Chương

1

Tổng quan về bảo mật

Nội dung

- Giới thiệu về bảo mật
- Những tài nguyên cần bảo vệ
- Hacker là ai?
- Những lỗ hổng bảo mật
- Các kiểu tấn công của hacker
- Các biện pháp phát hiện hệ thống bị tấn công
- Các quy tắc bảo mật
- Xây dựng chính sách bảo mật

Giới thiệu về bảo mật

- Bảo mật là nhu cầu tất yếu của sự phát triển CNTT
- Hệ thống mạng luôn tiềm ẩn những mối nguy hiểm tiềm tàng
- Số vụ tấn công hệ thống không ngừng tăng lên
- Internet là một nơi cực kỳ hỗn loạn
- Internet là một nơi không an toàn

Những tài nguyên cần bảo vệ

- Dữ liệu và những yếu tố cần quan tâm:
  - Tính bảo mật
  - Tính toàn vẹn dữ liệu
  - Tính sẵn sàng
  - Tính chính xác
  - Tính không khước từ

Những tài nguyên cần bảo vệ

- Hệ thống máy tính
- Bộ nhớ
- Hệ thống ổ đĩa
- Máy in và nhiều tài nguyên trên hệ thống máy tính
- Các thiết bị mạng
- Thông tin cá nhân.

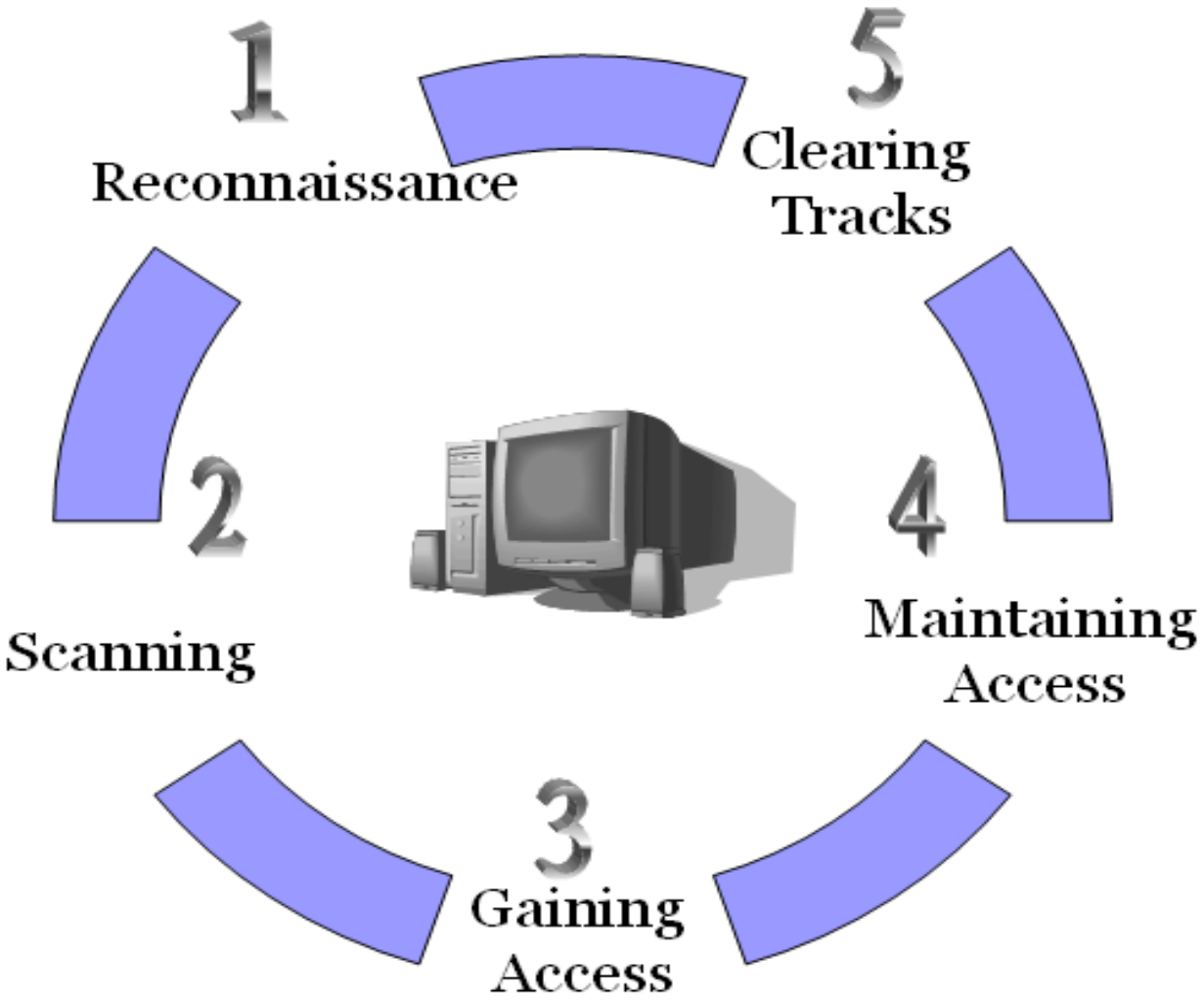
Hacker là ai?

- Hacker là lập trình viên giỏi
- Hacker là chuyên gia mạng và hệ thống
- Hacker là chuyên gia phần cứng
- Các lớp hacker:
  - Hacker mũ đen
  - Hacker mũ trắng
  - Hacker mũ xám

Những lỗ hổng bảo mật

- Các lỗ hổng loại A có mức độ rất nguy hiểm
- Các lỗ hổng loại B có mức độ nguy hiểm hơn lỗ hổng loại C
- Các lỗ hổng loại B khác là các chương trình có mã nguồn viết bằng C
- Các lỗ hổng loại C cho phép tấn công DoS

Quá trình tấn công hệ thống



Quá trình tấn công hệ thống

- Reconnaissance: trinh sát chủ động và thụ động.
- Scanning: quét hệ thống mục tiêu
- Gaining Access: xâm nhập hệ thống
- Maintaining Access: duy trì truy cập cho lần sau
- Covering Track: Che đậy dấu vết để không bị phát hiện

Các kiểu tấn công của hacker

- Tấn công trực tiếp: sử dụng máy tính và các phần mềm công cụ
- Sử dụng “Kỹ thuật đánh lừa” để tấn công
- Kỹ thuật tấn công vào vùng ẩn
- Tấn công vào các lỗ hổng bảo mật
- Tấn công khai thác tình trạng tràn bộ đệm
- Sử dụng kỹ thuật “Nghe trộm”

Các kiểu tấn công của hacker

- Sử dụng kỹ thuật giả mạo địa chỉ
- Sử dụng kỹ thuật chèn mã lệnh
- Tấn công vào hệ thống có cấu hình không an toàn
- Tấn công dùng Cookies
- Tấn công can thiệp vào tham số trên URL
- Tấn công vô hiệu hóa dịch vụ DoS

Các kiểu tấn công khác

- Tấn công lỗ hổng không cần đăng nhập
- Tấn công thay đổi dữ liệu
- Tấn công dùng mật khẩu mặc định
- Tấn công giả danh

Biện pháp phát hiện bị tấn công

- Kiểm tra các dấu hiệu hệ thống bị tấn công
- Kiểm tra các tài khoản người dùng mới trên hệ thống
- Kiểm tra sự xuất hiện các tập tin lạ
- Kiểm tra thay đổi thời gian trên hệ thống
- Kiểm tra hiệu năng của hệ thống

Biện pháp phát hiện bị tấn công

- Kiểm tra hoạt động của các dịch vụ
- Kiểm tra truy nhập hệ thống bằng các tài khoản thông thường
- Kiểm tra các tập tin liên quan đến cấu hình mạng và dịch vụ
- Kiểm tra các phiên bản của sendmail, /bin/mail, FTP

Các quy tắc bảo mật

- Quy tắc 1: Nếu một người nào đó có thể thuyết phục bạn **chạy chương trình của anh ta trên máy tính của bạn**, khi đó máy tính sẽ không còn là của bạn nữa.
- Quy tắc 2: Nếu một người nào đó có thể **sửa đổi hệ điều hành trên máy tính của bạn**, khi đó máy tính sẽ không còn là của bạn nữa.
- Quy tắc 3: Nếu một người nào đó **truy cập vật lý không hạn chế tới máy tính của bạn**, khi đó máy tính sẽ không còn là của bạn nữa.

Các quy tắc bảo mật

- Quy tắc 4: Nếu bạn cho phép một người nào đó **đẩy các chương trình tới website của bạn**, khi đó website sẽ không còn là của bạn nữa.
- Quy tắc 5: Các mật khẩu dễ nhận có thể làm hỏng hệ thống bảo mật mạnh.
- Quy tắc 6: Một hệ thống chỉ có độ an toàn như sự tin tưởng nhà quản trị.

Các quy tắc bảo mật

- Quy tắc 7: Dữ liệu được mã hóa chỉ như chìa khóa giải mã.
- Quy tắc 8: Một hệ thống quét virus hết hạn thì cũng còn tốt hơn không có hệ thống diệt virus nào.
- Quy tắc 9: Tình trạng dấu tên hoàn toàn không thực tế.
- Quy tắc 10: Công nghệ không phải là tất cả.

Xây dựng chính sách bảo mật

- Các bước chuẩn bị
  - Xác định đối tượng cần bảo vệ
  - Xác định nguy cơ đối với hệ thống
  - Xác định phương án thực thi chính sách bảo mật
- Thiết lập các quy tắc
  - Các thủ tục đối với hoạt động truy nhập không hợp lệ
  - Triển khai chính sách bảo mật

Xây dựng chính sách bảo mật

- Thiết lập các thủ tục bảo vệ hệ thống
  - Thủ tục quản lý tài khoản người sử dụng
  - Thủ tục quản lý mật khẩu
  - Thủ tục quản lý cấu hình hệ thống
  - Thủ tục sao lưu và khôi phục dữ liệu
  - Thủ tục báo cáo sự cố

Tổng kết

- Hiểu các thuật ngữ cần thiết của hacker
- Hiểu sự khác biệt giữa hacker mũ trắng và cracker
- Biết các lớp hacker
- Biết các giai đoạn của hacker
- Nhận thức được các loại tấn công
- Hiểu về các loại kiểm tra an ninh
- Biết nội dung của báo cáo hacker mũ trắng

Tài nguyên học tập

- Giáo trình học “Hacker mũ trắng”.
- Bộ công cụ phục vụ học tập.
- Video demo.
- Các website tài liệu tham khảo:
  - http://www.securiteam.com
  - http://www.securityfocus.com
  - http://www.securitytracker.com
  - http://ceh.vn
  - http://hvaonline.net

Tài nguyên học tập

- Giáo trình học “Hacker mũ trắng”.
- Bộ công cụ phục vụ học tập.
- Video demo
- Tài liệu tham khảo:
  - http://www.securiteam.com
  - http://www.securityfocus.com
  - http://www.securitytracker.com
  - http://ceh.vn
  - http://hvaonline.net