BÁO CÁO LAB

**Môn học**: **Phương pháp học máy trong an toàn thông tin**

**LAB 2 : Machine Learning based Malware Detection**

**Nhóm: 05**

**THÔNG TIN CHUNG:**

Lớp: NT522.N21.ATCL

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **STT** | **Họ và tên** | **MSSV** | **Phân công** | **Hoàn thành** |
| 1 | Đỗ Quang Thắng | 20521893 | 2,6,7,8 | 100% |
| 2 | Nguyễn Đoàn Thiên Cung | 20521146 | 1,4,5 | 100% |

1. **NỘI DUNG THỰC HIỆN:**

**BÁO CÁO CHI TIẾT**

Câu 1,4,5 : <https://drive.google.com/drive/folders/13kQGk_janXoDqHyBT07cnDAZIeQJXKHw?usp=sharing>

Câu 2,6,7,8:

<https://colab.research.google.com/drive/1egTPqvqVpKxrKmsBUZXJh1DceB9iK_qk?usp=sharing>

1. Sinh viên so sánh kết quả băm với VirusTotal và website Python.

Hàm băm của code so với VirusTotal và website Python là giống nhau

Graphical user interface, text, application, email

Description automatically generated

Graphical user interface, text, application, email

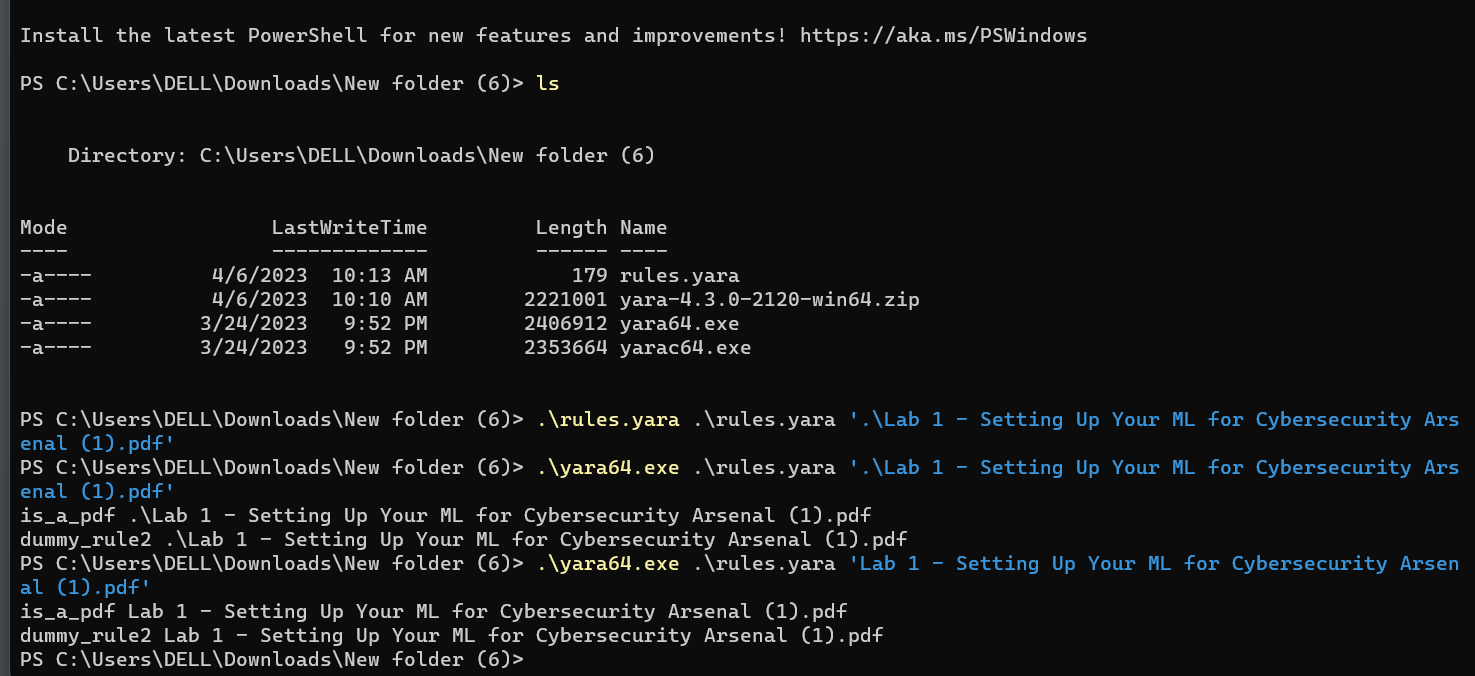
Description automatically generated

Graphical user interface, application, Teams

Description automatically generated

1. Thực hiện đoạn code và in ra kết quả.

b) YARA



c) Kiểm tra PE header

Ảnh có chứa văn bản

Mô tả được tạo tự động

d) Featurizing the PE header

Ảnh có chứa văn bản

Mô tả được tạo tự động

4. Tương tự sinh viên hãy làm các câu truy vấn về Python và Powershell

- Powershell

Graphical user interface, text, application, chat or text message

Description automatically generated

- Python

Graphical user interface, text, application, email

Description automatically generated

5. Sinh viên cho biết quả của đoạn code trên

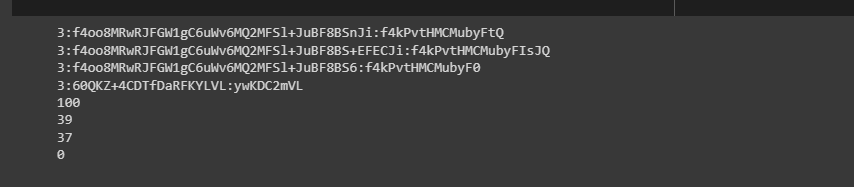
- Kết quả ta thu được từ đoạn code đã cho

A picture containing table

Description automatically generated

6. Thực thi và kiểm tra kết quả.

g) Đo lường sự giống nhau giữa hai chuỗi



h) Đo lường mức độ giống nhau giữa hai tập tin

**Ảnh có chứa văn bản, trong nhà

Mô tả được tạo tự động**

**Ảnh có chứa văn bản

Mô tả được tạo tự động**

7. Thực thi và kiểm tra kết quả.

i) Trích xuất N-grams

**Ảnh có chứa văn bản

Mô tả được tạo tự động**

j) Chọn N-grams tốt nhất

**Ảnh có chứa văn bản

Mô tả được tạo tự động**

8. Thực thi và kiểm tra kết quả.

Ảnh có chứa văn bản

Mô tả được tạo tự động