ĐỀ CƯƠNG ÔN TẬP HỌC PHẦN

KIỂM THỬ VÀ ĐÁNH GIÁ AN TOÀN HỆ THỐNG THÔNG TIN

1. **Tổng quan**

* Hình thức thi: Thi trắc nghiệm
* Tổng số câu hỏi: 60 câu.
* Thời gian làm bài: 60 phút.
* Tài liệu được phép sử dụng: Không

1. **Lý thuyết**
2. Tổng quan về kiểm thử và đánh giá an toàn hệ thống thông tin (6 LT)
   1. Các khái niệm cơ bản
      1. Mối đe dọa an toàn thông tin
      2. Lỗ hổng an toàn thông tin
      3. Điểm yếu an toàn thông tin
      4. Kiểm thử an toàn thông tin
      5. Đánh giá an toàn thông tin
      6. Kiểm định an toàn thông tin
   2. Phương pháp luận kiểm thử và đánh giá an toàn hệ thống thông tin
      1. NIST 800-115
      2. ISSAF
      3. OSSTMM
   3. Kỹ thuật kiểm thử và đánh giá an toàn hệ thống thông tin
      1. Hộp đen
      2. Hộp trắng
      3. Hộp xám
   4. Một số lưu ý khi thực hiện kiểm thử và đánh giá an toàn hệ thống thông tin
      1. Giai đoạn lập kế hoạch
      2. Giai đoạn thực hiện kiểm thử và đánh giá
      3. Giai đoạn sau kiểm thử và đánh giá
   5. Một số công cụ hỗ trợ trong kiểm thử an toàn hệ thống thông tin
      1. Kali Linux
      2. Metasploit
      3. BurpSuite

Tổng kết chương 1

1. 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. Kiểm thử hệ thống (6 LT + 6 TH)
   1. Kiểm thử mật khẩu
   2. Kiểm thử khả năng khai thác lỗ hổng
   3. Kiểm thử leo thang đặc quyền
   4. Kiểm thử duy trì truy cập
   5. Kiểm thử chính sách hệ thống

Tổng kết chương 3

1. 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 mạng không dây (3 LT + 3 TH)
   1. Chặn bắt gói tin không dây
   2. Phân tích điểm truy cập không dây
   3. Kiểm thử xác thực mạng không dây
   4. Kiểm thử chức năng WPS

Tổng kết chương 5

1. Lập báo cáo (3 LT)
   1. Tổng hợp thông tin
   2. Đánh dấu các thông tin quan trọng
   3. Thêm tài liệu hỗ trợ
   4. Đảm bảo chất lượng báo cáo

Tổng kết chương 6

1. Thực hành

|  |  |  |
| --- | --- | --- |
|  | ***1*** | ***TỔNG QUAN*** |
|  | 1.1 | Khái niệm cơ bản |
|  | 1.2 | Phương pháp luận kiểm thử |
|  | 1.3 | Quy trình kiểm thử |
|  | 2 | ***THU THẬP THÔNG TIN & XÁC ĐỊNH LỖ HỔNG*** |
|  | 2.1 | Kỹ thuật thu thập thông tin & xác định lỗ hổng |
|  | 2.2 | Vận dụng công cụ thu thập thông tin & xác định lỗ hổng |
|  | 2.2.1 | Thu thập thông tin & xác định lỗ hổng sử dụng nmap |
|  | 2.2.2 | Thu thập thông tin & xác định lỗ hổng sử dụng Google |
|  | 2.2.3 | Thu thập thông tin & xác định lỗ hổng sử dụng Shodan |
|  | 2.2.4 | Thu thập thông tin & xác định lỗ hổng sử dụng các công cụ khác |
|  | 3 | ***KIỂM THỬ HỆ THỐNG*** |
|  | 3.1 | Kỹ thuật kiểm thử hệ thống |
|  | 3.1.1 | Bẻ khóa mật khẩu |
|  | 3.2 | Vận dụng công cụ kiểm thử hệ thống |
|  | 3.2.1 | Vận dụng công cụ bẻ khóa mật khẩu |
|  | 3.2.2 | Vận dụng công cụ kiểm thử truy cập & leo thang đặc quyền |
|  | 3.2.3 | Vận dụng công cụ kiểm thử các tác vụ khác |
|  | 4 | ***KIỂM THỬ MÁY CHỦ & ỨNG DỤNG WEB*** |
|  | 4.1 | Kỹ thuật kiểm thử máy chủ & ứng dụng Web |
|  | 4.1.1 | Kỹ thuật thu thập thông tin máy chủ & ứng dụng Web |
|  | 4.1.2 | Kỹ thuật kiểm thử lỗ hổng máy chủ & ứng dụng Web |
|  | 4.1.2.1 | Kỹ thuật kiểm thử lỗ hổng XSS |
|  | 4.1.2.2 | Kỹ thuật kiểm thử lỗ hổng SQL injection |
|  | 4.1.2.3 | Kỹ thuật kiểm thử 1 số lỗ hổng ứng dụng web khác |
|  | 4.2 | Vận dụng công cụ kiểm thử máy chủ & ứng dụng Web |
|  | 4.2.1 | *Kiểm thử máy chủ & ứng dụng Web sử dụng Burp Suite* |
|  | 4.2.2 | *Kiểm thử máy chủ & ứng dụng Web sử dụng các công cụ khác* |
|  | 5 | ***KIỂM THỬ MẠNG KHÔNG DÂY*** |
|  | 5.1 | Kỹ thuật kiểm thử mạng không dây |
|  | 5.1.1 | *Tổng quan* |
|  | 5.1.2 | *Cơ chế hoạt động* |
|  | 5.1.3 | *Tấn công trong mạng không dây* |
|  | 5.2 | Vận dụng công cụ kiểm thử mạng không dây |
|  | 5.2.1 | *Kiểm thử mạng không dây sử dụng aircrack-ng* |
|  | 5.2.2 | *Kiểm thử mạng không dây sử dụng công cụ khác (kismet, netstumbler, reaver)* |