NỘI DUNG TRỌNG TÂM ÔN TẬP
MÔN: AN TOÀN MẠNG MÁY TÍNH
Học kì 1 – Năm học 2023-2024

- Hình thức thi: Trắc nghiệm
- Thời gian: 75 phút
- Tài liệu: Được phép sử dụng 02 tờ giấy A4 viết tay (không đánh máy, không photo của người khác), trên tài liệu ghi rõ họ tên và MSSV

STT	Nội dung	Chi tiết
1	Tổng quan về An ninh mạng	- Các kiến thức cơ bản về mạng, mô hình OSI, TCP/IP - Một số khái niệm về bảo mật: đặc tính của thông tin; mối quan hệ giữa threat, vulnerability, risk, exposure, safeguard, ... - CIA, AAA là gì? - Phân tích Mô hình phòng thủ theo chiều sâu (Defense in Depth)?
2	Các giai đoạn tấn công, nguyên lý phân quyền tối thiểu, kiểm soát truy cập	- Các kỹ thuật tấn công phổ biến: nghe lén, mật khẩu, giả mạo, dos, … - Các nguyên lý chung về các giai đoạn Hacking: reconnaissance, scanning, gaining access, maintain, clearing → Mục tiêu, kỹ thuật thực hiện, công cụ hỗ trợ thực hiện, … - Nguyên lý hoạt động của các kỹ thuật scanning: các loại TCP/UDP scan? - Least privilege? Privilege Separation là gì?
3	Tổng quan về các phần mềm độc hại	Phân biệt được các loại mã độc, đặc điểm kỹ thuật, nguyên tắc hoạt động, lây nhiễm của chúng:

		- Trojan, Spyware, Back Door, Rootkit, Malware, Virus, Worms, Ransomware, …
4	Tổng quan về mật mã học và các ứng dụng	- Hiểu rõ và thực hiện chạy tay được các loại Mã hóa cổ điển (input --> output) - Hiểu rõ mã hoá hiện đại: đặc biệt là chi tiết kỹ thuật của DES, AES *(Lưu ý kỹ các ma trận trong hoán vị ở các bước lặp)* - Mã hóa đối xứng/ bất đối xứng? - Hệ mã hóa khóa bí mật? hệ mã hoá khoá công khai? - Giao thức trao đổi khóa Diffie-Hellman, RSA, quản lý khóa? Tính được khoá từ các giao thức trên với các dữ liệu cho trước. - Hàm băm? Các tiêu chuẩn của hàm băm? - Chữ kí số/chứng thực số? - Một số ứng dụng của mật mã học? - *Khả năng tấn công trên một hệ thống mã hóa là gì? (tấn công thuật toán, tấn công khóa?)* - ***Đọc hiểu được sơ đồ hoạt động của các hệ mật mã và ứng dụng mật mã đã nêu ở trên (từ sơ đồ viết được công thức tổng quát và ngược lại)***
5	Các giao thức bảo mật mạng.	Nắm rõ thành phần, nguyên tắc, các bước và thứ tự hoạt động của các bước của từng giao thức sau: - PKI, X509 - IPSec - SSL/TLS

		- VPN/SSH - PGP và S/MIME - Kerberos
6	Bảo mật mạng ngoại vi (Firewall)	- Hiểu và phân biệt các phân vùng mạng của một tổ chức/doanh nghiệp - Tường lửa? Hoạt động ở những layer nào trong OSI? Nắm được những loại tường lửa tương ứng với từng layer? - Các loại cấu hình tường lửa? - Bộ lọc gói tin, cấu trúc rule, đọc hiểu được rule …
7	IDS/IPS	- IDS/IPS là gì? - Các loại IDS/IPS? Cách đặt và vị trí đặt các loại trên trong hệ thống mạng? - Snort? Snort Rules?
8	Một số tool	Biết và Sử dụng được cơ bản một số tool phổ biến dùng trong an toàn, bảo mật mạng?