BÁO CÁO THỰC HÀNH

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

**Lab 3: Window 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 | Hoàng Văn Anh Đức | 20520890 | 20520890@gm.uit.edu.vn |
| 2 | Nguyễn Mạnh Cường | 20520421 | 20520421@gm.uit.edu.vn |
| 3 | Lê Quang Minh | 20520245 | 20520245@gm.uit.edu.vn |

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

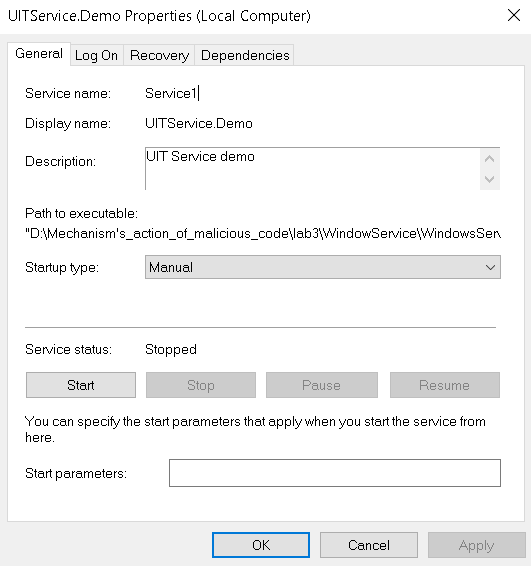
|  |  |  |
| --- | --- | --- |
| **STT** | **Công việc** | **Kết quả tự đánh giá** |
| 1 | trình bày cách gỡ cài đặt Window service | 100% |
| 2 | Viết một Windows service có nhiệm vụ kiểm tra một “process” ở trạng thái hoạt động run/stop hay không và run/stop “process” theo một lịch biểu | 100% |
| 3 | Viết một Windows service có nhiệm vụ kiểm tra kết nối internet của máy hiện tại (HTTP) và tạo reverse shell đơn giản. | 100% |

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Công việc** | **Thành viên thực hiện** | **Kết quả tự đánh giá** |
| 1 | 1 | Đức | 100% |
| 2 | 2 | Đức+Cường | 100% |
| 3 | 3 | Đức | 100% |

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

Để gỡ cài đặt một Window service, bạn có thể làm theo các bước sau đây:

1. Mở "Services" bằng cách nhấn tổ hợp phím "Win + R" để mở hộp thoại "Run", gõ "services.msc" và nhấn Enter.
2. Tìm và chọn dịch vụ mà bạn muốn gỡ cài đặt.
3. Nhấp chuột phải vào dịch vụ đó và chọn "Stop" để dừng dịch vụ.
4. Nhấp chuột phải vào dịch vụ một lần nữa và chọn "Properties".
5. Chuyển đến tab "General" và ghi lại tên của dịch vụ trong trường "Service name".
6. Đóng cửa sổ "Properties" và mở "Command Prompt" với quyền quản trị bằng cách nhấn tổ hợp phím "Win + X" và chọn "Command Prompt (Admin)".
7. Gõ lệnh sau đây và nhấn Enter: sc delete <service name>
8. Trong đó, "<service name>" là tên dịch vụ đã ghi lại ở bước trước đó. Sau khi lệnh được thực thi thành công, có thể đóng cửa sổ "Command Prompt" và khởi động lại máy tính.





**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.**

Thông tin của Service

A screenshot of a computer

Description automatically generated with medium confidence

Text

Description automatically generated

Text

Description automatically generated

Text

Description automatically generated

Text

Description automatically generated

Text

Description automatically generated

Graphical user interface

Description automatically generated

Chương trình sẽ theo lịch trình sẽ bật/tắt sau 5s

Text

Description automatically generated

**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.**

Text

Description automatically generated

Text

Description automatically generated

Text

Description automatically generated

Text

Description automatically generated

Text

Description automatically generated

Text

Description automatically generated

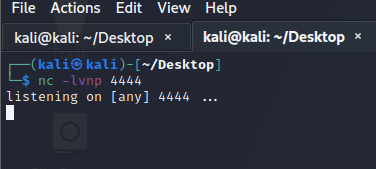
Text

Description automatically generated

Text

Description automatically generated

Mở máy kali lắng nghe trên port 4444



Tắt chương trình ngăn chặn tạo windowservice

Text

Description automatically generated

Tạo Service

Text

Description automatically generated

Start Service

Graphical user interface, text, application, email

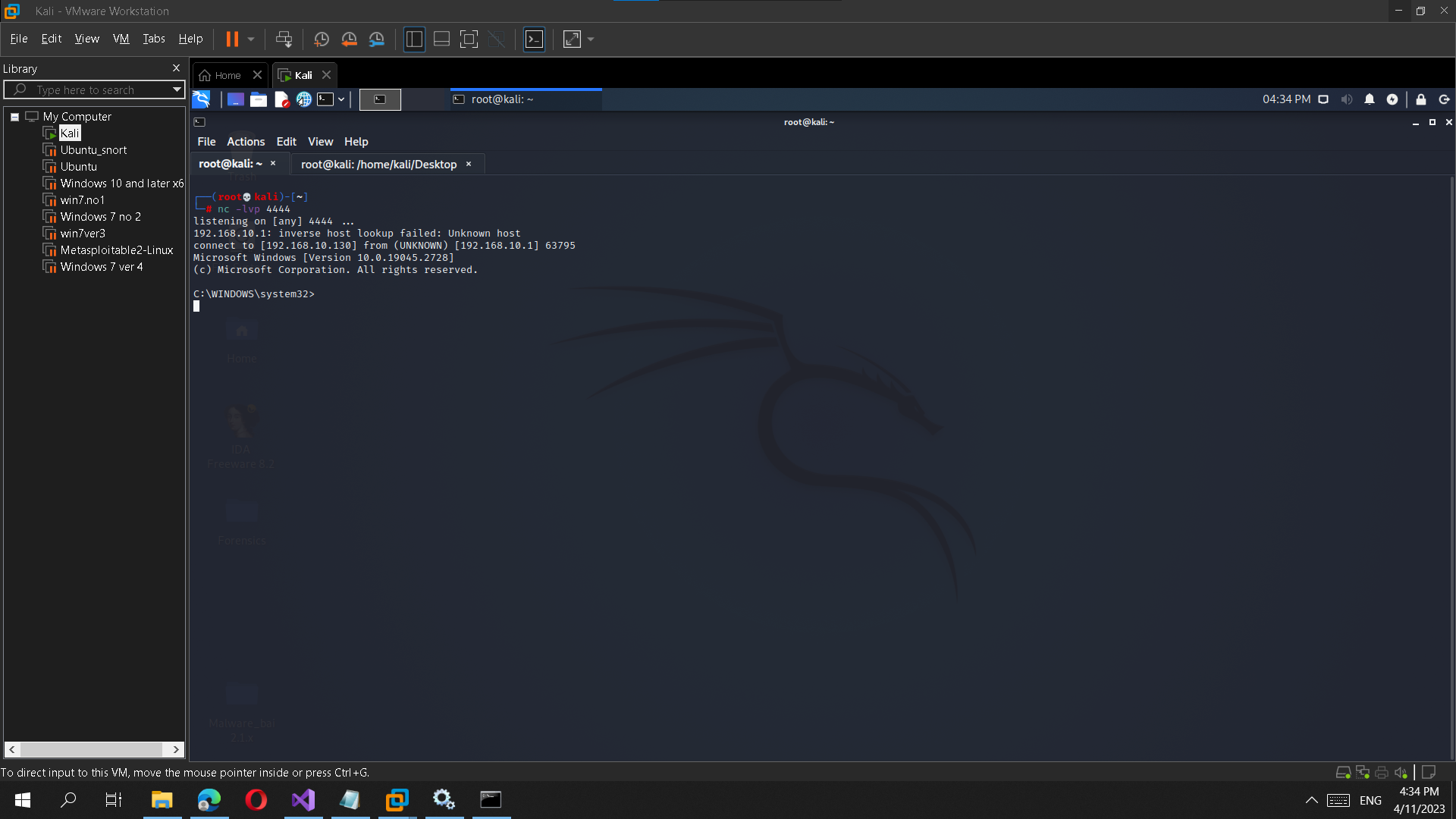
Description automatically generated

Logs

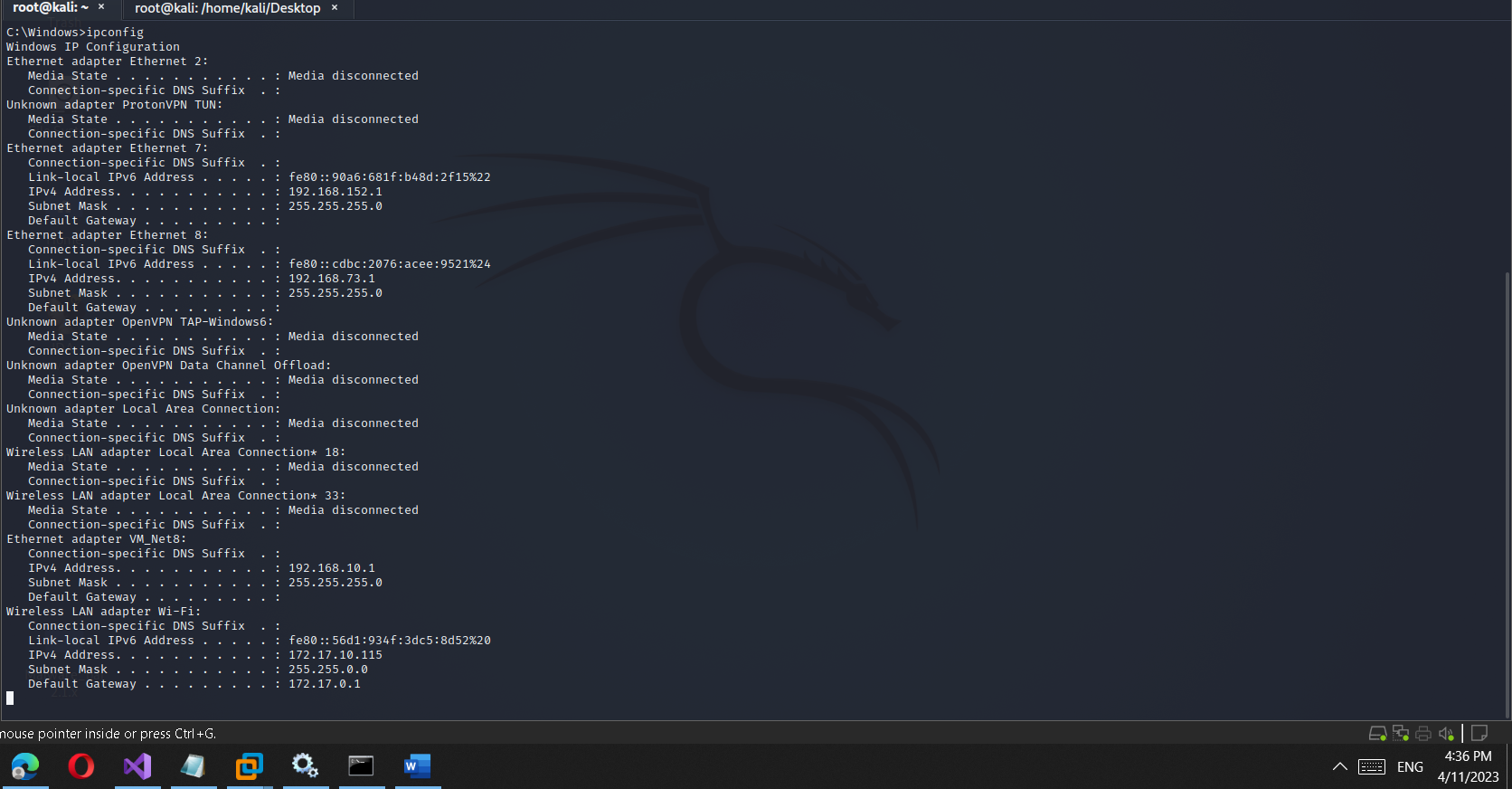
Graphical user interface

Description automatically generated

Kết nối thành công



Test thử



Ổn áp

Background pattern

Description automatically generated with low confidence

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