**ĐỀ CƯƠNG ÔN TẬP LÝ THUYẾT**

1. Anh/chị hãy giải thích tại sao cần phải đảm bảo an toàn cho thông tin và hệ thống thông tin?

2. Anh/chị hãy giải thích các thuộc tính an ninh an toàn của hệ thống thông tin theo mô hình CIA?

3. Anh chị hãy so sánh 2 loại phần mềm độc hại: virus và worm?

4. Anh/chị hãy trình bày sơ đồ phân loại và cách phòng chống các phần mềm độc hại?

5. Anh/chị hãy giải thích các lớp phòng vệ điển hình trong mô hình bảo đảm an toàn hệ thống thông tin có chiều sâu Defence in Depth?

6. Anh/chị hãy giải thích tấn công giả mạo địa chỉ và nêu cách phòng chống?

7. Anh/chị hãy giải thích về các dạng tấn công vào mật khẩu và nêu cách phòng tấn công vào mật khẩu?

8. Anh/chị hãy giải thích cơ chế phát hiện xâm nhập dựa trên bất thường của hệ thống IDS/IPS?

9. Anh/chị hãy giải thích cơ chế phát hiện xâm nhập dựa trên chữ ký của hệ thống IDS/IPS?

10. Anh/chị hãy giải thích tấn công kiểu Social Engineering và nêu các cách phòng chống?

11. Anh/chị hãy phân tích các kỹ thuật kiểm soát truy nhập trên tường lửa? Liệt kê các hạn chế tường lửa?

12. Anh/chị hãy giải thích quan hệ giữa mối đe dọa và lỗ hổng trong hệ thống thông tin và liệt kê các mối đe dọa thường gặp?

13. Anh/chị hãy trình bày về biện pháp điều khiển truy nhập MAC và cho ví dụ?

14. Anh/chị hãy trình bày về biện pháp điều khiển truy nhập DAC và cho ví dụ?

15. Anh/chị hãy so sánh đặc điểm của hệ mật mã khóa đối xứng với hệ mật mã khóa bất đối xứng?

16. Trong hệ mã hóa DES, anh/chị hãy vẽ sơ đồ thuật toán các bước xử lý chính của hệ mã, giải thích sơ đồ?

17. Trong hệ mã hóa DES, anh/chị hãy vẽ sơ đồ thuật toán các bước sinh khóa phụ của hệ mã, giải thích sơ đồ?

18. Anh/chị hãy cho biết các thành phần và chức năng của hạ tầng quản lý khóa công khai PKI?

19. Anh/chị hãy vẽ sơ đồ quá trình tạo và kiểm tra chữ ký số, giải thích sơ đồ?

20. Anh/chị hãy vẽ sơ đồ cấp và sử dụng chứng chỉ số, giải thích sơ đồ?