1. Lý thuyết nền tảng của chủ đề: “Phát hiện các trang web lừa đảo bằng máy học.” bao gồm:

+ Thuật toán Máy Học: Sử dụng các thuật toán có khả năng học từ dữ liệu để xác định các mô hình và đặc điểm của trang web lừa đảo.

+ Trích xuất Đặc trưng: Xác định các đặc trưng cụ thể từ dữ liệu trang web cho thấy hoạt động gian lận, như cấu trúc URL, nội dung trang web và thông tin tên miền.

+ Dữ liệu Huấn luyện: Thu thập bộ dữ liệu của các trang web lừa đảo và hợp pháp đã biết để huấn luyện mô hình máy học.

+ Đánh giá Mô hình: Đánh giá hiệu suất của mô hình máy học trong việc phân loại chính xác trang web là lừa đảo hay hợp pháp.

1. SVM là gì (tổng quan, ứng dụng, ngữ cảnh và kịch bản bảo mật, tài liệu tham khảo, …)?

+ Support Vector Machine (SVM) là một mô hình học máy giám sát mạnh mẽ, được thiết kế cho các bài toán phân loại, hồi quy và phát hiện ngoại lệ. SVM có thể sử dụng các kỹ thuật như kernel trick để xử lý dữ liệu không tuyến tính và có thể mô hình hóa các mối quan hệ phức tạp. Trong ngữ cảnh của Support Vector Machine (SVM), “kernel” là một hàm số được sử dụng để biến đổi dữ liệu không tuyến tính thành dữ liệu có thể phân biệt tuyến tính trong một không gian mới. Cụ thể, Kernel SVM là việc tìm một hàm số biến đổi dữ liệu từ không gian feature ban đầu thành dữ liệu trong một không gian mới bằng hàm số Φ(x). Ý tưởng cơ bản của Kernel SVM và các phương pháp kernel nói chung là tìm một phép biến đổi sao cho dữ liệu ban đầu không phân biệt tuyến tính được biến sang không gian mới. Ở không gian mới này, dữ liệu trở nên phân biệt tuyến tính. Ví dụ, ta có thể biến dữ liệu không phân biệt tuyến tính trong không gian hai chiều thành phân biệt tuyến tính trong không gian ba chiều bằng cách giới thiệu thêm một chiều mới. Một số hàm kernel thông dụng bao gồm Linear, Polynomial, Radial Basic Function (RBF), và Sigmoid. Dưới đây là thông tin tổng quan, ứng dụng, ngữ cảnh sử dụng và kịch bản bảo mật liên quan đến SVM:

* Tổng quan về SVM: SVM tìm kiếm một siêu phẳng trong không gian nhiều chiều để tối ưu hóa biên giới giữa các lớp dữ liệu khác nhau. Trong không gian nhiều chiều, siêu phẳng này được gọi là “hyperplane”. Nó đặc biệt hữu ích khi dữ liệu có nhiều tính năng hoặc khi có một ranh giới rõ ràng giữa các lớp dữ liệu.
* Ứng dụng của SVM: SVM được ứng dụng trong nhiều lĩnh vực như nhận dạng khuôn mặt, phân loại văn bản và hình ảnh, sinh học tính toán, và nhận dạng chữ viết tay. Nó cũng được sử dụng trong các hệ thống kiểm soát hỗn loạn và bảo mật, như phát hiện xâm nhập và tấn công mạng.
* Ngữ cảnh sử dụng SVM: SVM hiệu quả trong không gian đa chiều và vẫn hiệu quả ngay cả khi số lượng chiều lớn hơn số lượng mẫu. Nó sử dụng một tập hợp con của các điểm dữ liệu trong hàm quyết định, gọi là vector hỗ trợ, vì vậy nó cũng tiết kiệm bộ nhớ.
* Kịch bản bảo mật liên quan đến SVM: Trong bảo mật, SVM có thể được sử dụng để phát hiện các hành vi bất thường hoặc tấn công mạng. Nghiên cứu đã chỉ ra rằng SVM có thể được áp dụng an toàn cho các nhiệm vụ nhạy cảm về bảo mật, nhưng cần phải hiểu rõ về các mối đe dọa tiềm tàng khi sử dụng các thuật toán học máy trong các ứng dụng thực tế.
* Tài liệu tham khảo về SVM:

[1.4. Support Vector Machines — scikit-learn 1.4.1 documentation](https://scikit-learn.org/stable/modules/svm.html)

[Support Vector Machines for Classification | SpringerLink](https://link.springer.com/chapter/10.1007/978-1-4302-5990-9_3)

[Support Vector Machines | IEEE Intelligent Systems (acm.org)](https://dl.acm.org/doi/10.1109/5254.708428)

[A structural SVM approach for reference parsing - PMC (nih.gov)](https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3111593/)

[SVM Tutorial — Classification, Regression and Ranking | SpringerLink](https://link.springer.com/referenceworkentry/10.1007/978-3-540-92910-9_15)

1. Sau đây là một kịch bản bảo mật được đề xuất sử dụng SVM để phát hiện xâm nhập trong một hệ thống mạng. Kịch bản này sẽ bao gồm cài đặt hệ thống, thuật toán SVM, và một bản demo sử dụng Python.

* Cài đặt Hệ Thống:
* Một hệ thống mạng với các điểm cuối và máy chủ.
* Dữ liệu lưu lượng mạng được thu thập và ghi lại.
* Một mô hình SVM được huấn luyện để phân loại lưu lượng mạng là bình thường hoặc độc hại.
* Thuật Toán SVM:
* Sử dụng SVM với kernel RBF để xử lý tính phi tuyến của dữ liệu.
* Tinh chỉnh tham số như C (độ lỗi phạt) và gamma (độ rộng của kernel).
* Bản demo:

from sklearn.svm import SVC

from sklearn.datasets import make\_classification

from sklearn.model\_selection import train\_test\_split

from sklearn.metrics import classification\_report

# Tạo dữ liệu giả lập cho việc phân loại

X, y = make\_classification(n\_samples=1000, n\_features=20, n\_informative=2, n\_redundant=10, random\_state=42)

# Chia dữ liệu thành tập huấn luyện và kiểm tra

X\_train, X\_test, y\_train, y\_test = train\_test\_split(X, y, test\_size=0.25, random\_state=42)

# Khởi tạo và huấn luyện mô hình SVM

model = SVC(kernel='rbf', C=1, gamma='auto')

model.fit(X\_train, y\_train)

# Đánh giá mô hình

predictions = model.predict(X\_test)

print(classification\_report(y\_test, predictions))

* Trong bản demo trên, tôi đã tạo dữ liệu giả lập với 1000 mẫu và 20 tính năng, sau đó chia chúng thành tập huấn luyện và kiểm tra. Mô hình SVM được huấn luyện sử dụng kernel RBF và sau đó được đánh giá trên tập kiểm tra.
* Để áp dụng kịch bản này vào một hệ thống thực tế thì chúng ta cần thu thập dữ liệu lưu lượng mạng thực tế và tiến hành tiền xử lý dữ liệu (như mã hóa, chuẩn hóa) trước khi huấn luyện mô hình SVM. Sau đó, mô hình có thể được triển khai để giám sát lưu lượng mạng và phát hiện các hoạt động độc hại dựa trên dữ liệu đã học.
* Đây chỉ là một ví dụ cơ bản và trong thực tế, việc triển khai một hệ thống phát hiện xâm nhập đầy đủ sẽ cần nhiều bước phức tạp hơn và tinh chỉnh kỹ lưỡng hơn.