**BÁO CÁO THỰC HÀNH LAB 3**

Môn học: Cơ chế hoạt động của mã độc

Tên chủ đề: Windows Service

*GVHD: Nguyễn Hữu Quyền*

1. **THÔNG TIN CHUNG:**

*(Liệt kê tất cả các thành viên trong nhóm)*

Lớp: NT230.N21.ATCL

|  |  |  |  |
| --- | --- | --- | --- |
| STT | Họ và tên | MSSV | Email |
| 1 | Bạch Văn Xuân Thông | 20521978 | 20521978@gm.uit.edu.vn |
| 2 | Trần Tấn Tài | 20521862 | 20521862@gm.uit.edu.vn |
| 3 | Phạm Bá Tín | 20522016 | 20522016@gm.uit.edu.vn |

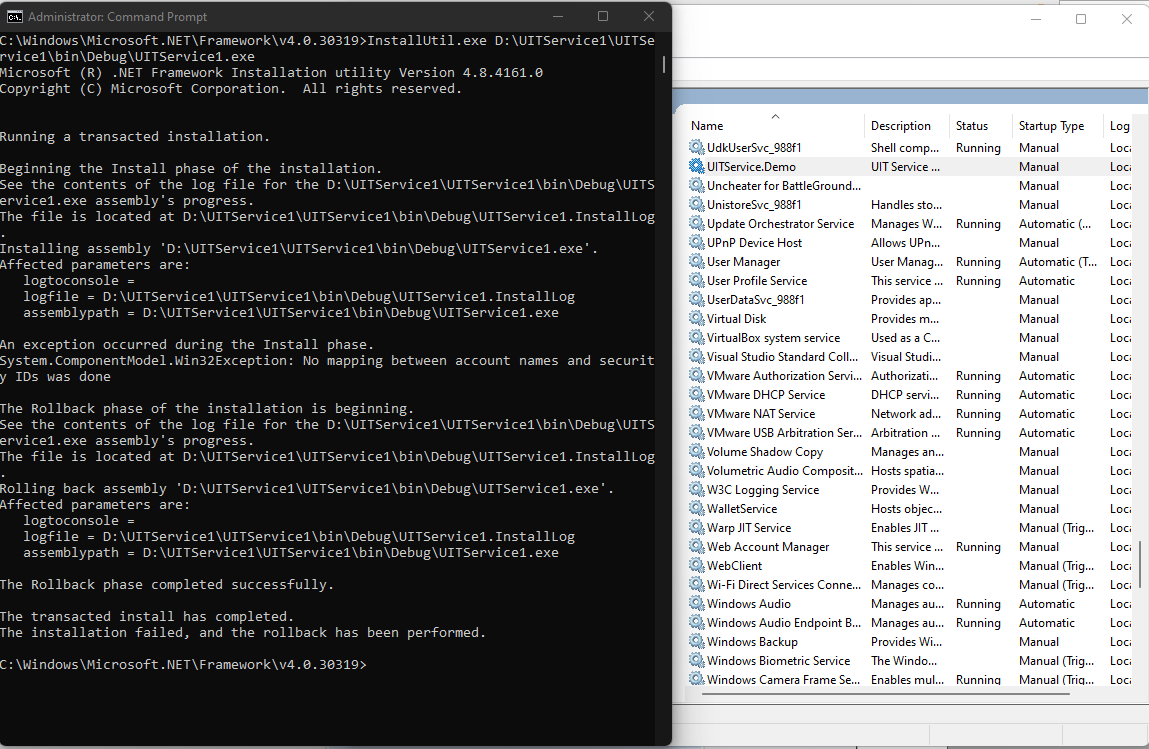
1. **NỘI DUNG THỰC HIỆN:[[1]](#footnote-0)**

|  |  |  |
| --- | --- | --- |
| STT | Công việc | Kết quả tự đánh giá |
| 1 | Bài thực hành 1 | 100% |
| 2 | Bài thực hành 2 | 100% |
| 3 | Bài thực hành 3 | 100% |

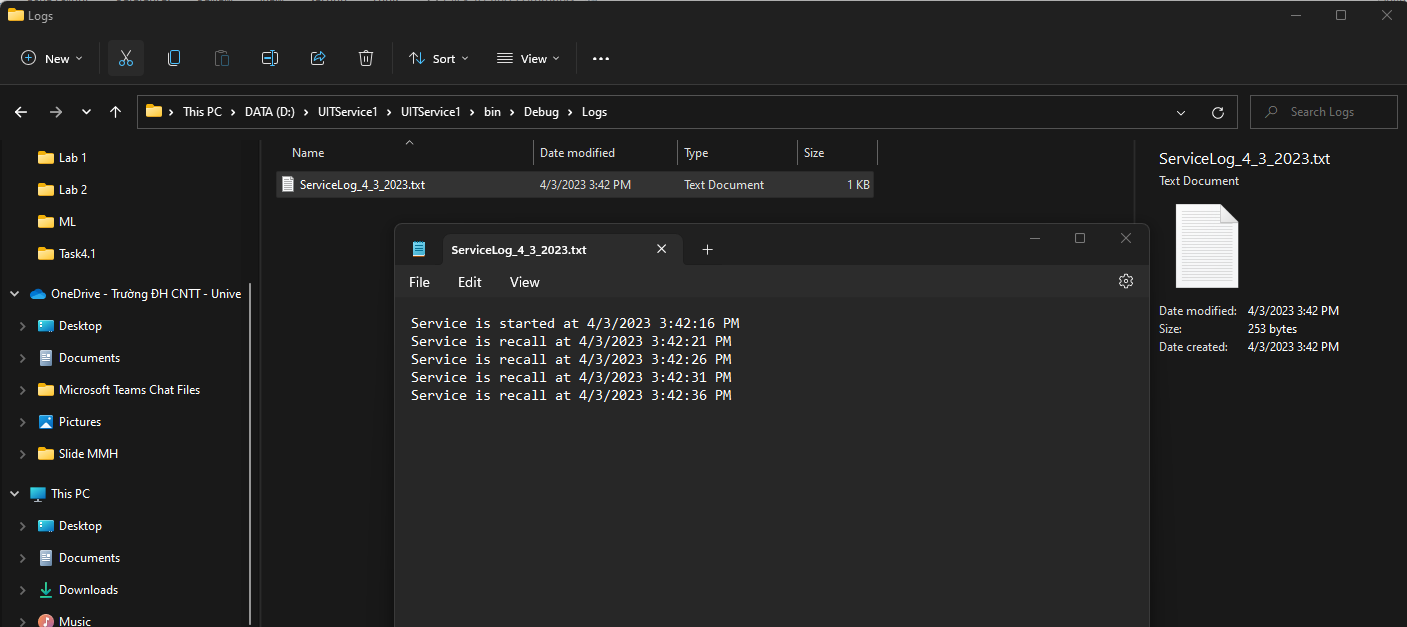
Phần bên dưới của báo cáo này là tài liệu báo cáo chi tiết của nhóm thực hiện.

**Báo cáo chi tiết**

Sau khi thực hiện theo các bước hướng dẫn, ta đã tạo được tạo và cài đặt thành công 1 windows service



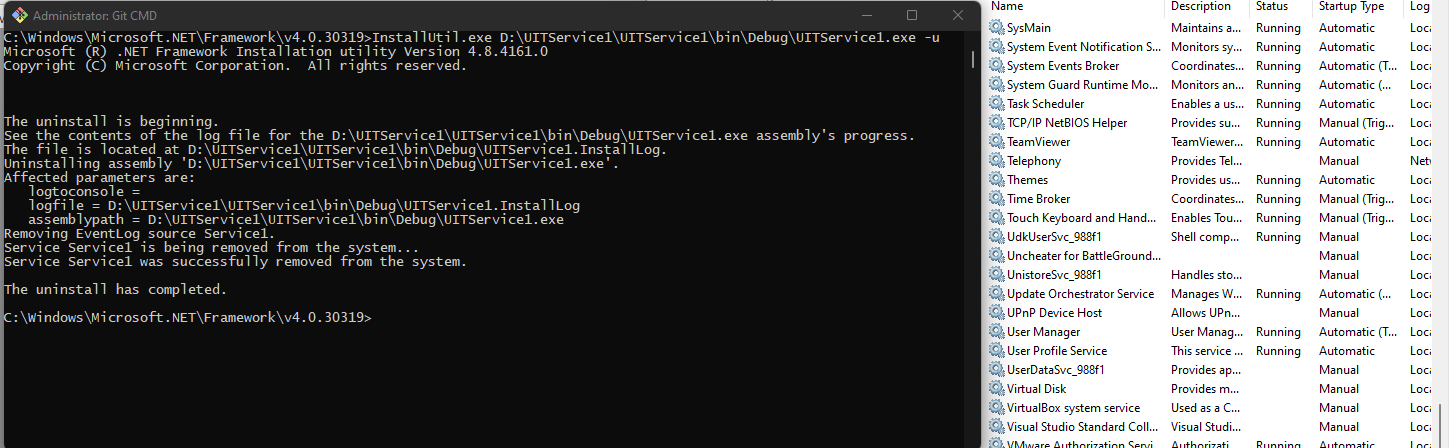
Thử start service, kết quả thu được là tập tin ghi log đã được tạo ra theo đường dẫn ta quy định:



**Bài thực hành 1: Sinh viên trình bày cách gỡ cài đặt Window service trên**

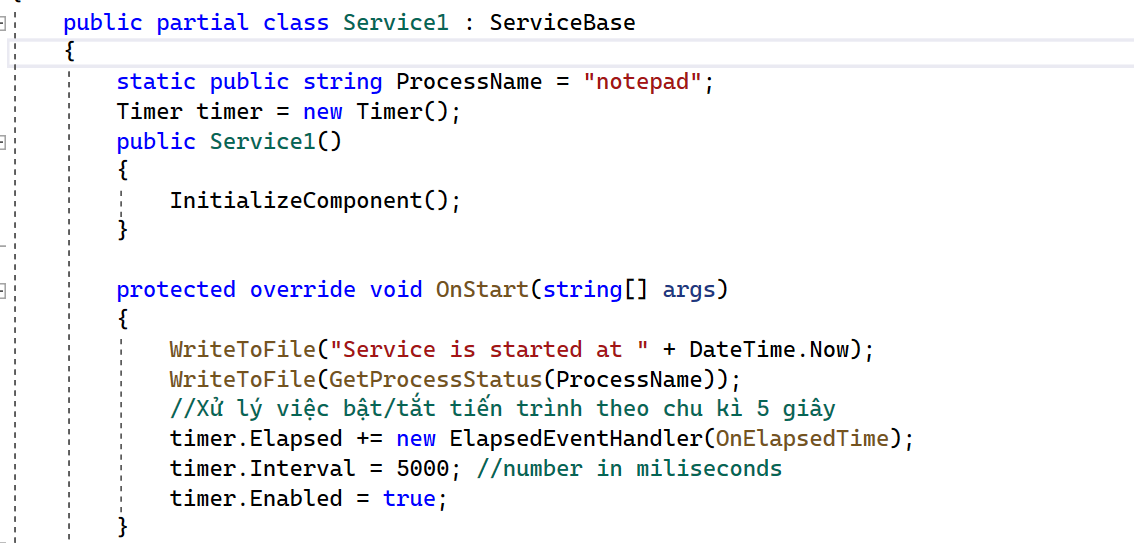
Chỉ cần chạy dòng lệnh theo cấu trúc

InstallUtil.exe D:\UITService1\UITService1\bin\Debug\UITService1.exe -u là có thể gỡ được Window service trên

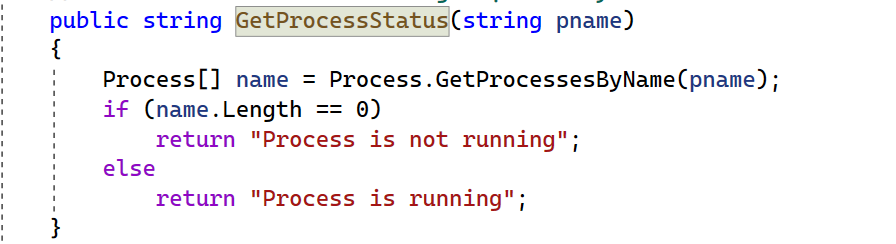


**Bài thực hành 2: Viết một Windows service có nhiệm vụ kiểm tra một “process” ở trạng thái hoạt động** run/stop **hay không và** run/stop **“process” theo một lịch biểu**

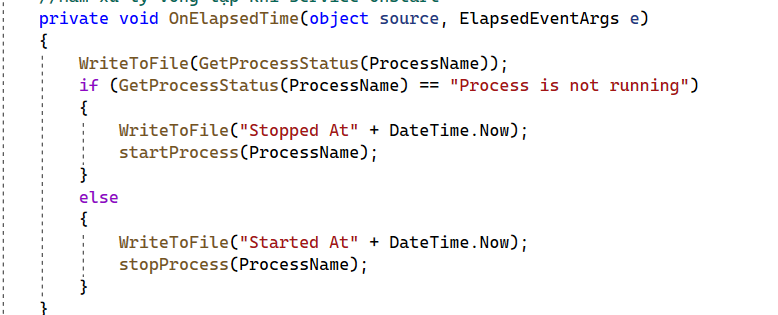
Thực hiện với process là notepad và set thời gian bật/tắt process là 5000ms



Hàm kiểm tra process bật hay tắt



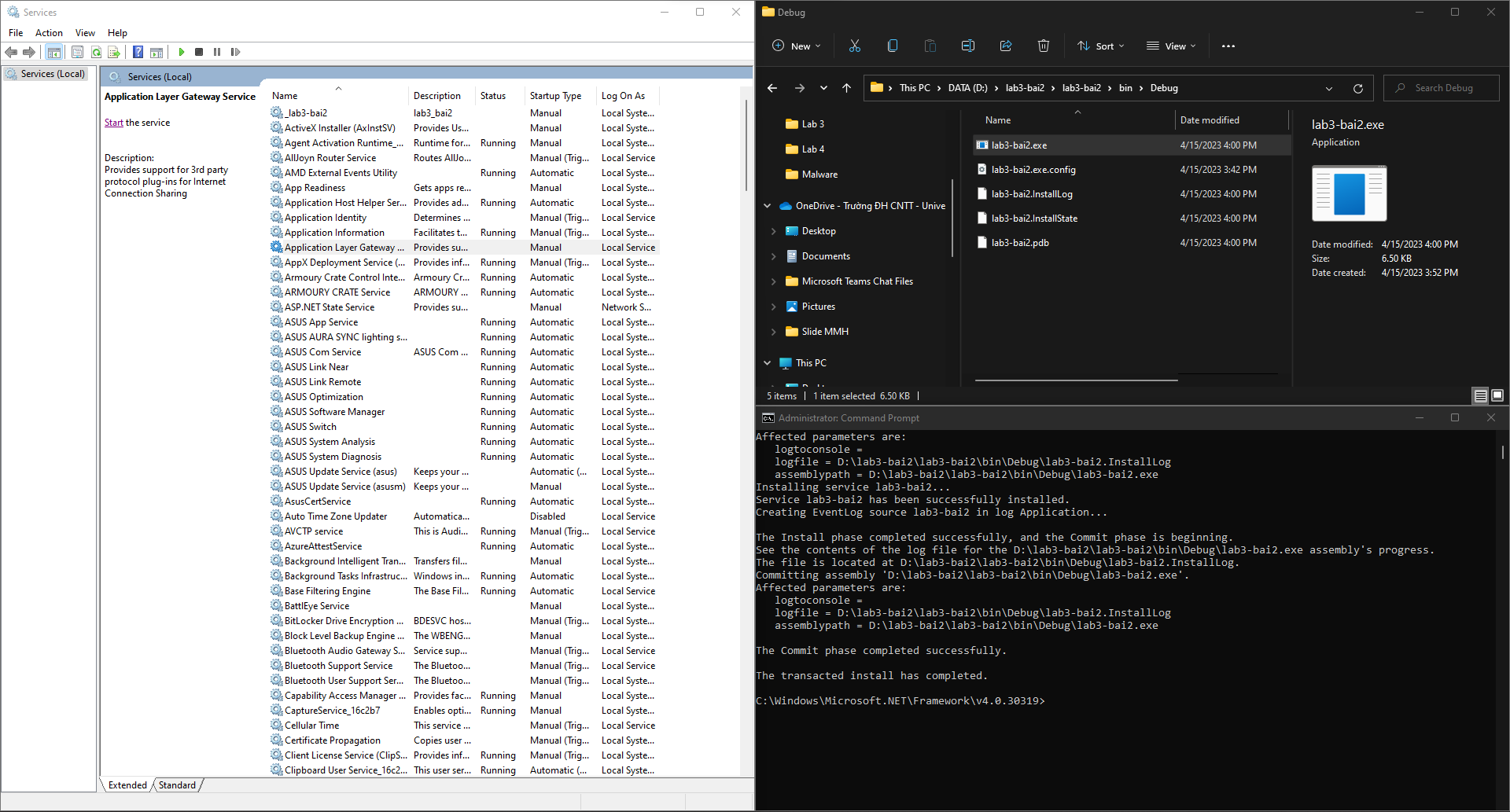
Hàm xử lý vòng lặp bật/tắt process khi service onStart



Tạo file log và ghi vào tập tin log trạng thái của process



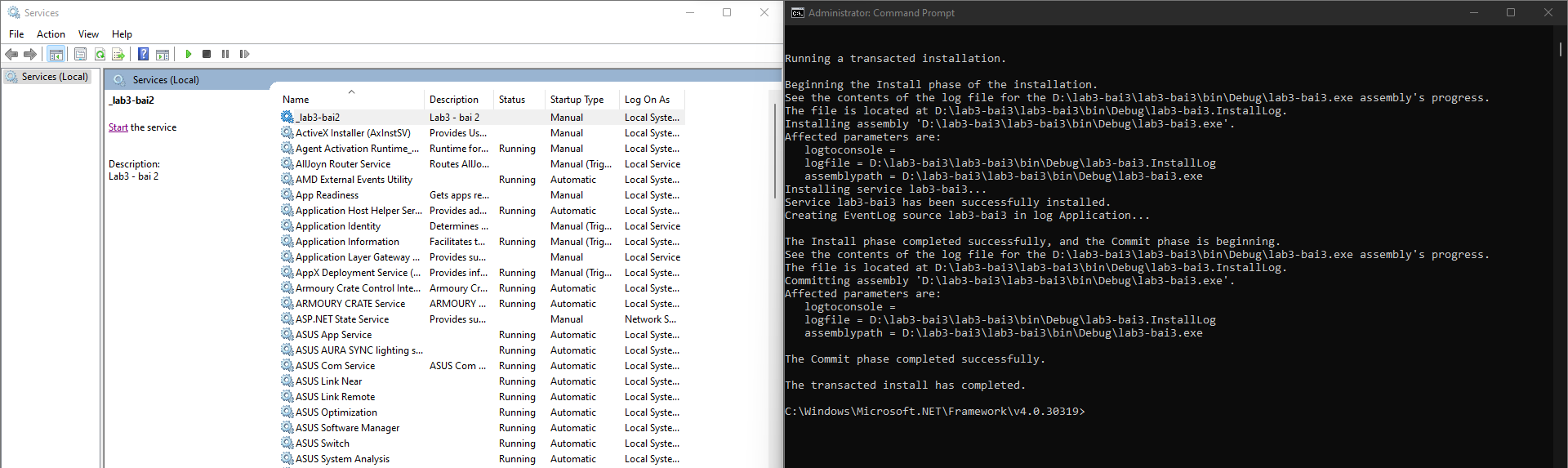
Ta cài đặt thành công Windows service với nhiệm vụ được yêu cầu



Kết quả khi khởi động windows service xem chi tiết tại https://www.youtube.com/watch?v=g1dwgegZC0k

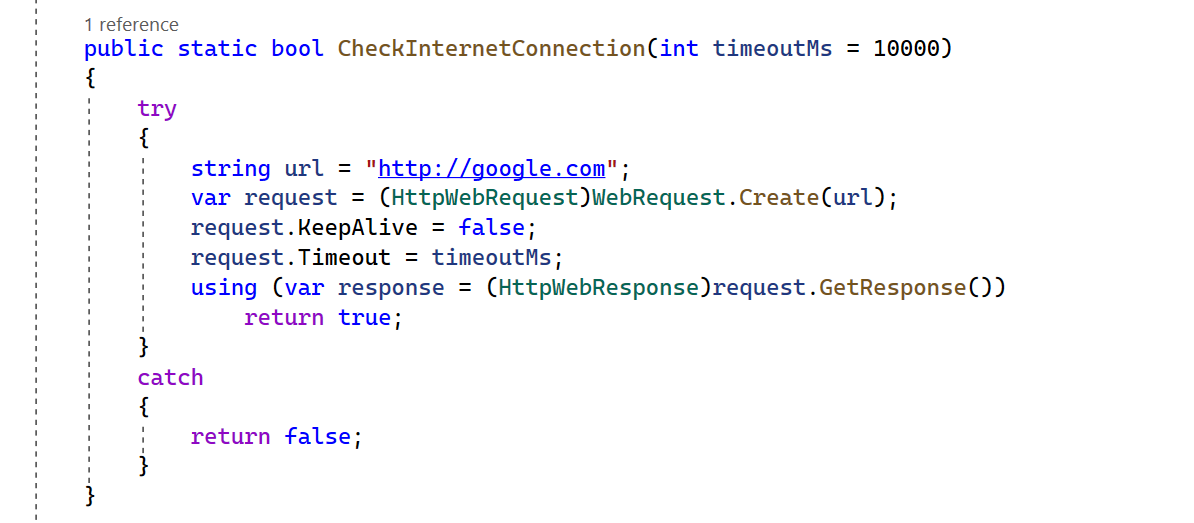
**Bài thực hành 3: Viết một Windows service có nhiệm vụ kiểm tra kết nối internet của  
máy hiện tại (HTTP) và tạo reverse shell đơn giản.**

Cài đặt thành công Windows service

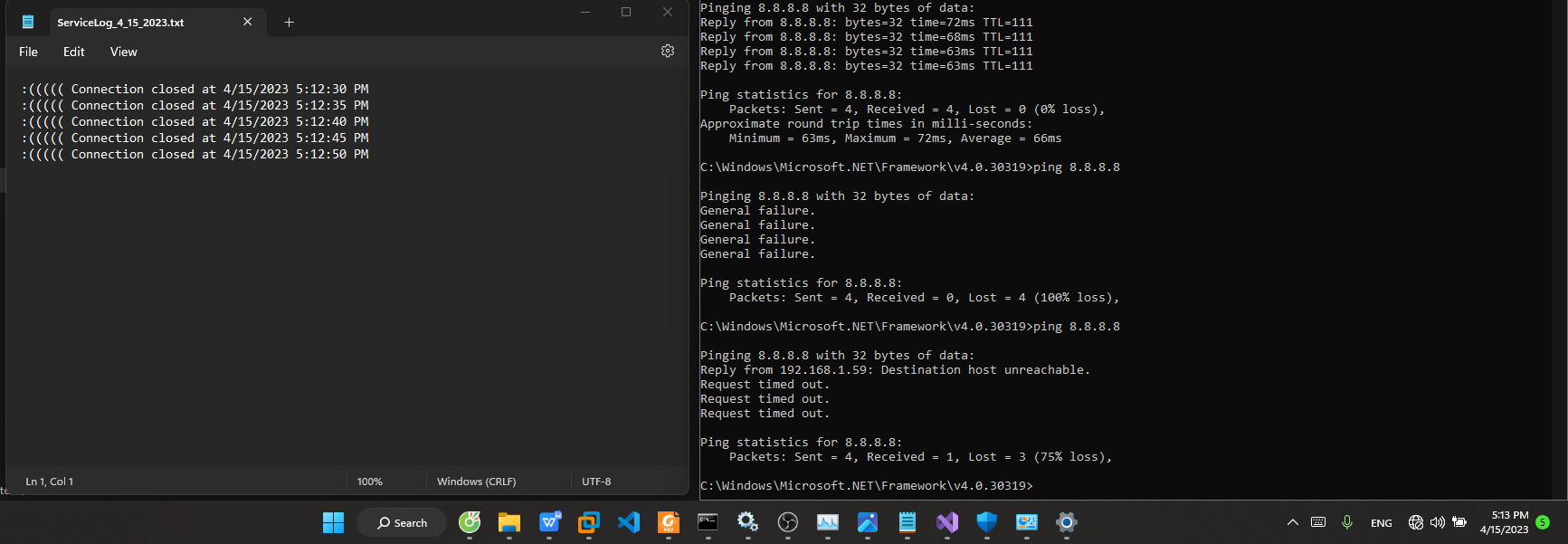


**\*Kiểm tra kết nối Internet**

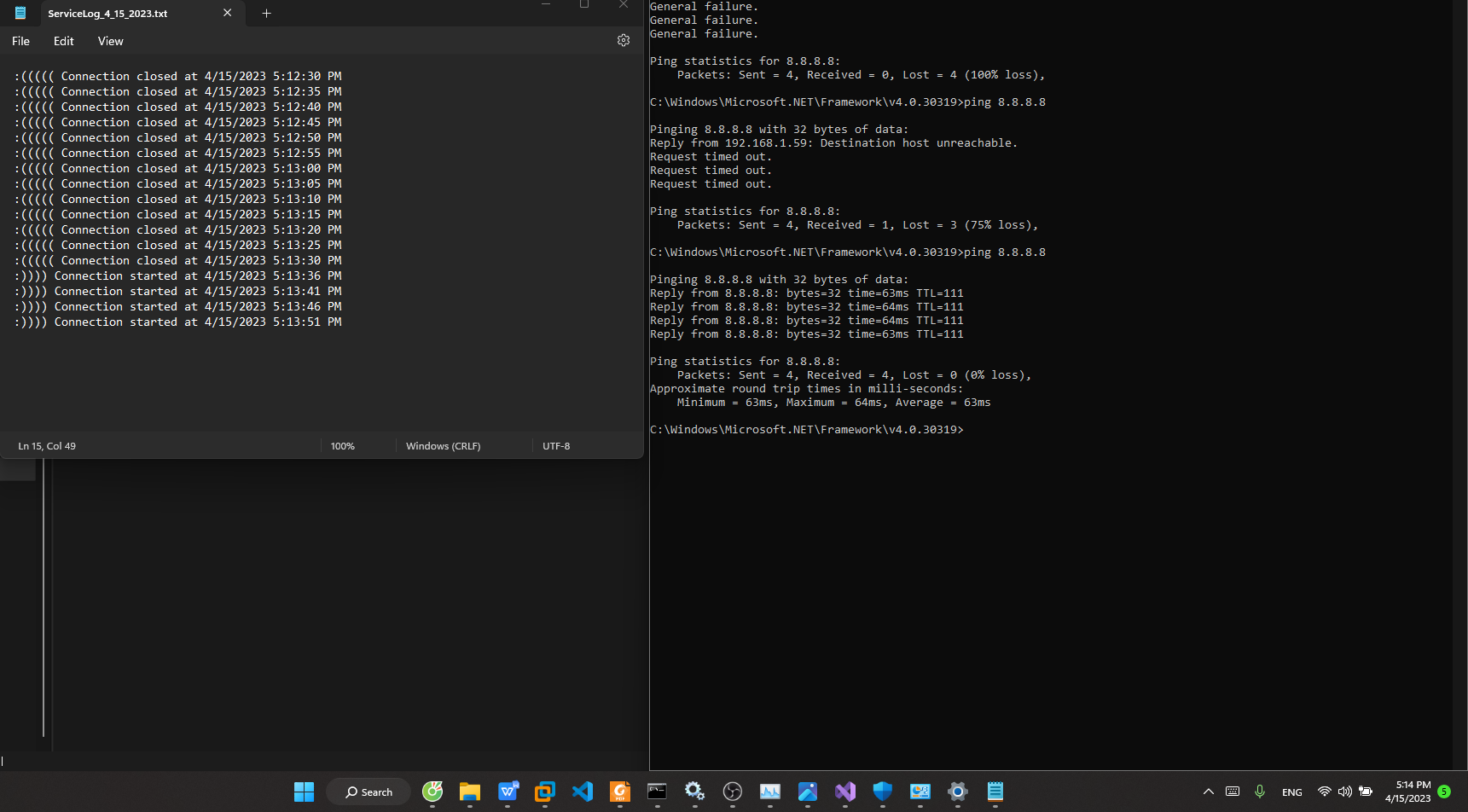
Để kiểm tra kết nối Internet, ta sử dụng HttpWebRequest để tạo request đến google.com



Tắt internet và ping google.com để xem kết quả. Kiểm tra folder Log và file log ta thấy services đã hoạt động

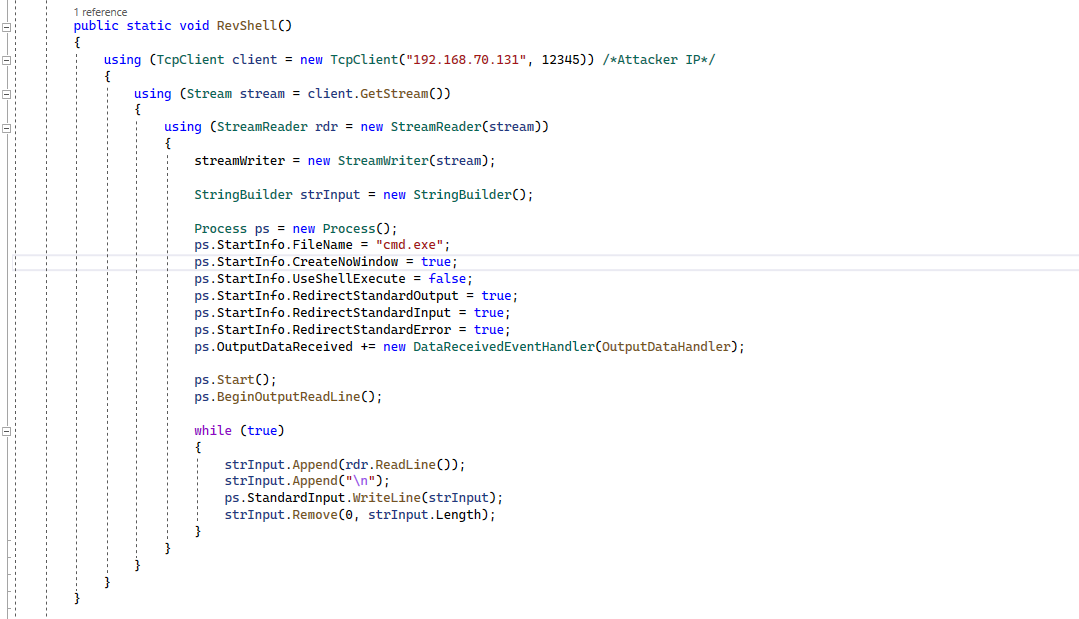


Bật lại kết nối Internet, ping google.com và kiểm tra file log

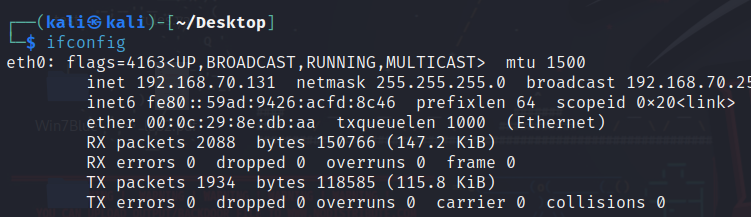
****

**\*Thực hiện tạo reverse shell**

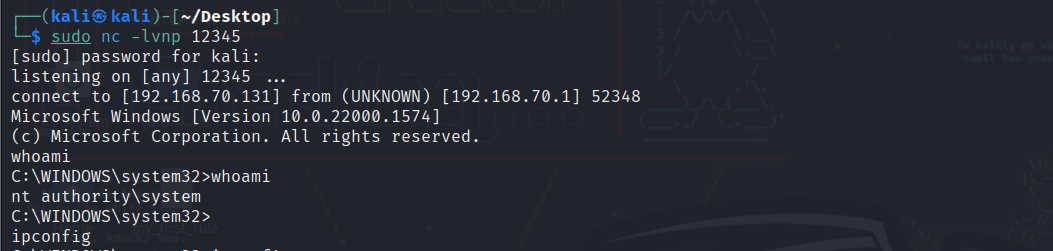
Sử dụng TcpClient với IP và port của attacker để thiết lập kết nối. Sử dụng StreamReader và StreamWriter để đọc và ghi luồng. Sử dụng Process để thiết lập tiến trình kết nối đến Command Line của máy nạn nhân cho attacker (cmd.exe)



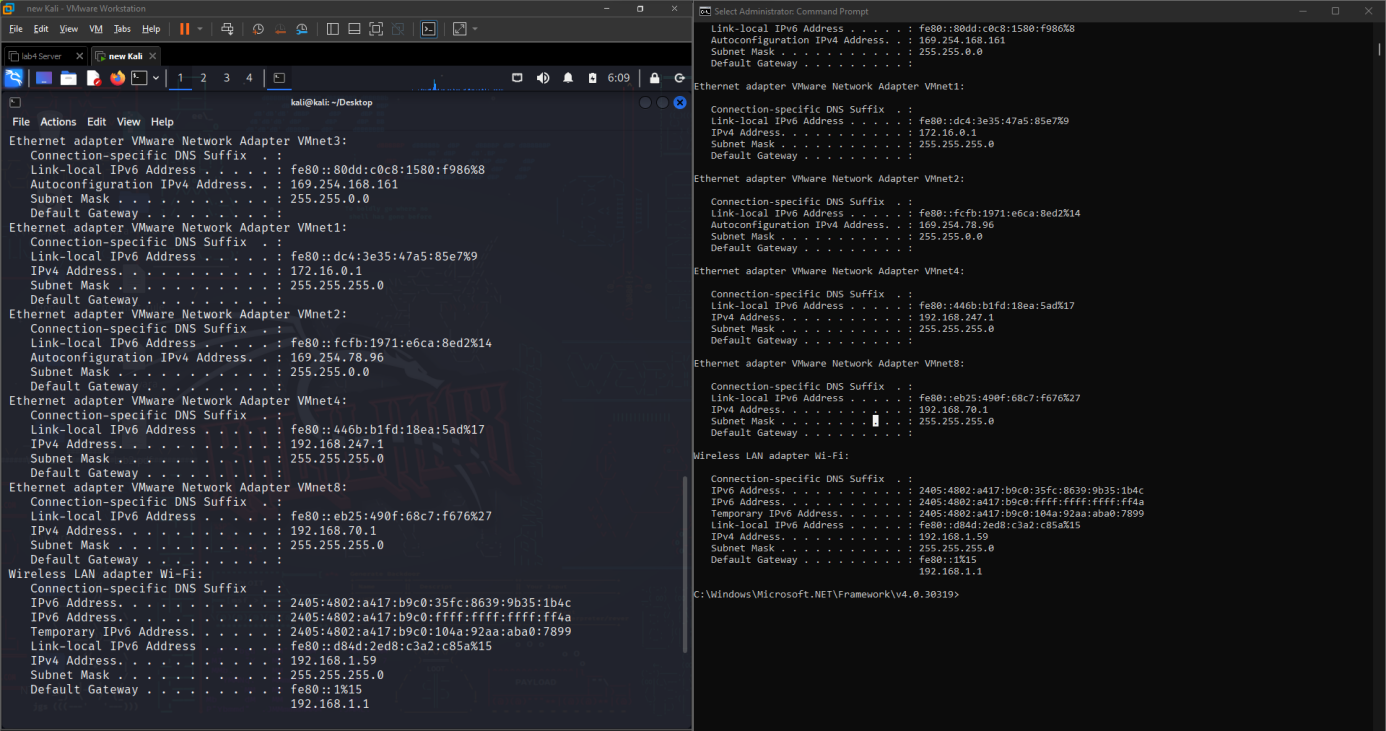
IP của attacker

  
Lúc này, khi bật services. OnElapsedTime sẽ kiểm tra kết nối Internet, nếu có, nó thực thi hàm RevShell(). Lúc này, ta có thể kết nối với Shell của nạn nhân

Thực hiện lắng nghe trên port 12345 ở máy attacker. Sau khi reset lại service thì sẽ tạo một connect tới shell máy victim



Kiểm tra lại bằng lệnh ipconfig



Reverse shell đã thiết lập thành công

Xem chi tiết tại https://www.youtube.com/watch?v=sDyzgC25QOs

1. Ghi nội dung công việc, các kịch bản trong bài Thực hành [↑](#footnote-ref-0)