Câu hỏi ôn tập môn: **Giám sát và ứng phó sự cố ATM**

*Tài liệu tham khảo:*

[1]. Slide bài giảng

[2]. Applied Network Security Monitoring. Collection, Detection, and Analysis (2014)

[3]. Tài liệu hướng dẫn đánh giá và quản lý rủi ro an toàn thông tin, Cục An toàn thông tin – Bộ thông tin truyền thông, 2021

[4]. Thông tư 20/2017/TT-BTTT. Quy định về điều phối, ứng cứu sự cố an toàn thông tin mạng trên toàn quốc

[5]. NIST.SP800-61. Computer Security Incident Handling Guide

1. ***Lý thuyết***
2. Vai trò của hệ thống giám sát trong việc đảm bảo an toàn hệ thống thông tin và mạng máy tính
3. So sánh công nghệ giám sát ATTT với công nghệ phát hiện xâm nhập IDS
4. So sánh giám sát an toàn mạng với giám sát an ninh liên tục
5. Phân tích ưu nhược điểm của hệ thống giám sát
6. Trình bày một số sản phẩm giám sát ATTT mà em biết
7. Kiến trúc và thành phần của hệ thống giám sát
8. Phân tích một số chức năng quan trọng trong hệ thống giám sát
9. Các loại dữ liệu đầu vào của hệ thống giám sát
10. Phương pháp thu thập dữ liệu của hệ thống giám sát
11. Lập kế hoạch thu thập dữ liệu theo Khung ACF (Applied Collection Framework)
12. Phương pháp phân tích dữ liệu
13. Lấy ví dụ và phân tích một số sự cố ATTT
14. Vai trò của ứng phó sự cố trong đảm bảo ATTT
15. Quy trình ứng phó sự cố ATTT
16. ***Bài tập***
17. Bài tập về tính toán dấu hiệu xâm nhập IOC. Tài liệu tham khảo [1] – Chương 2.1; [2]- Chapter 7. Indicators of Compromise and Signatures
18. Bài tập về thu thập dữ liệu theo ACF. [1]-Chương 2.2; [3]-Chương 2;
19. Bài tập về phân tích dữ liệu. [1]-Chương 2.2; [2]-Chapter 15. The Analysis Process
20. Bài tập về ứng phó sự cố ATTT. [1]-Chương 3,4; [5]- A.2 Scenarios