ĐỀ CƯƠNG ÔN TẬP HỌC PHẦN

KIỂM THỬ VÀ ĐÁNH GIÁ AN TOÀN HỆ THỐNG THÔNG TIN

1. **Lý thuyết**
2. Tổng quan
   1. Khái niệm đánh giá an toàn hệ thống thông tin
   2. Tầm quan trọng của đánh giá an toàn hệ thống thông tin
   3. Phương pháp đánh giá an toàn hệ thống thông tin
      1. NIST 800-115
      2. ISSAF
      3. OSSTMM
   4. Kiểm thử xâm nhập
      1. Giới thiệu
      2. Quy trình thực hiện kiểm thử xâm nhập
      3. Các loại kiểm thử xâm nhập
      4. Các giai đoạn kiểm thử xâm nhập
   5. Các nội dung kiểm thử xâm nhập
   6. Tổng kết chương 1
3. Thu thập thông tin và xác định lỗ hổng (6 LT + 9 TH)
   1. Thu thập thông tin
      1. Thu thập thông tin trên các website
      2. Thu thập thông tin dựa trên vị trí
      3. Thu thập thông tin dựa trên việc làm
      4. Thu thập thông tin thông qua email
      5. Thu thập thông tin sử dụng công cụ
   2. Khám phá mạng
   3. Xác định cổng và dịch vụ
      1. Quét đầy đủ
      2. Quét một nửa
      3. Quét XMAS
      4. Quét FIN
      5. Quét NULL
      6. Quét IDLE
   4. Xác định hệ điều hành
      1. Xác định hệ điều hành theo kiểu chủ động
      2. Xác định hệ điều hành theo kiểu bị động
   5. Dò quét lỗ hổng bảo mật
      1. Giới hạn của việc quét lỗ hổng
      2. Quy trình quét lỗ hổng
      3. Các phương pháp quét lỗ hổng
   6. Một số phương pháp thu thập thông tin nâng cao
      1. Tránh hệ thống phát hiện xâm nhập
      2. Vượt tường lửa

Tổng kết chương 2

1. Phân tích lỗ hổng
   1. Giới thiệu phân tích lỗ hổng
   2. Các bước đánh giá lỗ hổng
   3. Phân loại lỗ hổng
   4. Các kiểu đánh giá lỗ hổng
   5. Các giai đoạn đánh giá lỗ hổng
      1. Giai đoạn trước khi đánh giá
      2. Giai đoạn thực hiện đánh giá
      3. Giai đoạn sau khi thực hiện đánh giá
   6. Đối chiếu lỗ hổng với mức chấp nhận lỗ hổng
   7. Cân nhắc đánh giá lỗ hổng
   8. Báo cáo đánh giá lỗ hổng
      1. Mốc thời gian
      2. Loại báo cáo
   9. Tổng kết chương 4
2. Kiểm thử máy chủ và ứng dụng Web (6 LT + 9 TH)
   1. Giới thiệu quy trình kiểm thử OWASP
   2. Một số lỗ hổng điển hình trong ứng dụng Web
   3. Kiểm thử quản lý cấu hình
   4. Kiểm thử quản lý định danh
   5. Kiểm thử xác thực
   6. Kiểm thử phân quyền
   7. Kiểm thử quản lý phiên
   8. Kiểm thử giá trị nhập
   9. Kiểm thử vấn đề xử lý lỗi
   10. Kiểm thử điểm yếu khi sử dụng mật mã
   11. Kiểm thử Logic
   12. Kiểm thử phía Client

Tổng kết chương 4

1. Kiểm thử ngoài mạng
   1. Giới thiệu về kiểm thử ngoài mạng
   2. Các bước thực hiện kiểm thử ngoài mạng
   3. Tổng kết chương 5
2. Kiểm thử mạng bên trong
   1. Giới thiệu về kiểm thử mạng bên trong
   2. Các bước thực hiện kiểm thử mạng bên trong
   3. Tổng kết chương 6
3. Lập báo cáo và bàn giao kết quả kiểm thử
   1. Giới thiệu về bàn giao kết quả kiểm thử
   2. Báo cáo kiểm thử an toàn
      1. Tóm tắt quy trình thực hiện kiểm thử
      2. Phạm vi dự án kiểm thử
      3. Phân tích các kết quả
      4. Các khuyến nghị
      5. Phụ lục
   3. Báo cáo kiểm thử phía client
      1. Báo cáo kiểm thử client
      2. Báo cáo kiểm thử người dùng
   4. Báo cáo kiểm thử ứng dụng Web
   5. Tài liệu kết thúc kiểm thử
   6. Tạo báo cáo cuối cùng
      1. Định dạng báo cáo
      2. Bàn giao báo cáo
      3. Lưu trữ báo cáo
   7. Tổng kết chương 7
4. Các hoạt động sau kiểm thử
   1. Giới thiệu các hoạt động sau kiểm thử
   2. Các kiến nghị về mức ưu tiên
   3. Phát triển kế hoạch hành động
   4. Tạo quy trình giảm thiếu cấu hình sai
   5. Cập nhật và áp dụng các bản vá
   6. Bài học kinh nghiệm và thực tiễn
   7. Tạo chính sách an toàn
   8. Triển khai tập huấn
   9. Triển khai lớp đào tạo kỹ nghệ xã hội
   10. Hủy báo cáo kiểm thử
   11. Tổng kết chương 8
5. Thực hành

* Biết cách vận hành, sử dụng các công cụ đã được nghiên cứu trong nội dung thực hành (nmap, metasploit, msfvenom, google search, nc….)
* ***Đề thi mở, sinh viên được phép sử dụng mọi loại tài liệu trong quá trình thực hiện bài thi (laptop, điện thoại, slide, giáo trình….)***