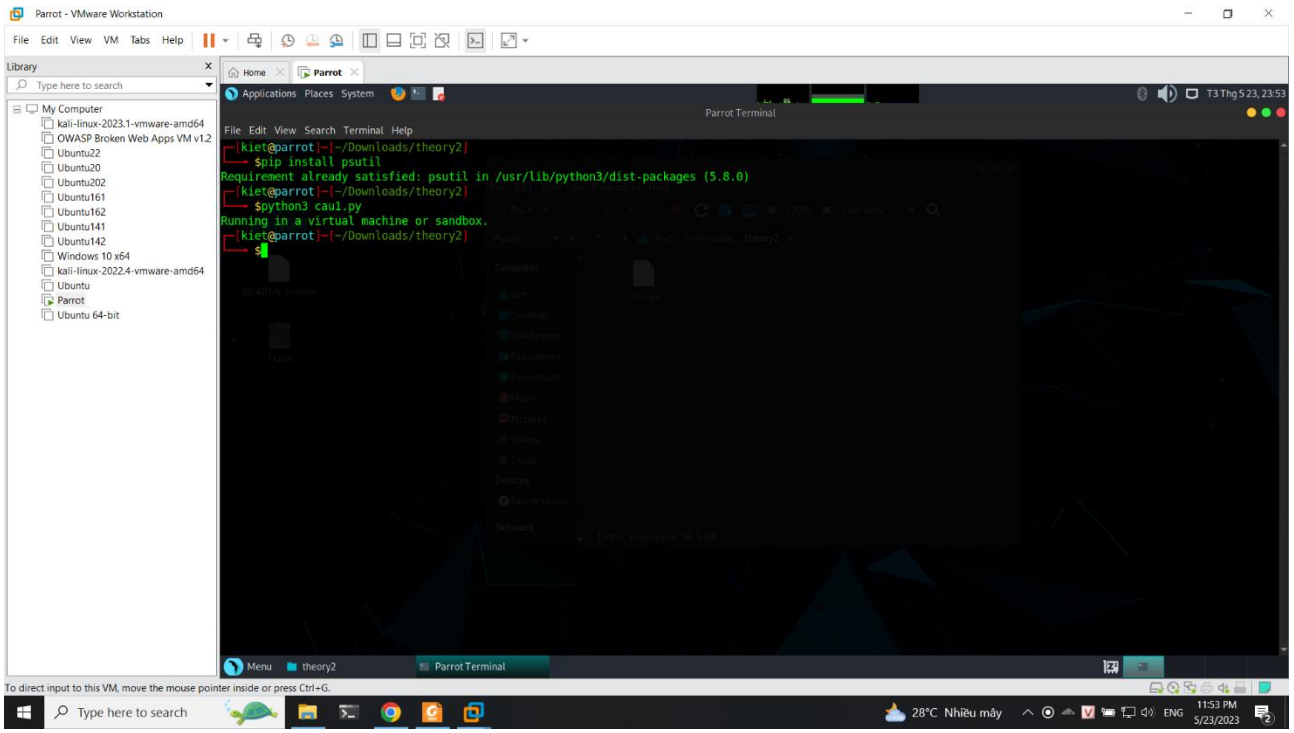
```python
def main():
    if is_virtualized():
        print("Running in a virtual machine or sandbox.")
    else:
        # Create a new window
        window = tk.Tk()

        # Set the window title
        window.title("Infection by NT230")

        # Create a label widget to display the message
        label = tk.Label(window, text="20520605_20520648_20520815")

        # Add padding around the label
        label.pack(padx=50, pady=50)

        # Start the Tkinter event loop
        window.mainloop()

# Run the main function
if __name__ == "__main__":
    main()
```

Ở chương trình này ta sẽ thực hiện thực thi ở các môi trường khác nhau

Môi trường thường:



Môi trường máy ảo



Ở đây ta thấy chương trình đã thực hiện đúng việc lẫn trốn trong các môi trường máy ảo và sandbox.

Tiếp theo ta cần phải thực hiện chuyển đổi code

Python → C → bytecode

Từ đó thực hiện truyền vào chương trình ở Ex01 để thực hiện tiêm vào chương trình.

Nhưng bước này tụi em thực hiện chưa tốt nên chưa thể hoàn thành yêu cầu này

2. Yêu cầu 2

Ở phần này ta sẽ thực hiện việc mã hoá và giải mã với kỹ thuật XOR

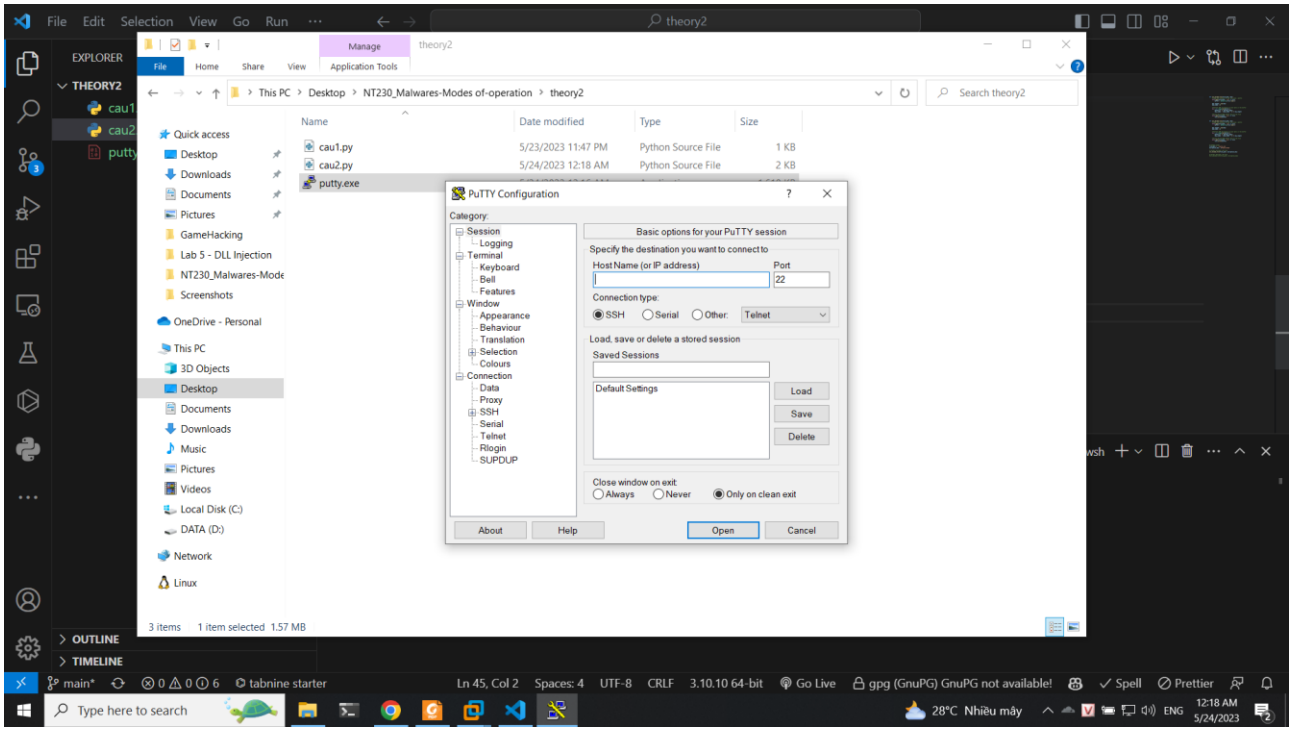
Đầy tiên ta sẽ thực hiện code

```
def xor_encode_file(file_path, key):
    # Read the contents of the file into a buffer
    with open(file_path, 'rb') as file:
        buffer = bytearray(file.read())

    key_length = len(key)
    key_index = 0

    # Perform XOR encryption on each byte in the buffer
    for i in range(len(buffer)):
        buffer[i] ^= key[key_index]
        key_index = (key_index + 1) % key_length

    # Write the encoded buffer back to the file
```

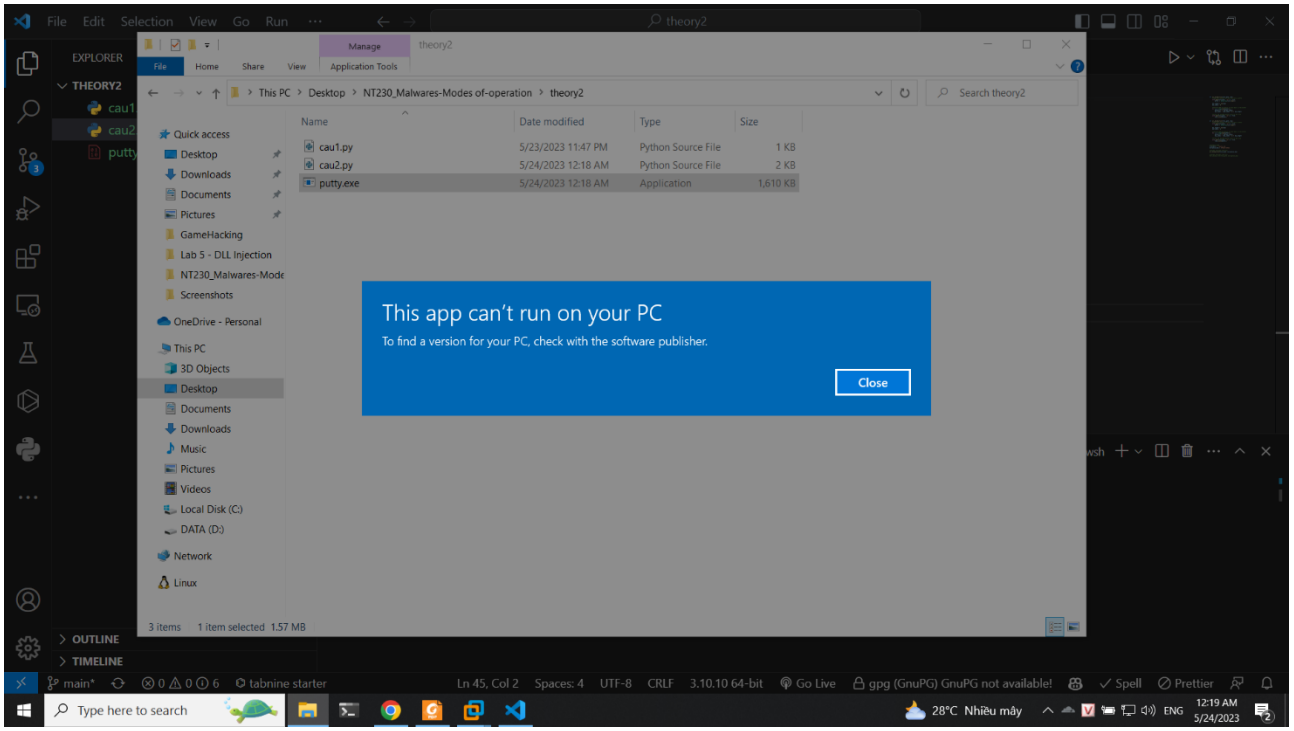
```
    with open(file_path, 'wb') as file:
        file.write(buffer)


def xor_decode_file(file_path, key):
    # Read the contents of the file into a buffer
    with open(file_path, 'rb') as file:
        buffer = bytearray(file.read())

    key_length = len(key)
    key_index = 0

    # Perform XOR decryption on each byte in the buffer
    for i in range(len(buffer)):
        buffer[i] ^= key[key_index]
        key_index = (key_index + 1) % key_length

    # Write the decoded buffer back to the file
    with open(file_path, 'wb') as file:
        file.write(buffer)


# Example usage
file_path = './putty.exe'
encryption_key = b'MySecretKey'

# Encode (encrypt) the file
xor_encode_file(file_path, encryption_key)

# Decode (decrypt) the file
xor_decode_file(file_path, encryption_key)
```

Đầu tiên ở code này ta sẽ thực nghiệm với chương trình thông thường là putty

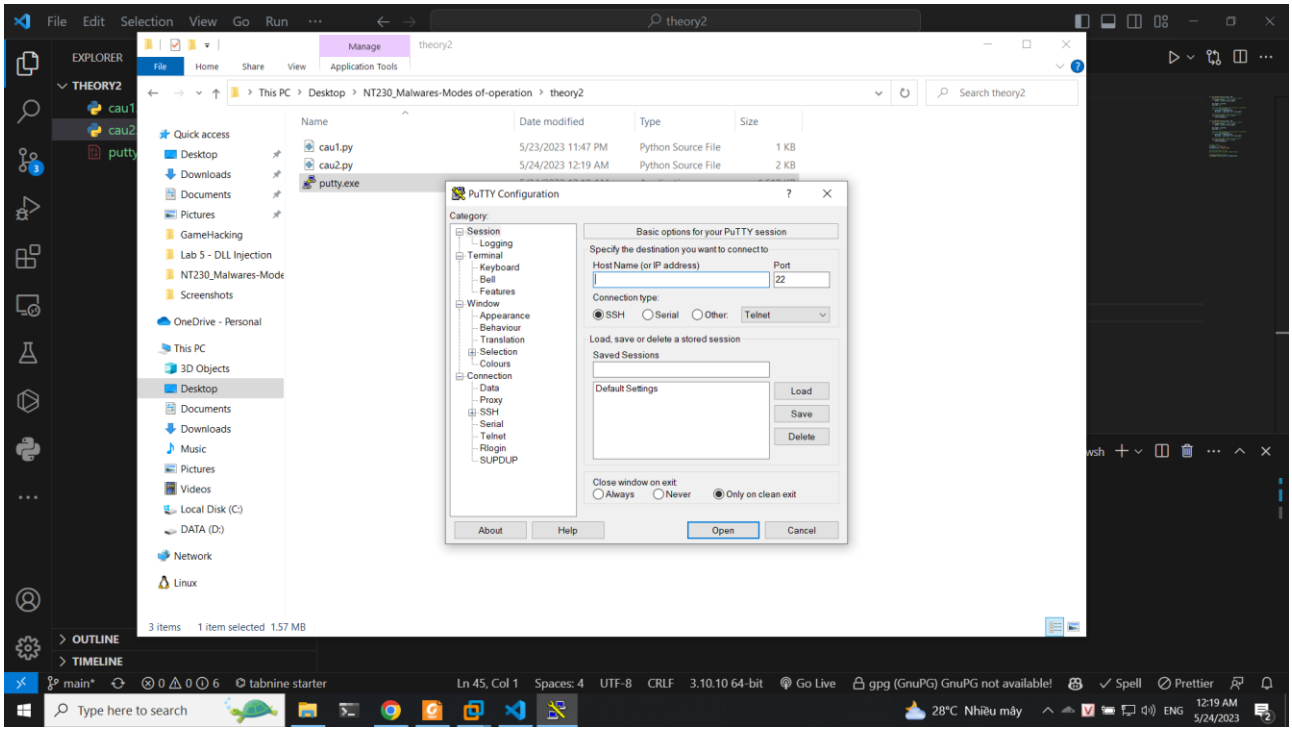
Trước khi thực hiện mã hoá, chương trình hoạt động bình thường



Sau khi thực hiện mã hoá

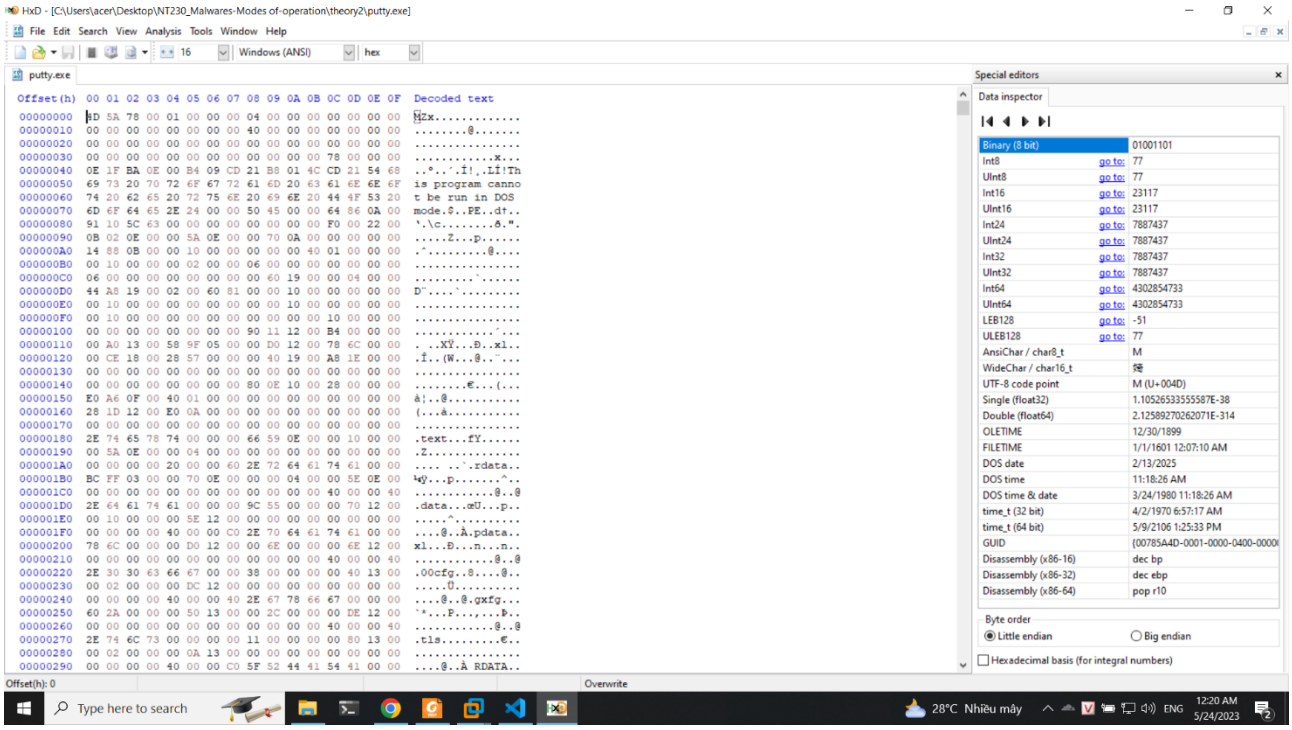


Sau khi thực hiện giải mã trở lại

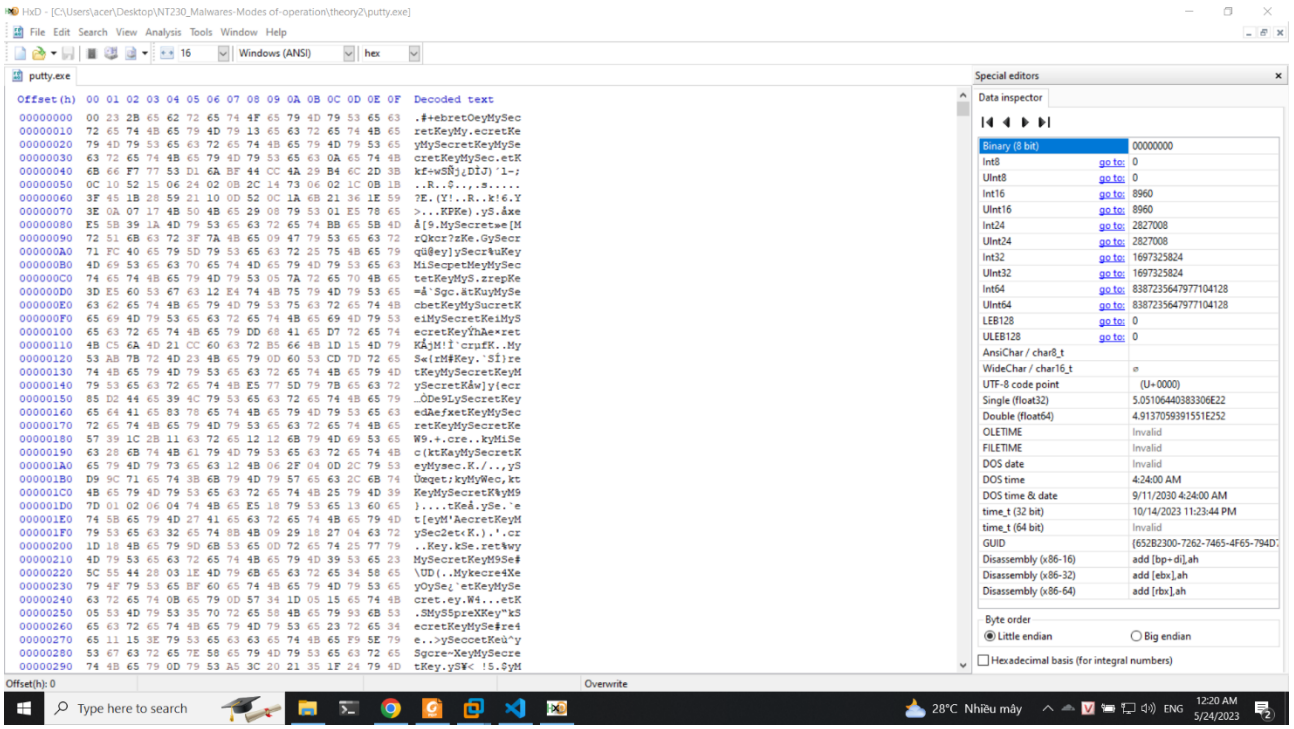


Thực hiện kiểm tra hex

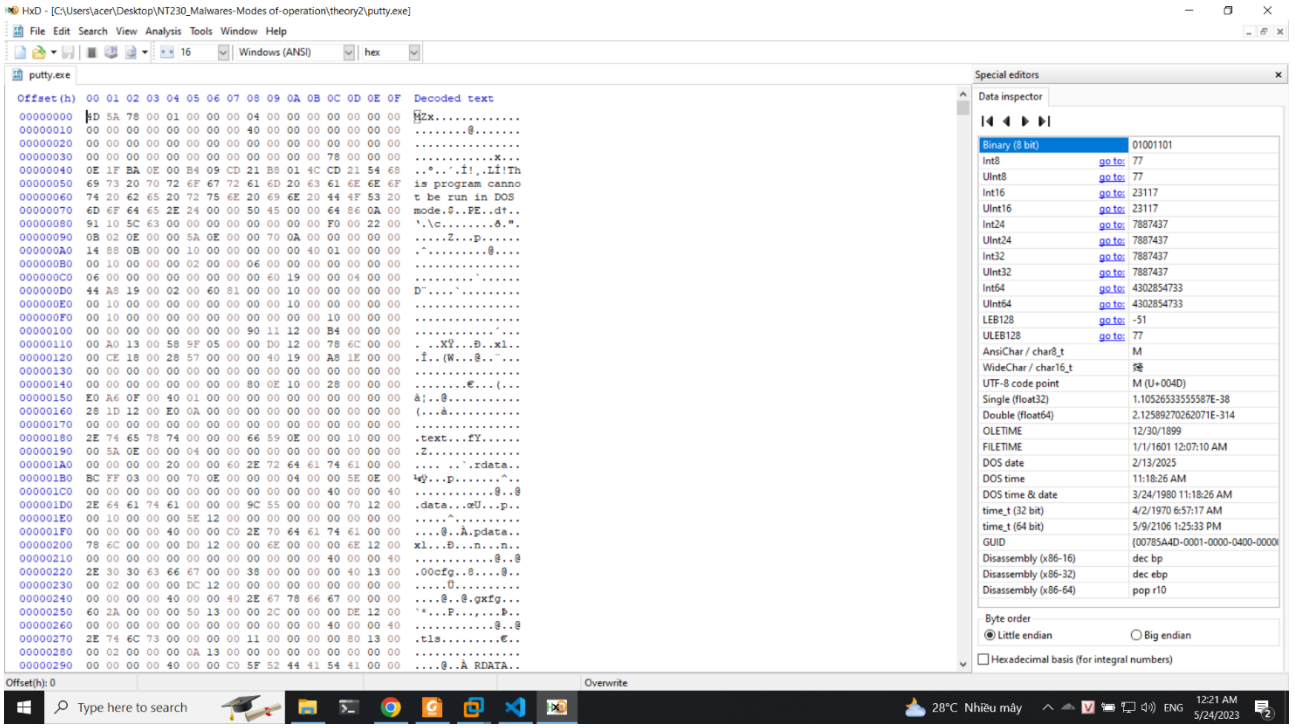
Trước khi mã hoá:



Sau khi thực hiện mã hoá

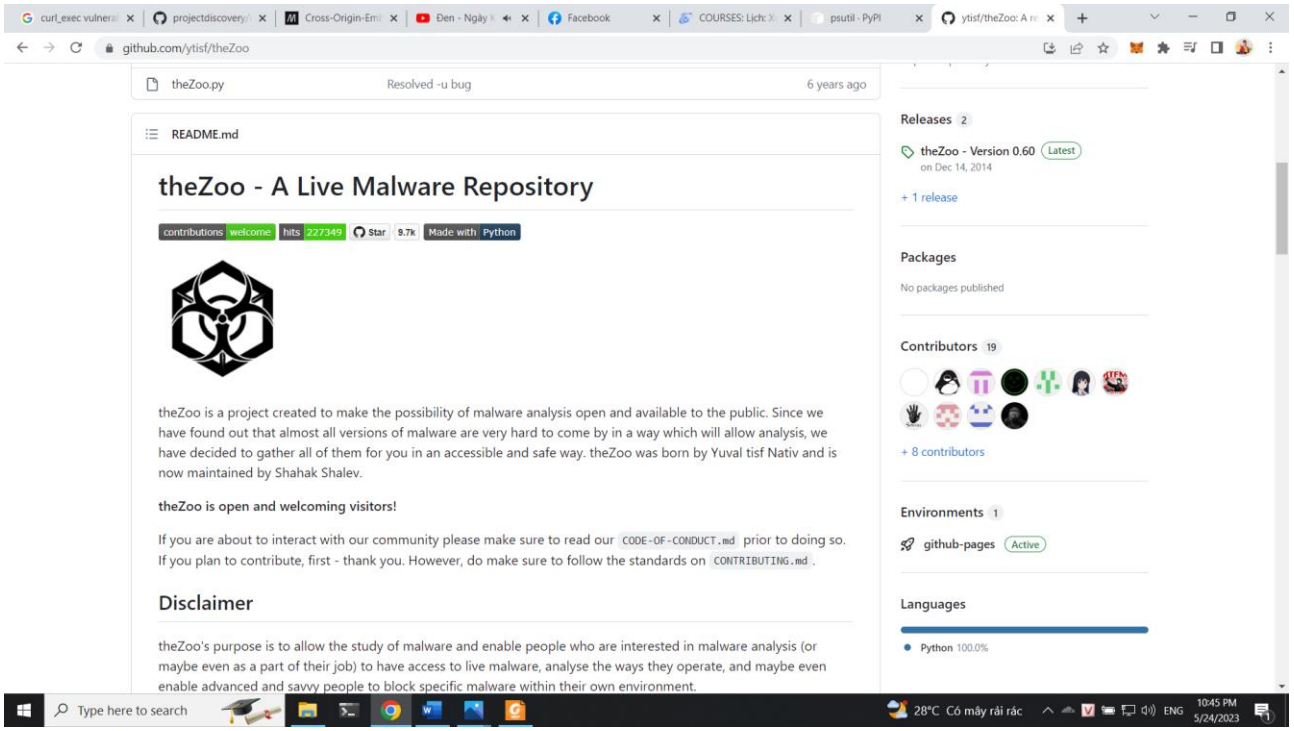


Sau khi thực hiện giải mã

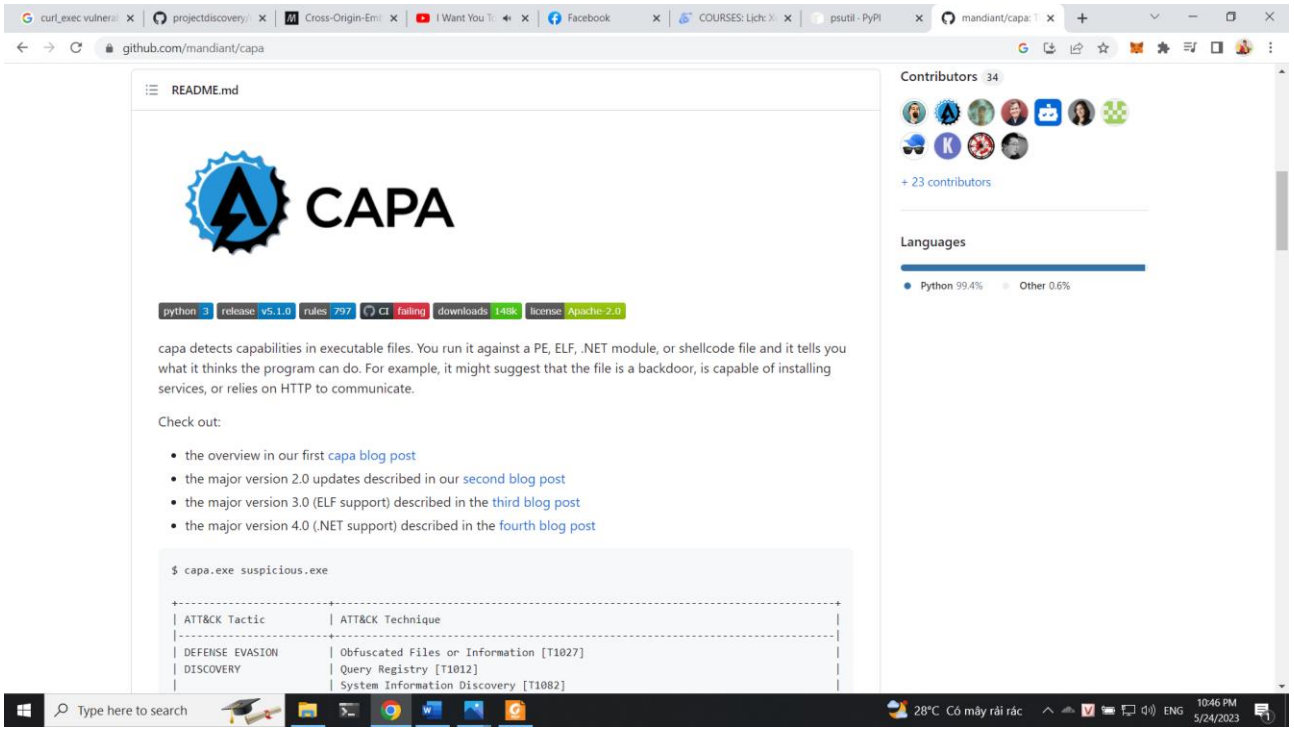


Tiếp tục ta sẽ thực hiện code này để mã hoá virus:

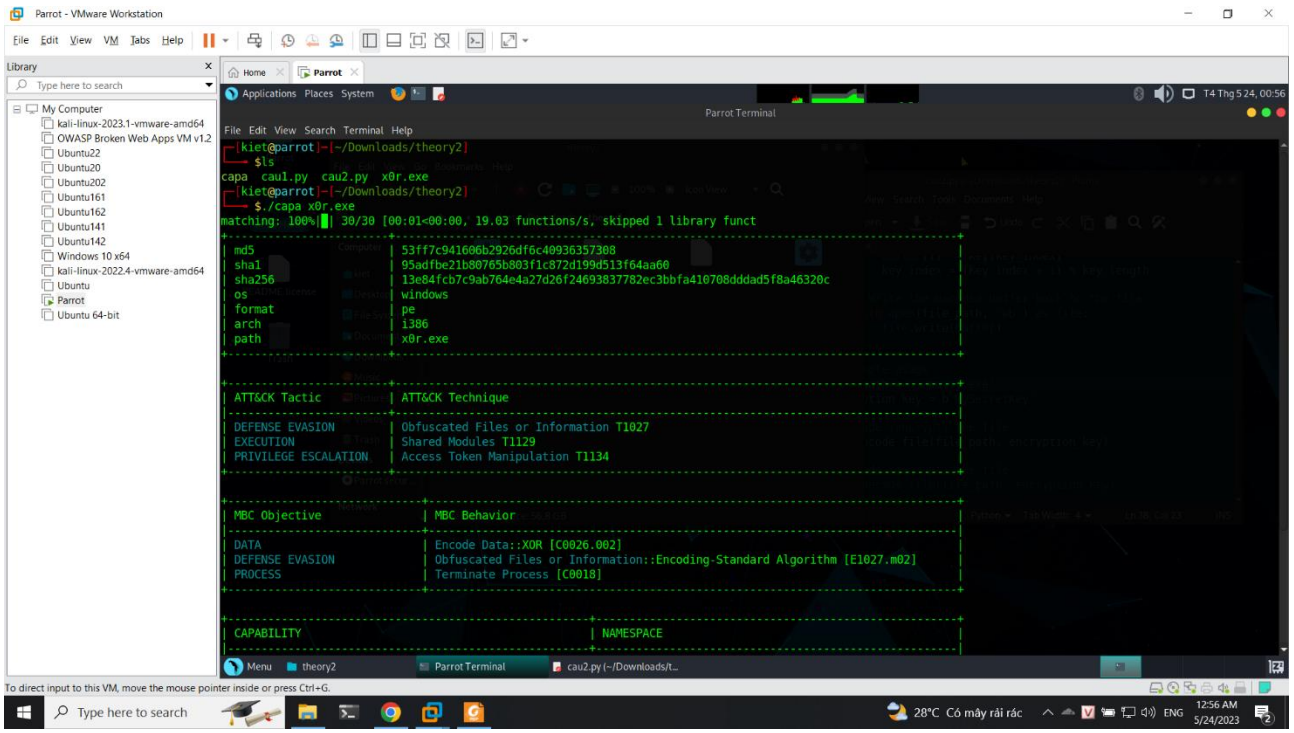
Nguồn virus: https://github.com/ytisf/theZoo



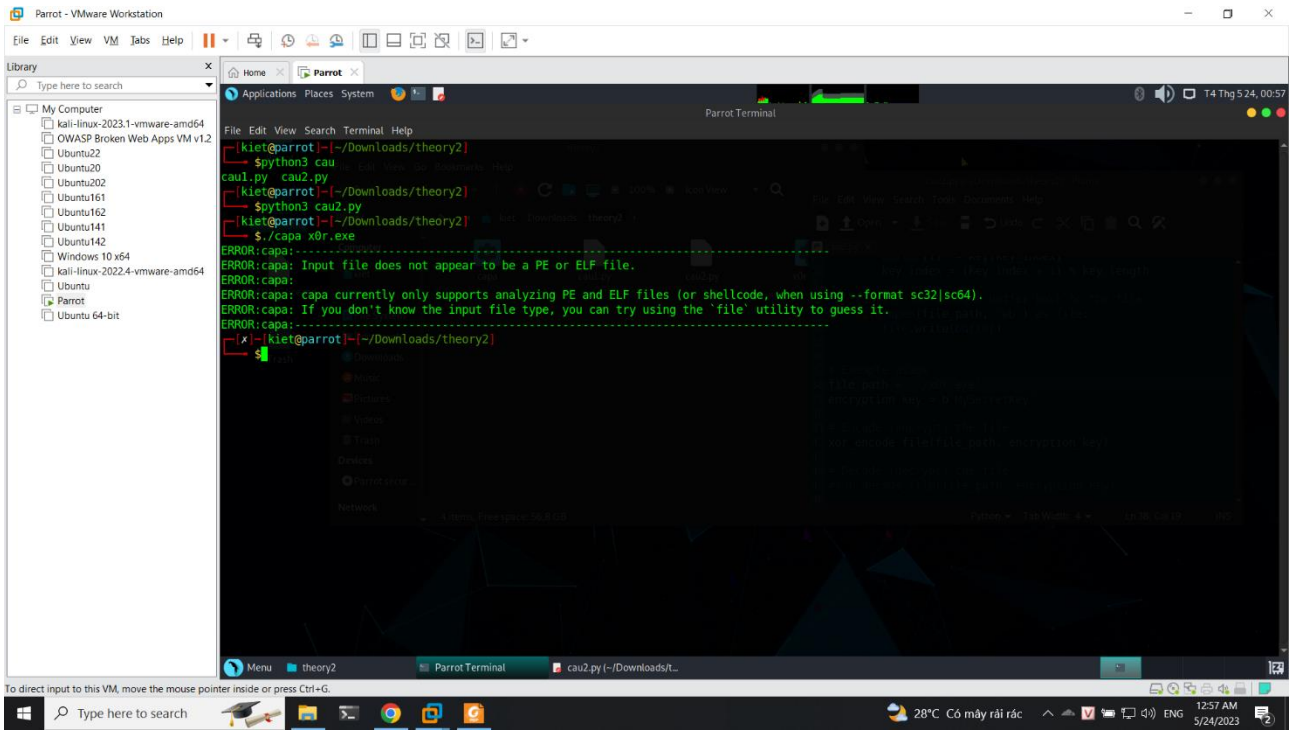
Nguồn tool thực hiện kiểm tra hành vi virus: https://github.com/mandiant/capa



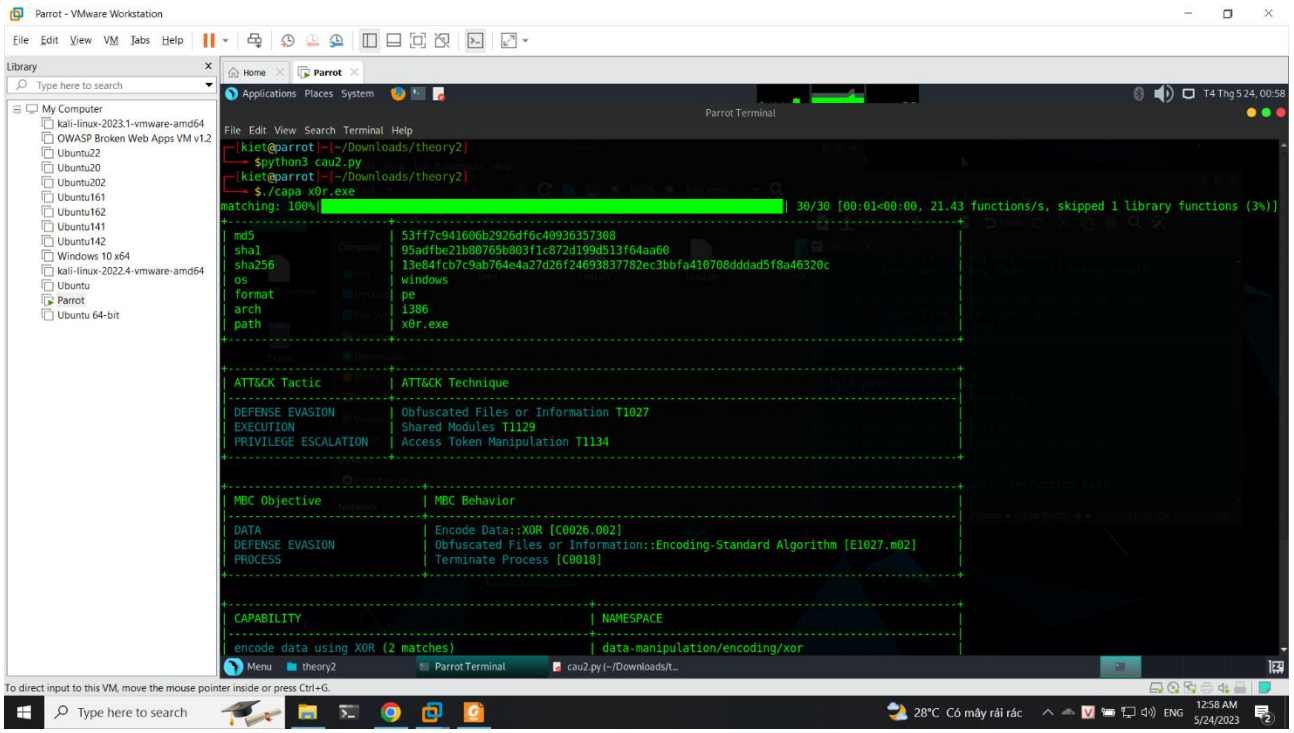
Đầu tiên ta sẽ sử dụng tool để kiểm tra hành vi của virus (phân tích được hành vi)



Thực hiện mã hoá virus và kiểm tra lại hành vi của virus: (đã trốn tránh)



Cuối cùng thực hiện giải mã và kiểm tra lại hành vi của virus (phân tích được hành vi)



Tiếp theo ta cần phải thực hiện chuyển đổi code

Python → C → bytecode

Từ đó thực hiện truyền vào chương trình ở Ex01 để thực hiện tiêm vào chương trình.

Nhưng bước này tụi em thực hiện chưa tốt nên chưa thể hoàn thành yêu cầu này

Các bước thực hiện/ Phương pháp thực hiện/Nội dung tìm hiểu (Ảnh chụp màn hình, có giải thích)

Sinh viên đọc kỹ yêu cầu trình bày bên dưới trang này

YÊU CẦU CHUNG

- Sinh viên tìm hiểu và thực hiện bài tập theo yêu cầu, hướng dẫn.
- Nộp báo cáo kết quả chi tiết những việc (**Report**) bạn đã thực hiện, quan sát thấy và kèm ảnh chụp màn hình kết quả (nếu có); giải thích cho quan sát (nếu có).
- Sinh viên báo cáo kết quả thực hiện và nộp bài.

Báo cáo:

- File .DOCX và .PDF. Tập trung vào nội dung, không mô tả lý thuyết.
- Nội dung trình bày bằng Font chữ Times New Romans/ hoặc font chữ của mẫu báo cáo này (UTM Neo Sans Intel/UTM Viet Sach)– cỡ chữ 13. Canh đều (Justify) cho văn bản. Canh giữa (Center) cho ảnh chụp.
- Đặt tên theo định dạng: [Mã lớp]-ExeX_GroupY. (trong đó X là Thứ tự Bài tập, Y là mã số thứ tự nhóm trong danh sách mà GV phụ trách công bố).

  *Ví dụ: [*NT101.K11.ANTT*]-Exe01_Group03.*
- Nếu báo cáo có nhiều file, nén tất cả file vào file .ZIP với cùng tên file báo cáo.
- Không đặt tên đúng định dạng – yêu cầu, sẽ **KHÔNG** chấm điểm bài nộp.
- Nộp file báo cáo trên theo thời gian đã thống nhất tại courses.uit.edu.vn.

Đánh giá:

- Hoàn thành tốt yêu cầu được giao.
- Có nội dung mở rộng, ứng dụng.

Bài sao chép, trễ, … sẽ được xử lý tùy mức độ vi phạm.

HẾT