HCMUTE

CHƯƠNG 7
An ninh mạng

GV. Nguyễn Thị Thanh Vân

Mục tiêu

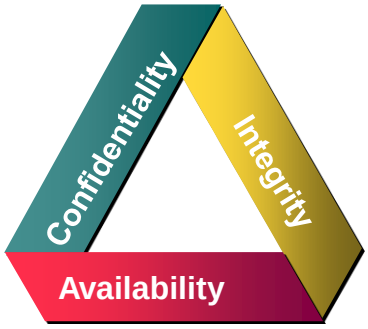
- Trình bày được một số khái niệm về lĩnh vực an ninh mạng
- Trình bày được các vấn đề cơ bản về chiến lược, giải pháp bảo mật
- Trình bày được một số đặc điểm cơ bản của các loại lỗ hổng bảo mật
- Trình bày được các dạng lỗ hổng, tấn công
- Trình bày được các hệ thống an ninh mạng
- Cài đặt được một tấn công đơn giản

Nội dung

- 7.1. Giới thiệu
- 7.2. Phân loại lỗ hổng mạng
- 7.3. Các dạng tấn công mạng
- 7.4. Một số tấn công mạng phổ biến
- 7.5. Các hệ thống an ninh mạng

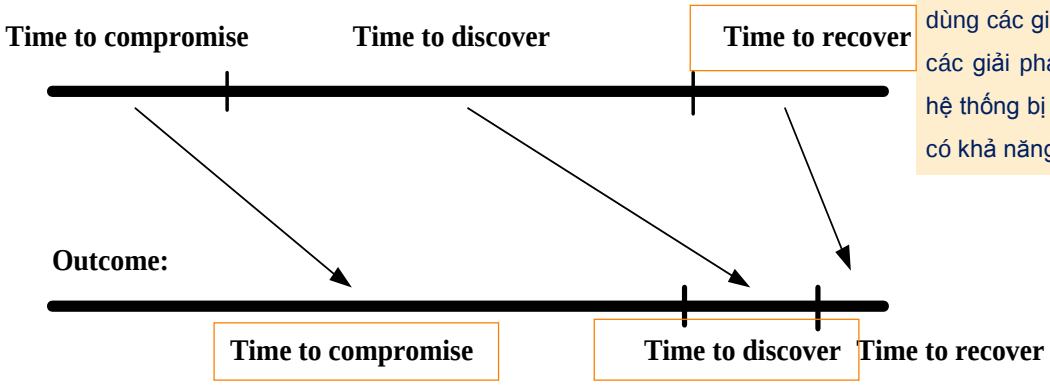
Giới thiệu
Tiêu chuẩn CIA

- Ba mục tiêu chính trong an toàn thông tin, thể hiện ở mô hình CIA (Confidentiality, Integrity, Availability)
  - Tính bí mật: đảm bảo rằng chỉ những người dùng hợp pháp mới có thể truy cập được hệ thống, dữ liệu.
  - Tính toàn vẹn: đảm bảo rằng dữ liệu không bị thay đổi bởi những người không được phép.
  - Tính sẵn sàng: đảm bảo rằng dữ liệu, hệ thống có thể phục vụ được việc truy cập của người dùng hợp pháp.



- Bất kỳ sự vi phạm nào trong ba tính chất trên đều dẫn đến nguy cơ mất an toàn thông tin.
- Môi trường mạng là public nên thông tin lưu truyền trên mạng có nhiều nguy cơ mất an toàn thông tin

Giới thiệu
Các giai đoạn bảo mật



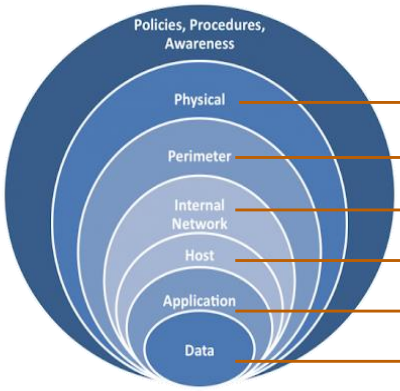
Giảm thời gian bằng cách dùng các giải pháp sử dụng các giải pháp để phòng khi hệ thống bị tấn công thì vẫn có khả năng khôi phục

Tăng thời gian bằng cách sử dụng các giải pháp để làm khó kẻ tấn công

Giảm thời gian bằng cách dùng các giải pháp để nhận diện sớm các tấn công

Giới thiệu
Bảo mật nhiều lớp

- Giải pháp bảo mật nhiều lớp:
  - được xem xét áp dụng để việc bảo mật toàn diện có hiệu quả.
  - còn có tên gọi khác là bảo vệ theo chiều sâu (defense-in-depth)



- Lock, Camera
- UTM, Firewall, VPN, Routers,…
- VLAN, IPS, IDS,…
- OS, Update Management, Enpoint Security,…
- Application Control, Antivirus,…
- AAA, Encryption, Digital Signature…

Giới thiệu
Chiến lược bảo vệ

- Bảo mật thông tin trên mạng theo chiến lược P-P-T
  - Con người: tuyển dụng người tài, đào tạo và trọng thưởng họ.
  - Công nghệ: đánh giá, thực hiện, kiểm tra và cải tiến.
  - Qui trình: bảo đảm sự cẩn trọng, phản ứng với các xâm phạm và chuẩn bị khôi phục các dữ liệu nhạy cảm

Phân loại lỗ hổng

- Lỗ hổng bảo mật là những điểm yếu, lỗi của hệ thống, khi bị khai thác sẽ dẫn tới rủi ro nghiêm trọng
- Các dạng:
  - Điểm yếu về mặt kỹ thuật gồm có điểm yếu trong giao thức, trong các hệ điều hành và các thiết bị phần cứng
  - Điểm yếu trong cấu hình hệ thống: do người quản trị tạo ra khi có các thiếu sót trong việc cấu hình hệ thống như: sử dụng các cấu hình mặc định, password đơn giản…
  - Điểm yếu trong chính sách bảo mật
    - Các cách thức, quy định và vị trí thực hiện chứa đựng nhiều bất ổn.
    - Mỗi công ty, tổ chức nên xây dựng chính sách bảo mật đặc thù cho đơn vị mình

Các dạng tấn công mạng

- Tấn công chủ động: kẻ tấn công làm thay đổi hoạt động của hệ thống và hoạt động của mạng khi tấn công làm ảnh hưởng đến tính toàn vẹn, sẵn sàng và xác thực của dữ liệu

- Tấn công bị động: kẻ tấn công cố gắng thu thập thông tin từ hoạt động của hệ thống và hoạt động của mạng làm phá vỡ tính bí mật của dữ liệu

Các dạng tấn công mạng

- Tấn công từ bên trong:
  - Người sử dụng muốn truy cập, lấy thông tin nhiều hơn quyền cho phép.
  - Chia sẻ thông tin ra bên ngoài
  - Tìm, yêu cầu truy xuất và lưu thông tin quan trọng
  - Cố vượt qua các giải pháp bảo mật
  - ….
- Tấn công từ bên ngoài: là những tấn công xuất phát từ bên ngoài Internet hay các kết nối truy cập từ xa.

Một số tấn công phổ biến

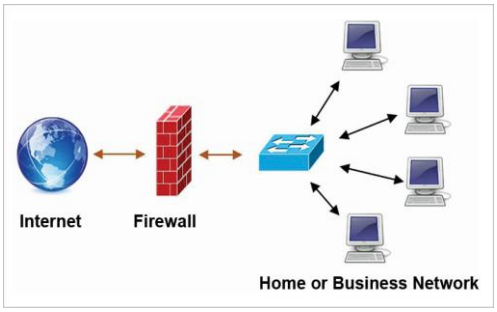
- Tấn công vào các trang Web: Website bị hacker tấn công chủ yếu do các vấn đề:
  - Lỗi kiểm soát truy cập: Việc truy cập vào các ứng dụng web không được bảo vệ an toàn sẽ bị các
  - Lỗ hổng phần mềm: Những phần mềm dùng viết và quản lý website cúng có những lỗ hổng như: máy chủ web, cơ sở hạ tầng, công cụ viết web....
- Tấn công từ chối dịch vụ - Denied of services. Dấu hiệu của một vụ tấn công từ chối dịch vụ gồm có:
  - Mạng thực thi chậm khác thường khi truy cập Website;
  - Không thể dùng một website cụ thể;
  - Tăng lượng thư rác nhận được.
- Tấn công bằng mã độc - Malicious software:
  - loại phần mềm được tạo ra và chèn vào hệ thống một cách bí mật
  - mục đích thâm nhập, phá hoại hệ thống hoặc lấy cắp thông tin, làm gián đoạn, tổn hại tới tính bí mật, tính toàn vẹn và tính sẵn sàng của máy tính nạn nhân.
  - Một số mã độc phổ biến như: virus, worm, trojan

Một số tấn công phổ biến
Các giải pháp hạn chế

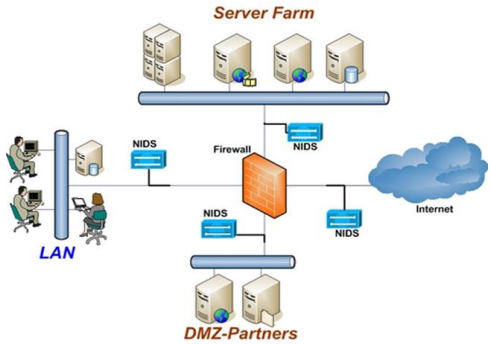
- Đối với cá nhân
  - Bảo vệ mật khẩu cá nhân bằng cách: đặt mật khẩu phức tạp, bật tính năng bảo mật 2 lớp – xác nhận qua điện thoại,…
  - Hạn chế truy cập vào các điểm Wifi công cộng
  - Không sử dụng phần mềm bẻ khóa (crack)
  - Luôn cập nhật phần mềm, hệ điều hành lên phiên bản mới nhất.
  - Cẩn trọng khi duyệt Email, kiểm tra kỹ tên người gửi để phòng tránh lừa đảo.
  - Tuyệt đối không tải các File hoặc nhấp vào đường link không rõ nguồn gốc.
  - Hạn chế sử dụng các thiết bị ngoại vi (USB, ổ cứng) dùng chung.
  - Sử dụng một phần mềm diệt Virus uy tín.

Các hệ thống an ninh mạng
Firewall. Intrusion Detection System

- Firewall là phần cứng hoặc phần mềm máy tính kiểm soát các truy cập vào/ra hệ thống thông qua các luật (rules).

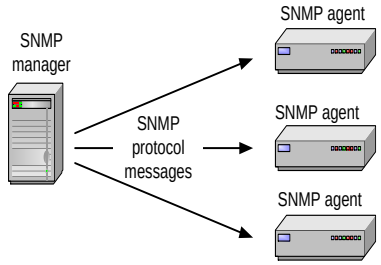


- IDS là một hệ thống lắng nghe, giám sát lưu lượng mạng và phát cảnh báo khi phát hiện bất kỳ loại xâm nhập nào vào hệ thống mạng.

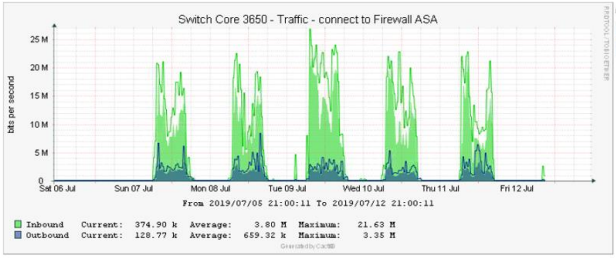


Các hệ thống an ninh mạng
Giám sát mạng

- Chức năng: theo dõi tình trạng của các thiết bị và dịch vụ nhằm phát hiện kịp thời những bất thường, đảm bảo hệ thống hoạt động ổn định.
  - Manager: nằm trên máy chủ giám sát hệ thống mạng
  - Agent:chương trình nằm trên các thiết bị cần giám sát, quản lý.
  - SNMP là một giao thức chính được sử dụng để theo dõi tình trạng hoạt động của các thiết bị và dịch vụ trong hệ thống mạng,

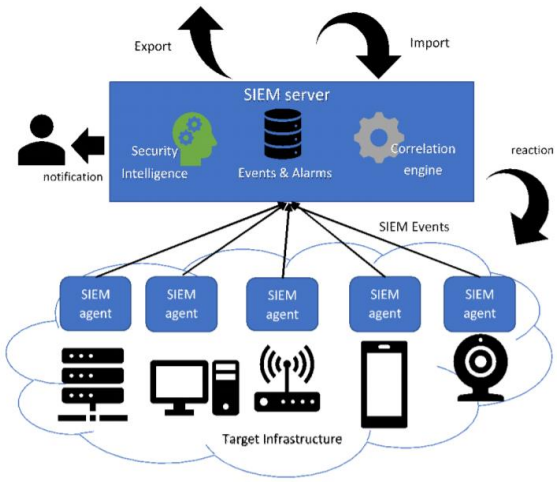


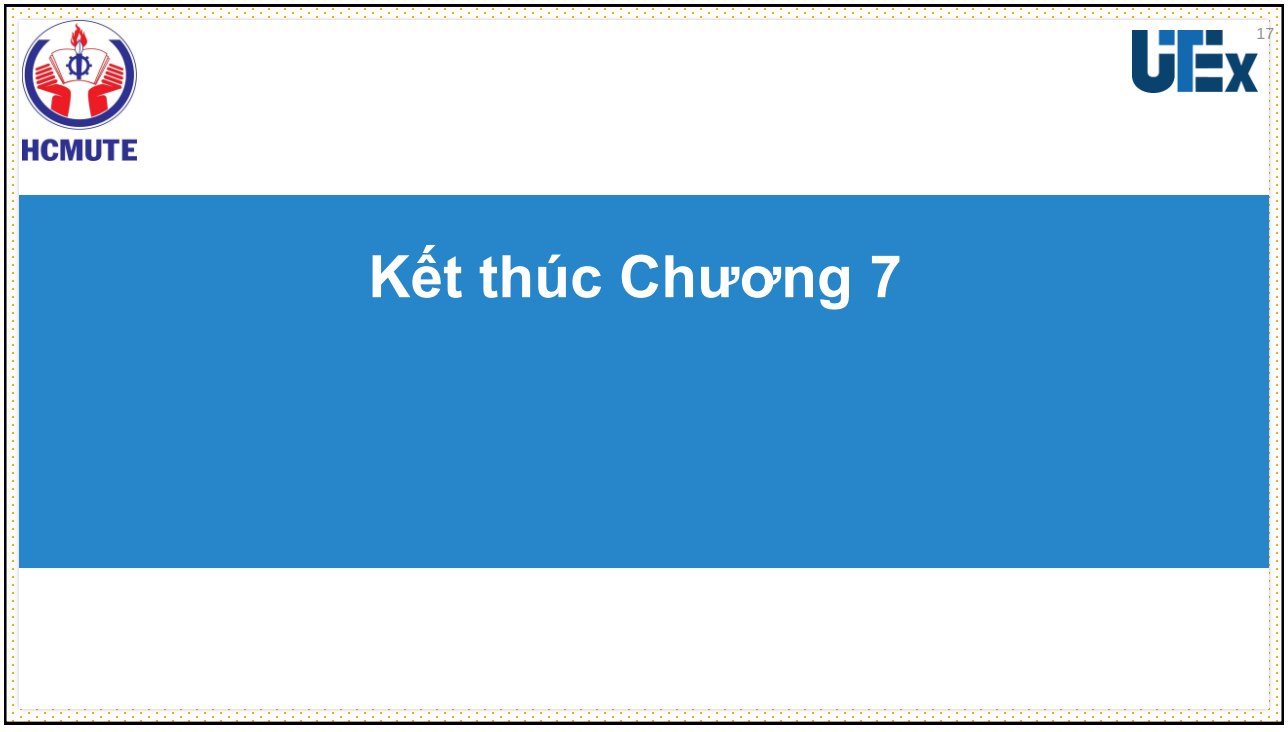
- Các thông tin giám sát:
  - Lưu lượng mạng
  - Tình trạng hoạt động
  - Dịch vụ
  - Tài nguyên của thiết bị



Các hệ thống an ninh mạng
SIEM

- SIEM (Security Information and Event Management) được thiết kế để thu thập các sự kiện an ninh từ các thiết bị đầu cuối và lưu trữ dữ liệu một cách tập trung, cho phép phân tích tập trung và báo cáo sự kiện an toàn của một hệ thống mạng, có thể phát hiện các cuộc tấn công




HCMUTE
17
Kết thúc Chương 7