CÂU HỎI ÔN TẬP

Môn học: NT522 – Phương pháp học máy trong An toàn thông tin

Cập nhật: 11.06.2024

Câu 1. Phân biệt các loại AI khác nhau? Trình bày được định nghĩa của các loại học máy (Học giám sát, không giám sát, bán giám sát, học tăng cường)?

Câu 2. Các tiêu chí để đánh giá mô hình học máy? Cách chọn tiêu chí đánh giá phù hợp trong một số ngữ cảnh bài toán An toàn thông tin.

Câu 3. Trình bày cách phân chia dữ liệu và tiền xử lí dữ liệu phổ biến?

Câu 4. Tác dụng của hàm kích hoạt (activation function) trong các mạng nơ-ron? Một số hàm activation phổ biến?

Câu 5. Phân biệt sự khác nhau của các dạng thuật toán học máy như Phân cụm (clustering), phát hiện sự dị thường (anomaly detection), phân loại (classification).

Câu 6. Học sâu (DL) là gì? Xác định được các lớp, đầu ra, đầu vào trong một số mô hình mạng nơ-ron nhân tạo, học sâu (DL)? Một số ứng dụng cơ bản trong lĩnh vực ATTT.

Câu 7. Nguyên tắc hoạt động của mạng sinh đối kháng? Một số ứng dụng của mô hình mạng sinh đối kháng (GANs) trong ATTT.

Câu 8. Điều gì xảy ra khi kẻ tấn công sử dụng kỹ thuật tấn công đối kháng để đánh lừa mô hình ML? Các biện pháp phòng ngừa là gì?

Câu 9. Học tăng cường là gì? Một số ứng dụng của Reinforcement Learning (RL) trong An toàn thông tin? Xác định được các khái niệm cơ bản, định nghĩa của RL trong các bài toán điển hình của ATTT.

Câu 10. Một số phương pháp phát hiện mã độc sử dụng các thuật toán học máy, học sâu?

Câu 11. Ảnh hưởng của tốc độ học, batch size và epoch lên quá trình huấn luyện mô hình học máy nói chung?

Câu 12. Khi xây dựng các ứng dụng dựa trên học máy, cần làm gì khi dữ liệu bị mất cân bằng? Tiêu chí nào có thể dùng để đánh giá mô hình trong trường hợp dữ liệu bị mất cân bằng?

Câu 13. Học liên kết (Federated Learning - FL) là gì? Ưu và nhược điểm của nó? Công thức tổng hợp mô hình trong FL (thuật toán tổng hợp FedAvg)?

Câu 14. Xử lý đặc trưng (feature engineering) là gì? Mục đích áp dụng? Có những kỹ thuật nào để thực hiện?

Câu 15. MLOps là gì? Nó giải quyết vấn đề gì trong ngữ cảnh các ứng dụng có sử dụng Học máy? Đánh giá tiềm năng và cơ hội của MLOps trong lĩnh vực An toàn thông tin?

Câu 16. Reinforcement Learning có thể được áp dụng để tự động hóa các quyết định an ninh mạng như thế nào? Cho ví dụ.

Câu 17. Qui trình kiểm thử xâm nhập hiện tại có những vấn đề nào mà các phương pháp học máy có thể giúp giải quyết? Trình bày phương pháp ứng dụng Học tăng cường trong bài toán Kiểm thử xâm nhập (Pentest/Network Exploitation)?

Câu 18. An ninh mạng thích ứng là gì? Các mô hình học tăng cường có thể được sử dụng để phát triển các hệ thống phòng thủ mạng thích ứng (adaptive cybersecurity) như thế nào?

Câu 19. Nêu một số ưu điểm mà các mô hình ngôn ngữ lớn (Large Language Model – LLM) trong 1 bài toán điển hình của an toàn thông tin? Gợi ý: phát hiện lỗ hổng phần mềm (vulnerability

detection), sửa lỗi bảo mật phần mềm (vulnerability fixing code generation), kiểm thử fuzzing, phát hiện mã độc (malware detection).

Câu 20. Generative AI là gì? Phân tích tiềm năng mang lại cũng như rủi ro có thể gây ra vấn đề mất an toàn thông tin, tấn công mạng, khống chế và điều khiển các hệ thống thông tin.