BÁO CÁO THỰC HÀNH

**Môn học: Cơ chế hoạt động của mã độc**

**Kỳ báo cáo: Buổi 01 (Session 01)**

**Tên chủ đề: Windows Service**

*GVHD: Nghi Hoàng Khoa*

*Ngày báo cáo: 3/07/2021*

1. **THÔNG TIN CHUNG:**

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

Lớp: NT230.L21.ANTT.1

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Họ và tên** | **MSSV** | **Email** |
| 1 | Nguyễn Hoàng Đông | 16520222 | 16520222@gm.uit.edu.vn |

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

|  |  |  |
| --- | --- | --- |
| **STT** | **Công việc** | **Kết quả tự đánh giá** |
| 1 | Yêu cầu 01 | 100% |
| 2 | Yêu cầu 02 | 100% |
| 3 | Yêu cầu 03 | 100% |

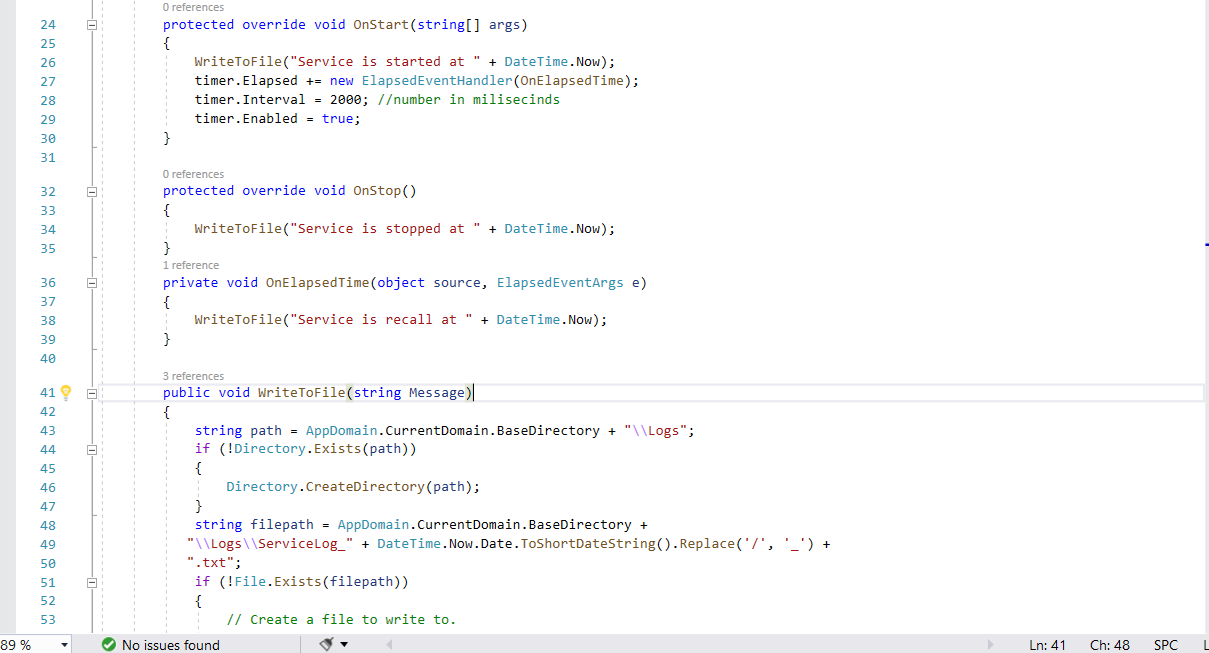
**Phần bên dưới của báo cáo này là tài liệu báo cáo chi tiết của nhóm thực hiện.**

BÁO CÁO CHI TIẾT

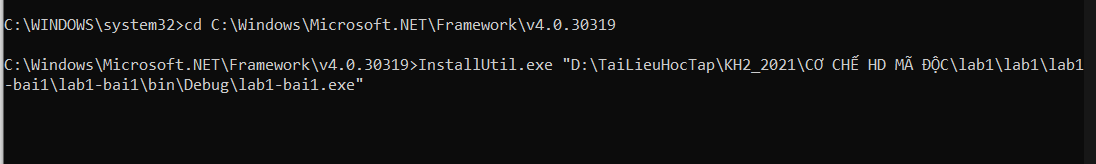
**Bài tập về nhà**

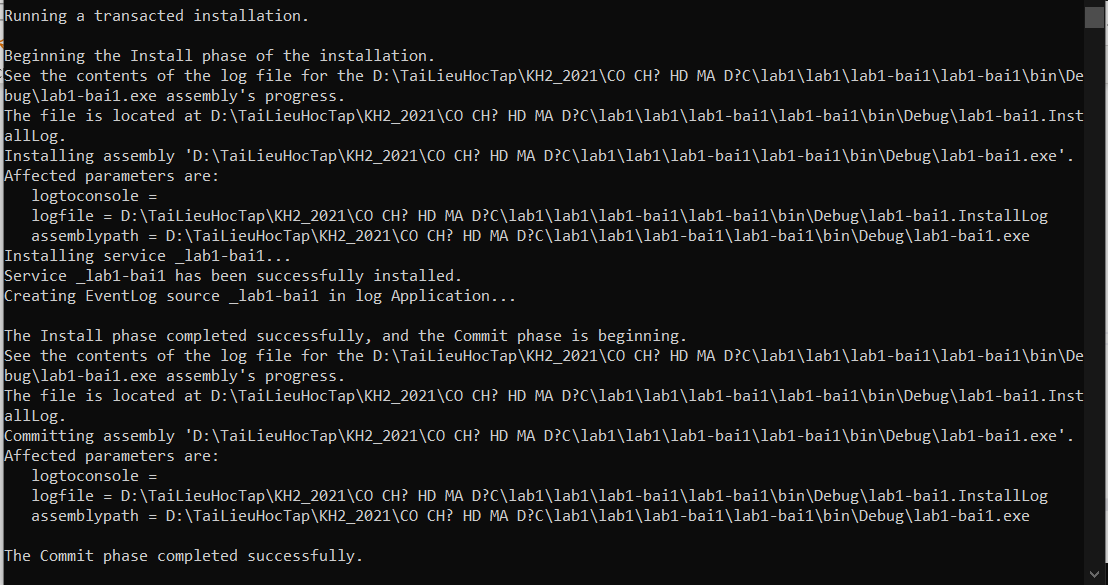
**Bài thực hành 1**: **Sinh viên trình bày cách gỡ cài đặt Window service trên**

* Đầu tiên ta tiến hành code như lab để tạo 1 services có chức năng ghi lại thời gian chạy chu kỳ 2s

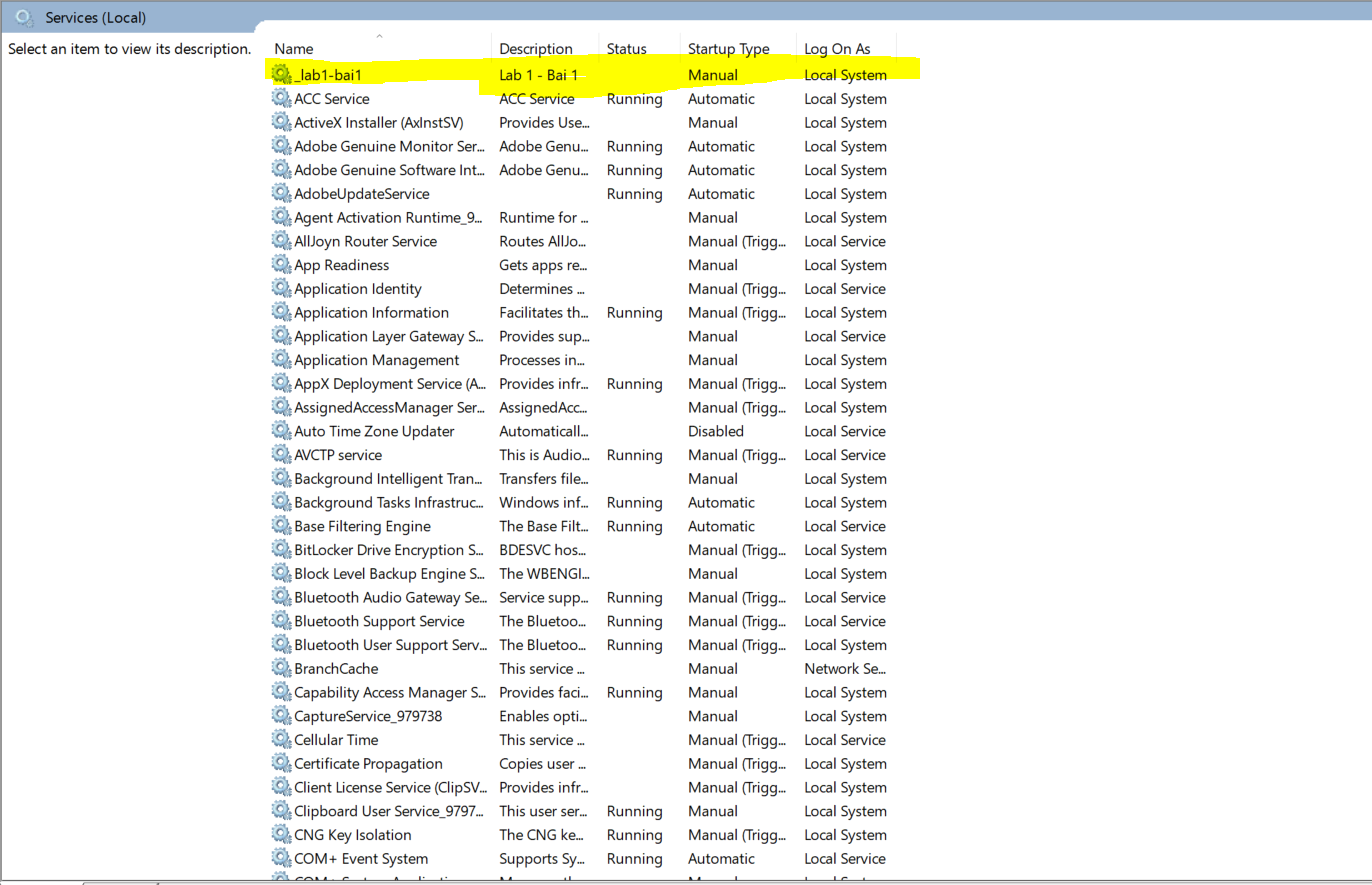


* Tiến hành cài đặt services



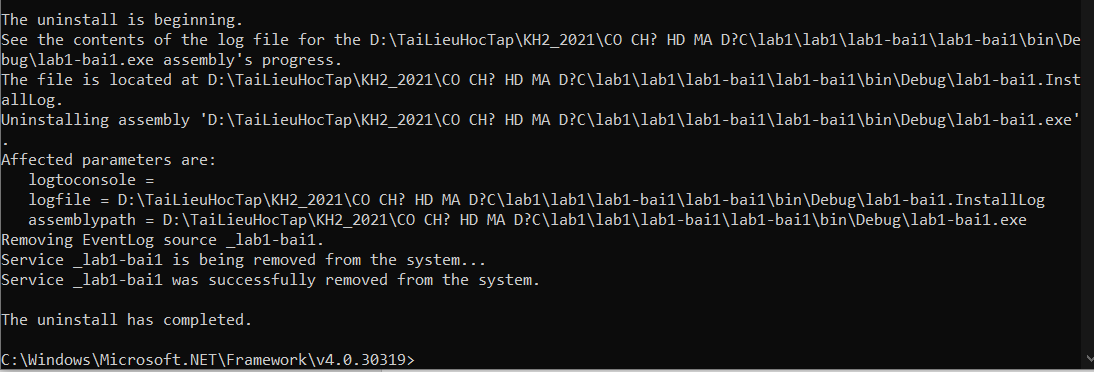


* Vào service window kiểm tra lại



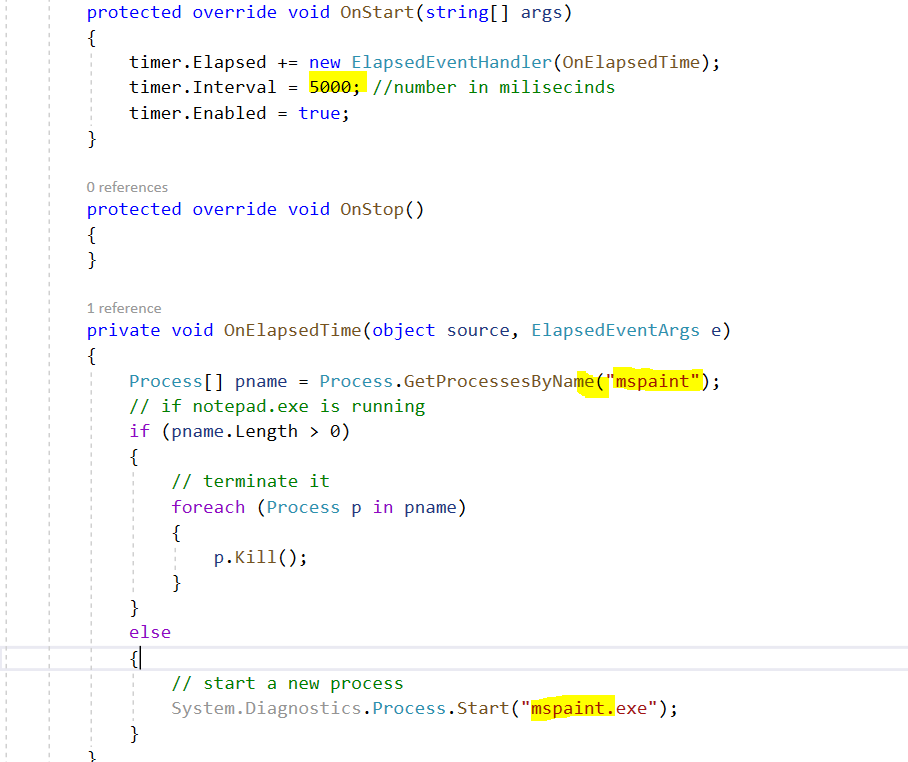
* Để gỡ tiến trình ta dung lệnh như cài đặt them -u để gỡ



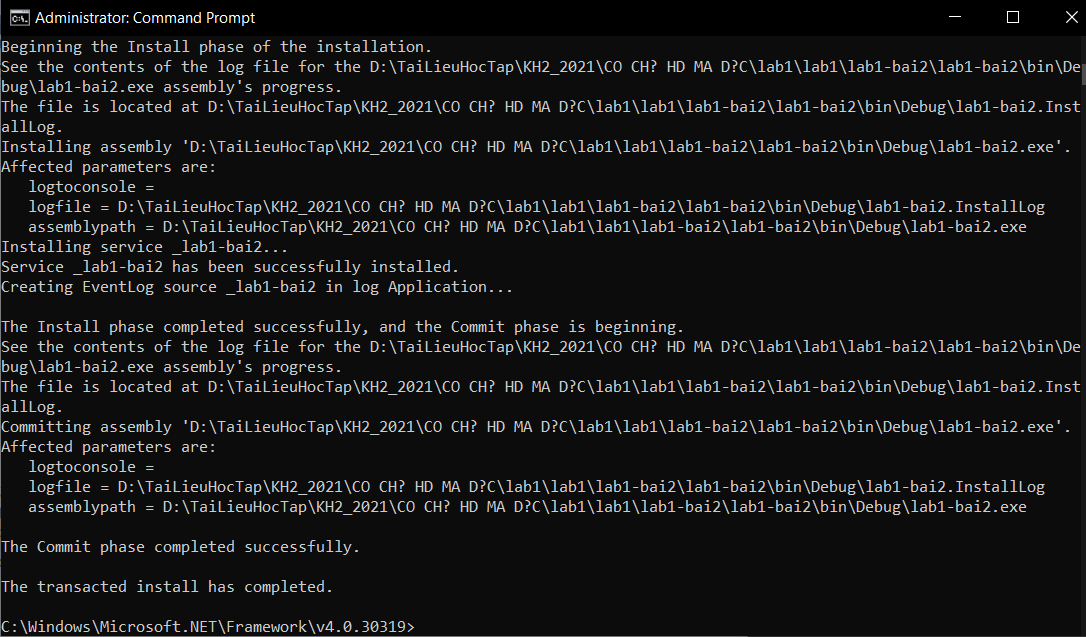


**Bài thực hành 2: Viết một Windows service có nhiệm vụ kiểm tra một “process” ở trạng thái hoạt động run/stop hay không và run/stop “process” theo một lịch biểu**.

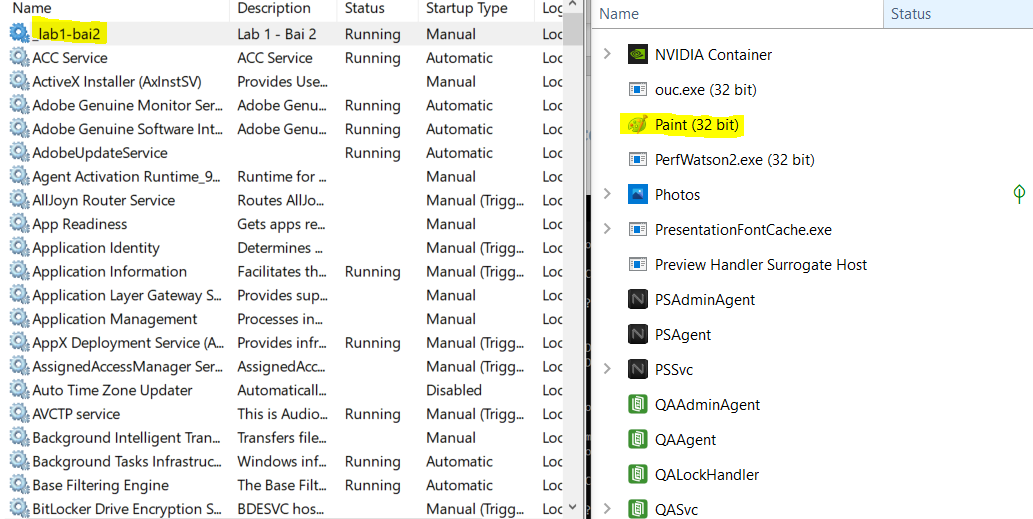
* Sau đây ta sẽ viết 1 tiến trình kiểm tra process Paint của window có hoạt động hay không. Nếu hoạt động ta tiến hành kill nó, ngược lại ta tiến hành chạy process đó theo 1 lịch biểu 5s .



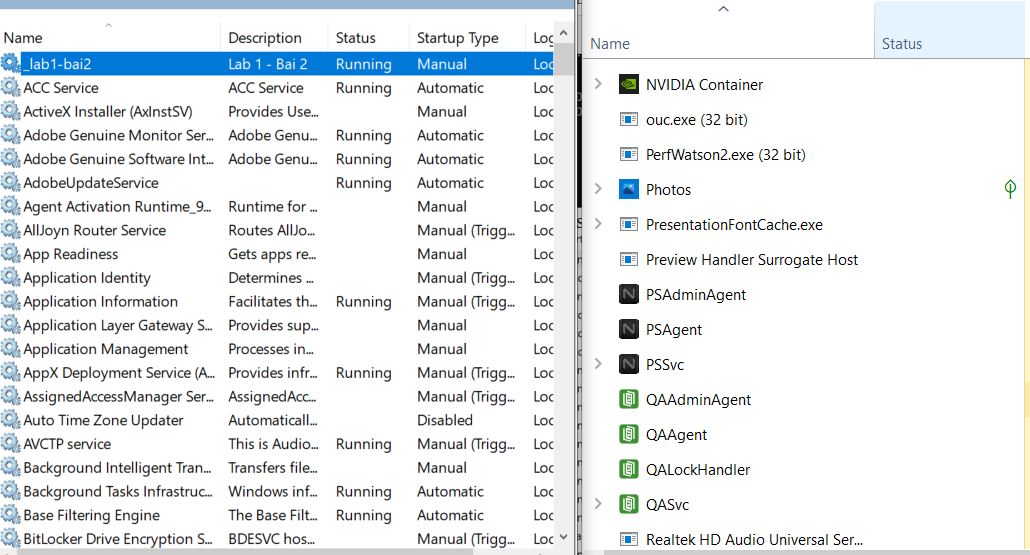
* Chạy services và kiểm tra process



* Bật services và kiểm tra process

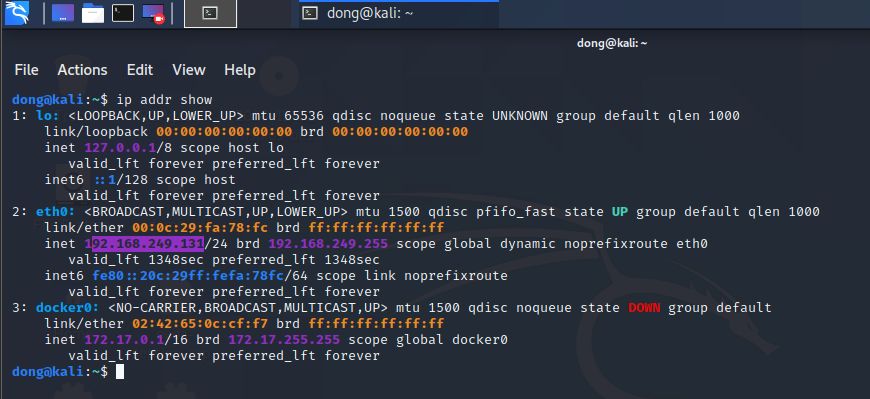


* Tiến trình sẽ sau 5s sẽ kiểm tra 1 lần nếu process đang chạy sẽ kill process



**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.**

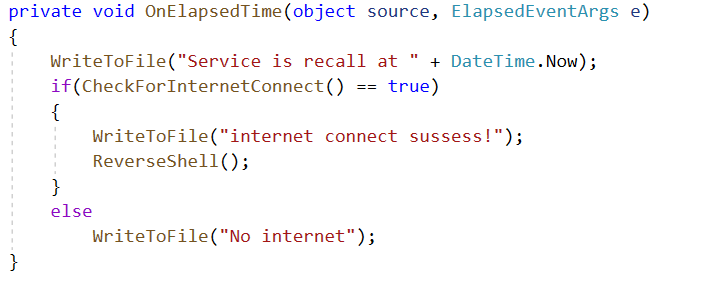
* Với máy attacker có ip:192.168.249.131 ta tiến hành tạo 1 reverse shell để connect back tại port 455



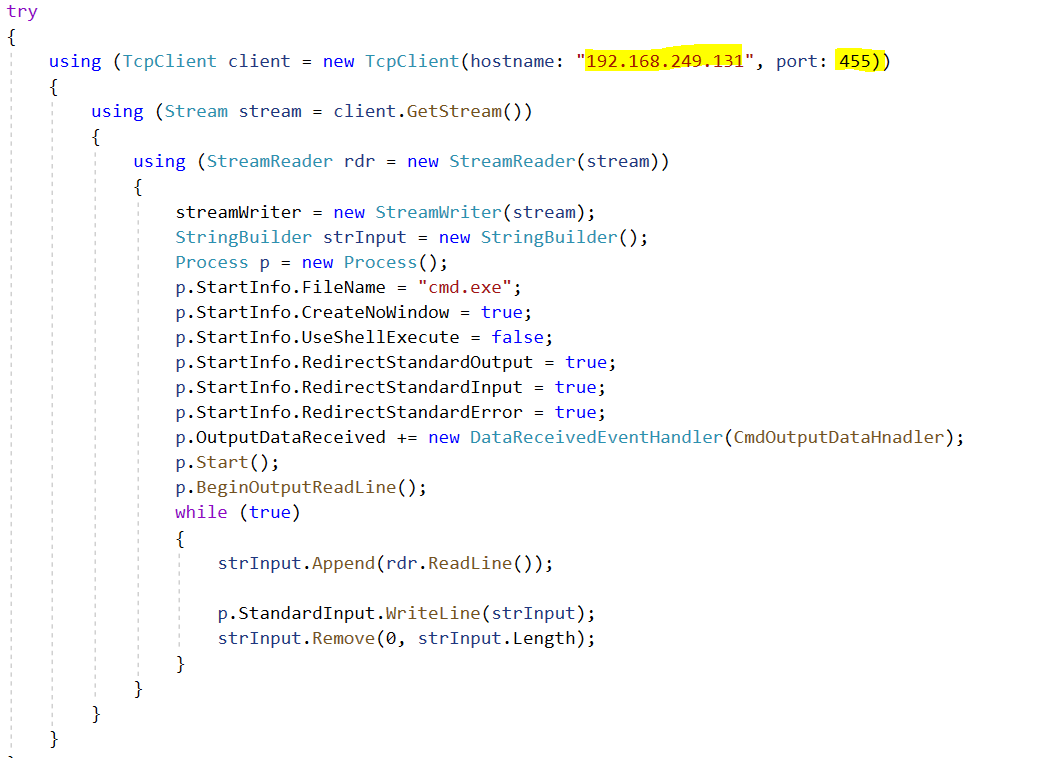
* Đầu tiên ta viết hàm kiểm tra kết nối



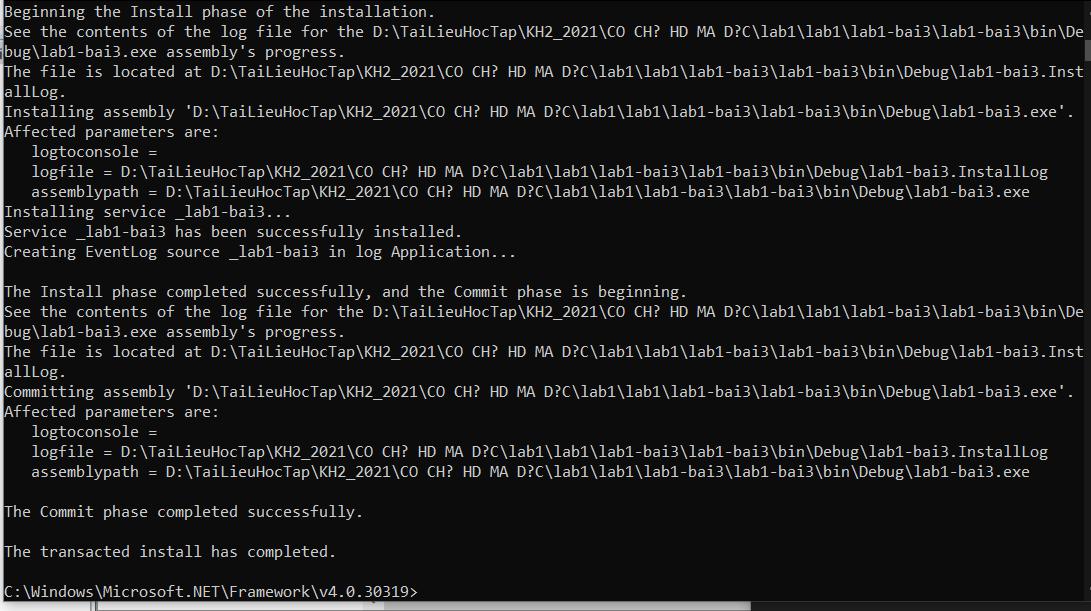
* Nếu hàm trả về true tức là có internet thì ta tiến hành ghi vào log là có internet, đồng thời ta chạy chương trình reverse Shell. Còn không có internet ta chỉ ghi và log là No internet thôi.



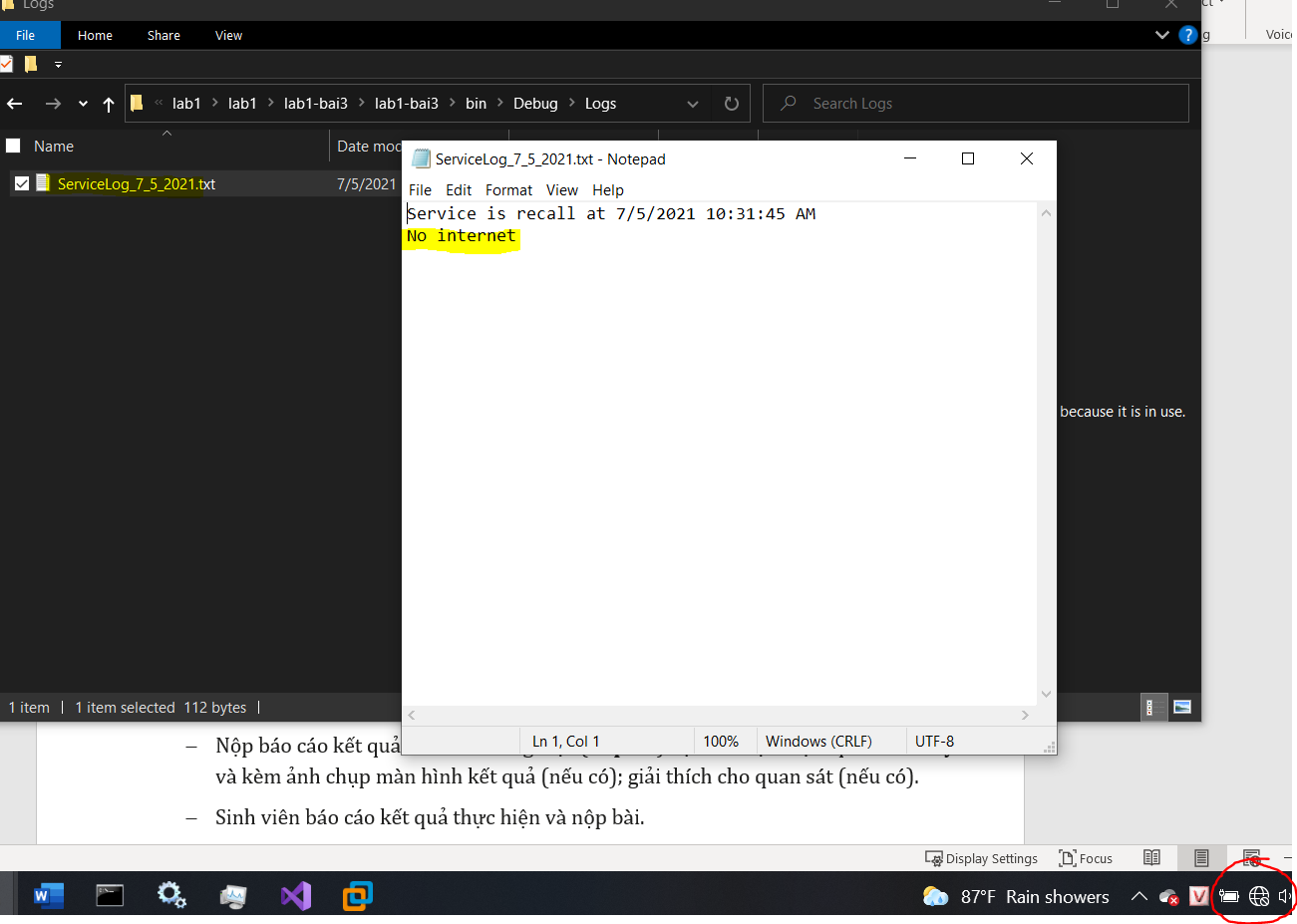
* Chương trình reverse shell



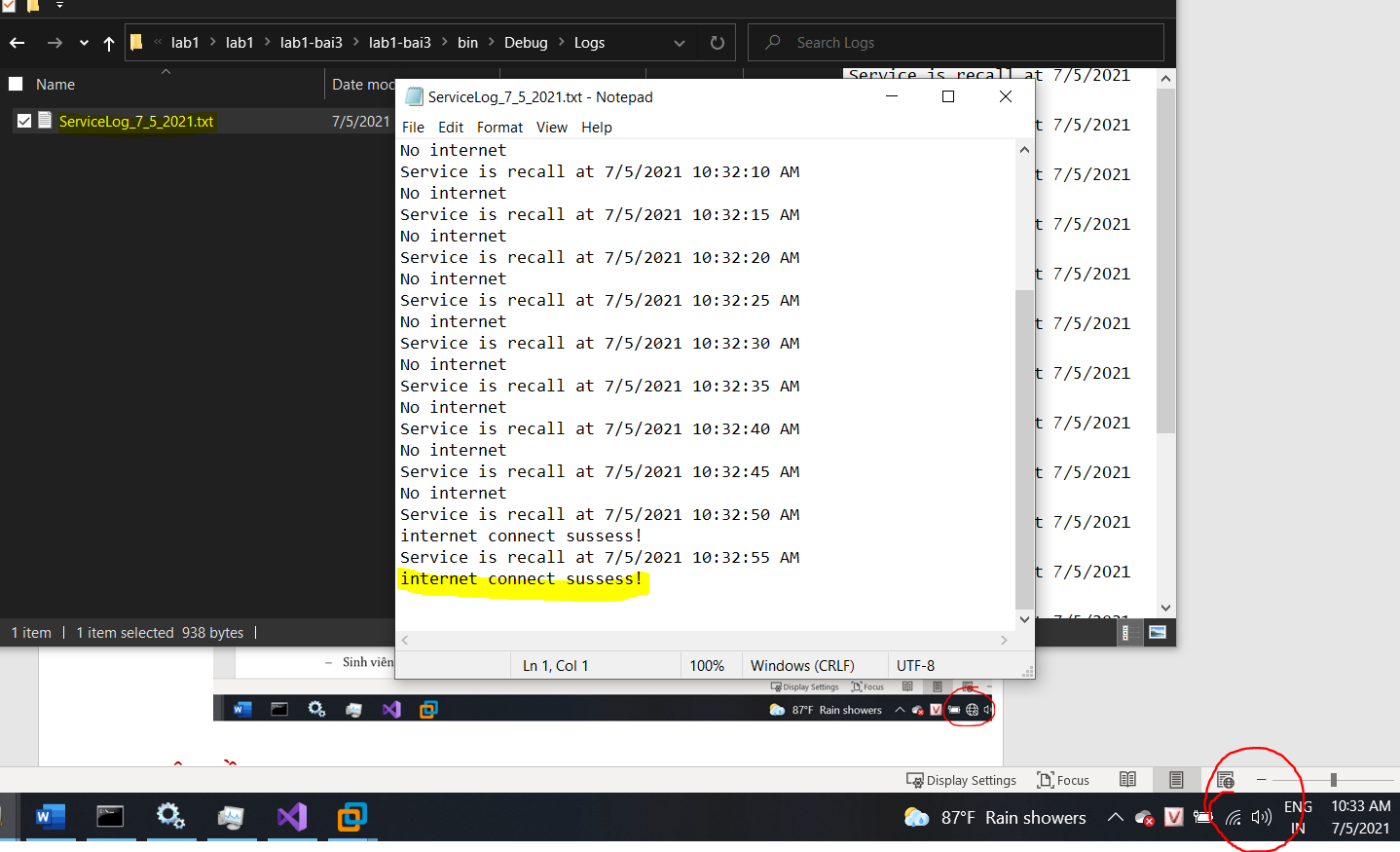
* Với ip máy attacker là 192.168.249.131 ta tiến hành tạo 1 reverse shell connect back tới máy attacker trên cổng 455.
* Khởi tạo service



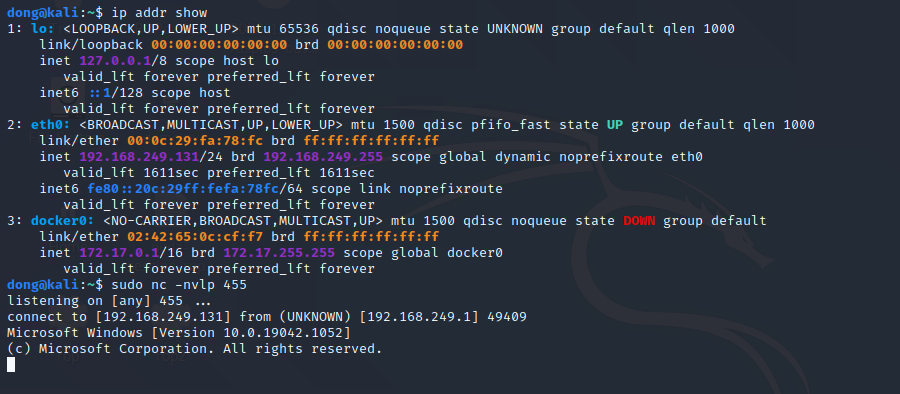
* Tiến hành start service và kiểm tra log



* Khi chưa kết nối mạng thì log ghi lại No internet.



* Khi có mạng log chuyển thành internet connect sussess! Và đồng thời reverse cũng đã được chạy.
* Từ máy attacker ta tiến hành lắng nghe bằng netcat với lệnh: nc -nvlp 455



* Kết quả ta đã tạo được 1 connect back từ máy nạn nhân sang máy attacker.

--------------------------HẾT----------------------------

# **YÊU CẦU CHUNG**

* Sinh viên tìm hiểu và thực hành theo 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]-SessionX\_ NT330.K21.1. (trong đó X là Thứ tự buổi Thực hành).

*Ví dụ: [*NT101.K11.ANTT*]-Session1\_13520401-13520387.*

* 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 Lab.
* Nộp file báo cáo trên theo thời gian đã thống nhất tại courses.uit.edu.vn.

**Đánh giá**: Sinh viên hiểu và tự thực hiện được bài thực hành. Khuyến khích:

* Chuẩn bị tốt.
* Có nội dung mở rộng, ứng dụng trong kịch bản phức tạp hơn, có đóng góp xây dựng bài thực hành.

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

**HẾT**

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