Chương 5

Hiện thực và bảo trì an toàn hệ thống mạng

Nội dung

- Nền tảng bảo mật
- Củng cố OS và NOS
- Củng cố các thiết bị mạng
- Củng cố các ứng dụng

5.1 Tổng quan các mối đe dọa mạng

- Cơ sở bảo mật:
  - Cần phát triển cơ sở tối thiểu hóa nhu cầu an toàn
  - Định nghĩa các cấp độ bảo mật
  - Cung cấp các thông tin đầu vào cho việc thiết kế, hiện thực và bảo trì tính bảo mật mạng
  - Chuẩn CC (Common Criteria): Canada, Pháp, Đức, Hà Lan, Anh và Mỹ. Gồm 7 cấp độ an toàn.

Chuẩn CC

- EAL 1: hệ thống hoạt động đúng, không xem yếu tố bảo mật là quan trọng
- EAL2: yêu cầu người thiết kế hệ thống sử dụng tốt các thủ tục thiết kế. Yếu tố bảo mật không có mức độ ưu tiên cao
- EAL 3: Yêu cầu phát triển cẩn thận cho mức độ an toàn
- EAL 4: đòi hỏi tích cực thiết kế bảo mật dựa trên các thủ tục an toàn được phát triển trong thương mại. Chuẩn để đo tính bảo mật các hệ thống.
- EAL 5: đảm bảo chắc chắn thiết kế bảo mật được xây dựng dựa trên các công cụ thương mại hóa từ giai đoạn đầu tiên. Mức độ bảo mật cao, các TH đặc biệt được xem xét
- EAL 6: cung cấp các mức độ bảo mật cao, chống các đe dọa lớn ở mức cao, chống xâm nhập ở mức cao
- EAL 7: các mức độ bảo mật cực cao. Yêu cầu mở rộng kiểm tra, đo đạc, và kiểm tra các thành phần riêng lẻ 1 cách độc lập.

- Ví dụ:
  - EAL 4: Sun Microsystems, September 2002, Sun Solaris 8, Operating Environment and Sun Trusted Solaris version 8 4/01
  - EAL 4+: Windows 2000, nếu phần hiện thực hệ thống không sử dụng các biện pháp bảo mật sẵn có thì hệ thống chỉ ở mức dưới EAL 4+

5.2 Củng cố OS và NOS

- Quá trình làm cho môi trường làm việc an toàn hơn
- Cấu hình các giao thức mạng
- Microsoft Windows 9*x*
- Củng cố Microsoft Windows NT 4
- Củng cố Microsoft Windows 2000
- Củng cố Microsoft Windows XP
- Củng cố Windows Server 2003
- Củng cố Unix/Linux
- Củng cố Novell NetWare
- Củng cố Apple Macintosh
- Củng cố hệ thống tập tin
- Cập nhật hệ điều hành

Cấu hình giao thức mạng

- NetBEUI
  - Khó bị tấn công từ bên ngoài
  - Vì NetBEUI không thể định tuyến -> không thể kết nối nó với mạng bên ngoài
- TCP/IP
  - Hiện nay được thiết kế hiện thực khá an toàn
- IPX/SPX
  - Giao thức hiệu quả, khả định tuyến, được thiết kế cho Novell Netware
  - Có thể định tuyến khi yêu cầu cấu hình router
  - NetBIOS có thể gán với IPX/SPX
- Không gán giao thức NetBIOS với bất kỳ giao thức khác.
- Protocol giao tiếp giữa client/server phải nằm vị trí đầu tiên trong list gán giao thức.

- Windows 9x
  - Cấu hình mạng, quản lý các dịch vụ, chia sẻ file, cập nhật các ứng dụng
  - Sử dụng System Policies để ngăn không cho thay đổi Registry.
  - System Policies đặt trên server và được download về cho mỗi kết nối client
- Windows NT 4
  - Có 6 service pack, SP6, SP6a
  - EAL 3
  - RAS, dịch vụ Web, FTP, chia sẻ tập tin
  - Tắt các dịch vụ không cần thiết.
  - Thiết lập các chính sách quản trị tài khoản

- Windows 2000
  - Cập nhật bảo mật: rất nhiều.
  - Tắt các dịch vụ IIS, FTP, và một số dịch vụ khác khi không cần
  - Microsoft TechNet http://www.microsoft.com/technet/default.mspx
  - Microsoft security http://www.microsoft.com/security/
  - System logs, báo cáo, các công cụ quản lý
  - Event Viewer
  - Performance Monitor
  - Active Directory, hạn chế: tất cả các máy trong mạng đều phải chạy windows 2000 hoặc cao hơn

- Windows XP
  - XP Home thay thế Windows 9x
  - XP Pro thay thế Windows 98, và 2000 Pro
  - Cài đặt các service pack
  - SP3

Củng cố hệ thống tập tin

- FAT, FAT16, FAT32: quyền truy xuất mức độ user và chia sẻ
  - User có quyền ghi hoặc thay đổi ổ đĩa, thư mục thì có quyền truy xuất đến toàn bộ các tập tin ở đó -> nguy hiểm trong Internet
- NTFS: hệ thống lưu giữ các giao tác, giúp phục hồi trạng thái khi hệ điều hành NT lỗi hoặc gặp sự cố mất điện.
  - Các tập tin, thư mục và ổ đĩa có thể có đặc tính bảo mật riêng.
  - Bảo mật của NTFS uyển chuyển và được xây dựng sẵn
  - Có các chương trình mã hóa tập tin đặc biệt lưu trữ dữ liệu trên đĩa cứng
  - Khuyến cáo: chi sẻ qua mạng nên sử dụng NTFS.

- Hệ thống tập tin Unix
  - Là hệ thống tập tin có cấu trúc đầy đủ.
  - Mỗi tập tin, hệ thống file, thư mục con có tính kiểm soát truy xuất nhất quán
  - 3 thuộc tính chính: Read, Write, và Execute.
  - Tính bảo mật cao nhất trong các hệ thống thương mại

Cập nhật hệ điều hành

- Hotfix
- Service patch
- Patch

5.3 Củng cố thiết bị mạng

- Cập nhật phần mềm điều khiển router, switch
- Có thể được cấu hình trước, người quản trị có thể cấu hình lại
- Cho phép thêm, mở rộng các đặc tính của thiết bị
- Có thể cấu hình các thiết bị dạng web
  - Cho phép và cấm các dịch vụ, các giao thức
  - Sử dụng ACL (Access Control List) để ngăn chặn sự xâm nhập trái phép của các IP

5.4 Củng cố các phần mềm

- Web Server
  - Lọc và kiểm soát truy cập đến các script
- E-mail Server
  - Sử dụng chương trình diệt virus
  - Quét định kỳ nhằm loại bỏ virus và các email rác
- FTP Server
  - Cho phép tạo tập tin trên bất kỳ ổ đĩa nào trong hệ thống
  - Nên tạo ổ đĩa hoặc thư mục riêng cho dịch vụ FTP
  - Sử dụng SSH, hoặc VPN trong dịch vụ
  - Tắt chế độ anymnomous
- DNS Server
  - Chú ý DNS DoS, Network footprint (NSLOOKUP), đảm bảo tính nhất quán của các record.

- Củng cố hệ thống tập tin, máy in và các dịch vụ
  - Tắt các dịch vụ liên quan NetBIOS
  - Các dịch vụ NetBIOS ở port 135, 137, 138, 139 dễ bị tấn công
  - Trên Unix, tắt port RPC 111.
  - Không nên share thư mục gốc
- Củng cố dịch vụ DHCP