ĐỀ CƯƠNG ÔN TẬP – CTF DTU 2025

1. GIỚI THIỆU CUỘC THI

- **Thời gian thi**: Ngày 04/4/2025
- **Địa điểm**: Đại học Duy Tân
- **Hình thức thi**: Jeopardy-style CTF
- **Mục đích**: Tuyển chọn đội tuyển CTF tham gia các giải trong nước và quốc tế
- **Đối tượng**: Sinh viên quan tâm đến an toàn thông tin, bảo mật, và đam mê CTF

2. KIẾN THỨC CẦN CHUẨN BỊ

2.1. MÔ HÌNH OSI & TCP/IP

- **Mô hình OSI (Open Systems Interconnection)**:
  - Lớp 1: Physical (Vật lý)
  - Lớp 2: Data Link (Liên kết dữ liệu)
  - Lớp 3: Network (Mạng)
  - Lớp 4: Transport (Vận chuyển)
  - Lớp 5: Session (Phiên)
  - Lớp 6: Presentation (Trình bày)
  - Lớp 7: Application (Ứng dụng)
- **Mô hình TCP/IP:**
  - Network Access
  - Internet
  - Transport
  - Application
- **Có kiến thức cơ bản về Linux**: Các lệnh cơ bản, cơ bản về hệ thống tập tin, các công cụ lọc (grep, cut, tr, wc, sort, head, tail, …) và lập trình Shell.
- **Các giao thức quan trọng**:
  - HTTP/HTTPS, FTP, SSH, DNS
  - ICMP, ARP, DHCP
  - TCP vs UDP

- …

2.2. CƠ BẢN VỀ AN TOÀN THÔNG TIN

- Mã hóa (Caesar, XOR, Base64, AES, RSA, …)
- Kĩ thuật khai thác lỗ hổ bảo mật:
  - SQL Injection
  - XSS (Cross-Site Scripting)
  - CSRF (Cross-Site Request Forgery)
  - Buffer Overflow
  - …
- Kĩ thuật OSINT (Open Source Intelligence)
- Các công cụ thường dùng:
  - Web Exploitation: Burp Suite, sqlmap, wfuzz.
  - Reverse Engineering: Ghidra, IDA Free, Radare2.
  - Forensics: Autopsy, binwalk, foremost, Wireshark.
  - Cryptography: CyberChef, Hashcat, RsaCtfTool.

2.3. CƠ BẢN VỀ CTF

- CTF là gì?
- Phân loại các thể loại CTF:
  - Jeopardy
  - Attack & Defense
  - Mixed
- Các dạng bài thi cốt lõi trong CTF Jeopardy:
  - Crypto (Mã hóa)
  - Forensics (Pháp chứng số)
  - Web Exploitation (Tấn công web)
  - Reverse Engineering (Dịch ngược)
  - Pwn (Khai thác lỗ hổ phần mềm)
  - Misc (các dạng bài tổng hợp)

2.4. TƯ DUY IQ

- Các bài toán logic, suy luận
- Các bài toán tìm quy luật
- …

2.5. KỸ NĂNG TIẾNG ANH

➢ Thuật ngữ chuyên ngành an toàn thông tin

➢ Các tài liệu tiếng Anh về CTF

➢ Đọc và hiểu tài liệu, write-up của các đội CTF quốc tế

3. PHƯƠNG PHÁP ÔN TẬP

➢ Luyện tập với các trang web CTF:

- **CTF Wiki (https://ctf-wiki.mahaloz.re/)**
- **PicoCTF (https://picoctf.org/)**
- Hack The Box (https://www.hackthebox.com/)
- TryHackMe (https://tryhackme.com/)
- OverTheWire (https://overthewire.org/)
- Hướng dẫn chơi CTF (Capture The Flag) cho người mới bắt đầu (https://www.youtube.com/watch?v=N2LIxNU-2VM&t=639s; https://www.youtube.com/watch?v=20hdoiYEIms)
- Hoặc tìm kiếm các bài giải với từ khoá tìm kiếm "**Writeups CTF**"

➢ Tham gia các nhóm CTF online

➢ Luyện tập với các bài write-up của các đội quốc tế

➢ Thực hành với các công cụ hacking

4. KẾ HOẠCH ÔN TẬP (TỰ ÔN)

- **Tuần 1**: Ôn lại kiến thức cơ bản về OSI, TCP/IP, an toàn thông tin
- **Tuần 2**: Luyện tập các thể loại bài Jeopardy-style CTF
- **Tuần 3**: Thực hành luyện tập với các bài CTF thực tế

Chúc các bạn ôn tập tốt và đạt kết quả cao trong cuộc thi!