BÁO CÁO THỰC HÀNH LAB 3

**Thực hành môn Phương pháp học máy trong an toàn thông tin**

**Advanced Malware  
Detection**

**Nhóm: N07**

**Graphical user interface, application

Description automatically generated**

1. **THÔNG TIN CHUNG:**

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

Lớp: NT101.M11.ANTN.1

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Họ và tên** | **MSSV** | **Email** |
| 1 | Trần Hoàng Khang | 19521671 | 19521671@gm.uit.edu.vn |
| 2 | Nguyễn Tú Ngọc | 20521665 | 20521665@gm.uit.edu.vn |

1. **NỘI DUNG THỰC HIỆN:**

|  |  |  |
| --- | --- | --- |
| **STT** | **Công việc** | **Kết quả tự đánh giá** |
| 1 | Câu hỏi 1 | 100% |
| 2 | Câu hỏi 2 | 100% |
| 3 | Câu hỏi 3 | 100% |
| 4 | Câu hỏi 4 | 100% |
| 5 | Câu hỏi 5 | 100% |
| 6 | Câu hỏi 6 | 100% |
| 7 | Câu hỏi 7 | 100% |
| 8 | Câu hỏi 8 | 0% |

BÁO CÁO CHI TIẾT

**Note**: Giải thích được trình bày cụ thể trong file, được viết bằng English theo ý cá nhân

*<More Practice, More Outstanding Result>*

|  |
| --- |
| ***1.*** *Cho biết kết quả accuracy và confusion matrix.* |

**<Xem kết quả chi tiết tại file Notebook (.ipynb)>**

Kết quả:

Text

Description automatically generated

|  |
| --- |
| ***2.*** *Cho biết kết quả vector X* |

**<Xem kết quả chi tiết tại file Notebook (.ipynb)>**

Kết quả:

File thứ nhất:

Text

Description automatically generated

- File thứ 2 và 2 mảng số lượng thuộc tính trả về.

Text

Description automatically generated

|  |
| --- |
| ***3.*** *Cho biết kết quả vector X* |

**<Xem kết quả chi tiết tại file Notebook (.ipynb)>**

Kết quả:

Graphical user interface

Description automatically generated with medium confidence

**Note:** Như comment, số lượng trả về phải là *1000*. Phần này chưa thực hiện được.

|  |
| --- |
| ***4.*** *Cho biết kết quả đánh giá* |

**<Xem kết quả chi tiết tại file Notebook (.ipynb)>**

Kết quả evalation:

Text

Description automatically generated

|  |
| --- |
| **5.** *Cho biết kết quả đánh giá mô hình qua tập test.* |

**<Xem kết quả chi tiết tại file Notebook (.ipynb)>**

Text

Description automatically generated

|  |
| --- |
| **6**. *Cài đặt. UPX từ https://github.com/1.upx/upx/releases, và tiến hành đóng gói các tập tin pe tại Benign PE Samples UPX* |

Vậy thêm 1 byte hoàn toàn trick được SSDeep.

|  |
| --- |
| **7.** *Cho biết kết quả đánh giá.* |

**<Xem kết quả chi tiết tại file Notebook (.ipynb)>**

**Text

Description automatically generated**

|  |
| --- |
| **8.** *Cho biết kết quả đánh giá mẫu mới trong việc đánh lừa bộ nhận diện.* |

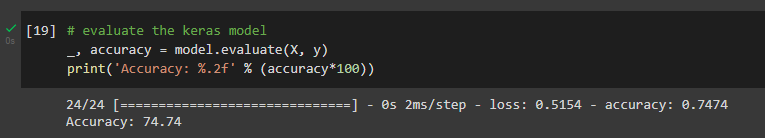
**<Xem kết quả chi tiết tại file Notebook (.ipynb)>**

Hiện tại đang gặp lỗi khi chạy model với các tài nguyên file **.py** cho trước. Sẽ fix trong tương lai

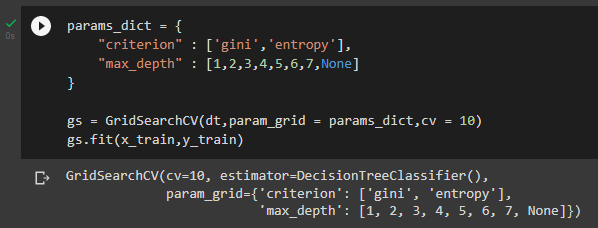
|  |
| --- |
| **Bonus round:** *Thực hiện chạy và giải thích model từ trang* [Your First Deep Learning Project in Python with Keras Step-by-Step (machinelearningmastery.com)](https://machinelearningmastery.com/tutorial-first-neural-network-python-keras/)*.*  ***-*** *Áp dụng GridSearch với* ***model cho trước***  ***-*** *Áp dụng GridSearch với* ***DecisionTree Classifier*** |

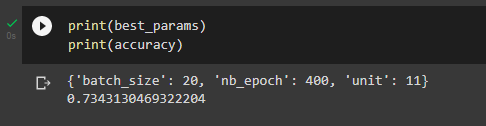
**<Xem kết quả chi tiết tại file Notebook (.ipynb)>**

Kết quả chạy model với tham số được định nghĩa trong blog:



Kết quả khi áp dụng *GridSearch* với các tham số trong mô hình huấn luyện (sử dụng model như trên):





Kết quả khi áp dụng *GridSearch* với các tham số khi cài đặt thuật toán ***Decision Tree:***

Text

Description automatically generated

A screenshot of a computer

Description automatically generated with medium confidence