HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG
Posts and Telecommunications Institute of Technology

KIỂM THỬ XÂM NHẬP

KHOA AN TOÀN THÔNG TIN
TS. ĐINH TRƯỜNG DUY

HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG
Posts and Telecommunications Institute of Technology

KIỂM THỬ XÂM NHẬP

Giới thiệu về kiểm thử xâm nhập

KHOA AN TOÀN THÔNG TIN
TS. ĐINH TRƯỜNG DUY

Biên soạn từ bài giảng: Nguyễn Ngọc Điệp, Bài giảng Kiểm thử xâm nhập, Học viện Công nghệ Bưu chính Viễn thông, 2021.

1.1 KHÁI NIỆM VÀ VAI TRÒ CỦA KIỂM THỬ XÂM NHẬP

1.1.1. Tổng quan về An toàn thông tin

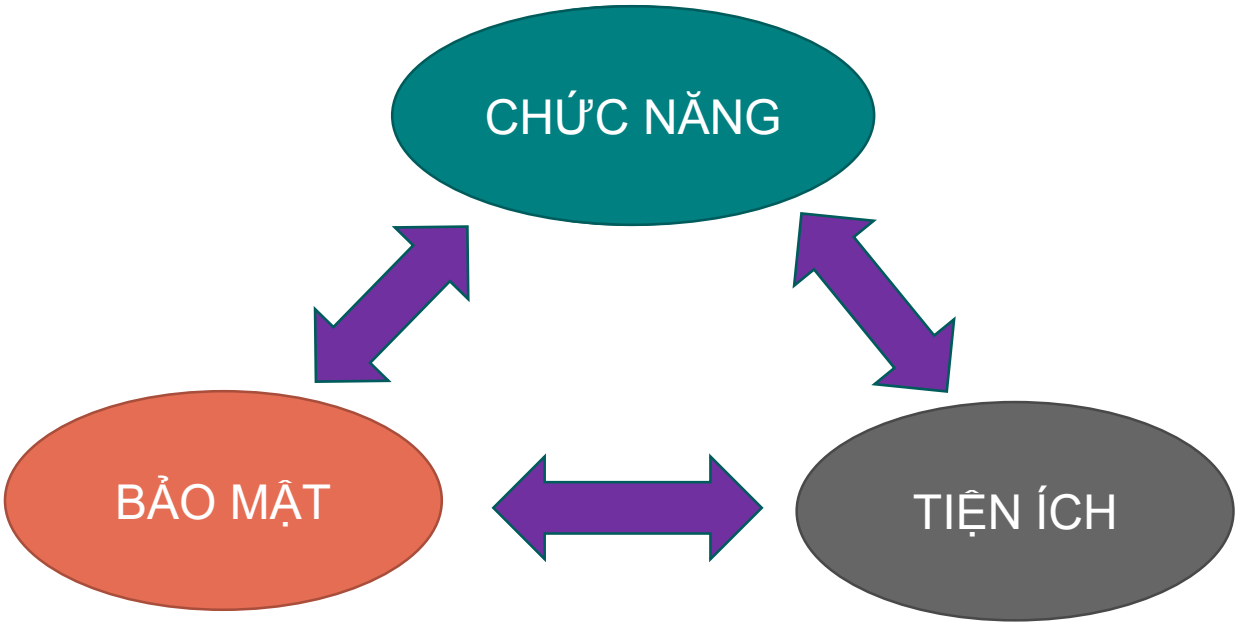
1.1.2. Một số kĩ thuật tấn công và giải pháp phòng chống

KHÁI NIỆM VÀ VAI TRÒ CỦA KIỂM THỬ XÂM NHẬP

- Tổng quan về an ninh mạng
- Khái niệm về tấn công mạng (hack)
- Các giai đoạn tấn công mạng
- Các loại tấn công mạng
- Kiểm thử xâm nhập
- Nghiên cứu lỗ hổng

Tổng quan về an ninh mạng

- Mức độ bảo mật của hệ thống có thể được xác định bởi khả năng của ba thành phần:



Mô hình tam giác

Tổng quan về an ninh mạng

- Các thách thức cần quan tâm:
  - Gia tăng tội phạm mạng tinh vi
  - Rò rỉ dữ liệu,thất thoát trong nội bộ và nhân viên làm việc xa
  - An ninh di động,xác thực và các phương tiện truyền thông xã hội
  - Nguồn nhân lực an ninh mạng
  - Khai thác các lỗ hổng ,vận hành hệ thống an ninh
  - Bảo vệ các cơ sở hạ tầng quan trọng
  - Cân bằng giữa việc công và tư
  - Tiếp cận với việc nhận dạng các chiến thuật và chu trình.

Tổng quan về an ninh mạng

- Danh sách các nguy cơ an ninh:

Trojans, đánh cắp thông tin, keylogger,…	Vishing
Mạng ma Flux Botnet	Chợ đen
Thất thoát giữ liệu,vi phạm an ninh	Tống tiền trên mạng
Các mối đe dọa an ninh trong nội bộ	Di chuyển dữ liệu (usb,máy tính xách tay,băng sao lưu..)
Tổ chức tội phạm mạng	Mạng ma
Lừa đảo	Lỗ hổng trong công nghệ mới
Các loại virus mới	Dự án gia công phần mềm
Gián điệp mạng	Mạng xã hội
Zero-Day	Gián đoạn kinh doanh
Mối đe dọa từ web 2.0	Công nghệ ảo hóa và điện toán đám mây

Khái niệm tấn công mạng (hack) (1)

- Ảnh hưởng của tấn công mạng
  - Theo thông tin nghiên cứu an ninh quốc gia Symantec, các cuộc tấn công của hacker gây thiệt hại cho các doanh nghiệp lớn khoản 2,2 triệu $ mỗi năm.
  - Hành vi trộm cắp tài khoản của khách hàng có thể làm giảm danh tiếng của doanh nghiệp.
  - Hacker có thể ăn cắp bí mật thông tin tài chính, hợp đồng quan trọng và bán chúng cho đối thủ cạnh tranh.
  - Botnet có thể được sử dụng để khởi động DOS và các cuộc tấn công dựa trên web khác, dẫn đến các doanh nghiệp bị giảm doanh thu.
  - Có thể làm các công ty phá sản.

Khái niệm tấn công mạng (hack) (2)

- Khái niệm hacker
  - Một người thông minh với kỹ năng máy tính xuất sắc, có thể tạo ra hay khám phá các phần mềm và phần cứng máy tính
  - Đối với một số hacker hack là một sở thích của họ có thể tấn công nhiều máy tính hoc mạng
  - Mục đích của họ là tìm hiểu kiến thức hoặc phá hoại bất hợp pháp
  - Một số mục đích xấu của hacker từ việc hack như: đánh cắp dữ liệu kinh doanh, thông tin thẻ tín dụng, sổ bảo hiểm xã hội, mật khẩu e-mail
- Các loại hacker
  - Mũ đen
  - Mũ trắng
  - Khủng bố (suicide hacker)
  - Mũ xám
  - Script Kiddie

Các giai đoạn tấn công (1)

1. Trinh sát
2. Quét
3. Truy cập
4. Duy trì truy cập
5. Xóa dấu vết

Các giai đoạn tấn công: Trinh sát

- Trinh sát đề cập đến giai đoạn chuẩn bị để một kẻ tấn công tìm kiếm để thu thập thông tin về 1 mục tiêu trước khi tung ra một cuộc tấn công.
- Mục đích chính là tìm hiểu một lượng lớn thông tin của mục tiêu để việc tấn công trong tương lai trở nên dễ dàng hơn.
- Phạm vi trinh sát mục tiêu có thể bao gồm các khách hàng, nhân viên, hoạt động, mạng, và hệ thống,..
- Các loại trinh sát
  - Trinh sát thụ động: Trinh sát mục tiêu mà không cần trực tiếp tương tác với mục tiêu. Vd : tìm kiếm hồ sơ công khai hoặc các bản tin đã phát hành.
  - Trinh sát chủ động: Trinh sát mục tiêu cần phải trực tiếp tương tác với mục tiêu qua nhiều phương tiện. Vd : các cuộc gọi để gọi để lấy thông tin kĩ thuật cá nhân

Các giai đoạn tấn công: Quét

- Trước khi tấn công, trên cơ sở các thông tin thu thập được qua quá trình trinh sát, kẻ tấn công quét mạng lưới thông tin của mục tiêu.
- Quét có thể bao gồm việc sử dụng các trình quay số, máy quét cổng, lập bản đồ mạng, quét bao quát, quét lỗ hổng,..
- Kẻ tấn công khai thác các thông tin như tên máy tinh, địa chỉ IP, và tài khoản người dùng để bắt đầu tấn công.

Các giai đoạn tấn công: Truy cập

- Truy cập dùng để chỉ việc kẻ tấn công có được quyền truy cập vào hệ thống điều hành hoặc ứng dụng mạng
- Kẻ tấn công có thể truy cập ở cấp hệ điều hành, cấp ứng dụng hoặc cấp mạng.
- Kẻ tấn công có thể nâng cấp quyền để có thể truy cập toàn bộ hệ thống. kẻ tấn công đoạt được quyền kiểm soát hệ thống rồi mới khai thác thông tin.
- Vd : bẻ mật khẩu, tràn bộ đệm, từ chối dịch vụ, đánh cắp tài khoản,..

Các giai đoạn tấn công: duy trì truy cập

- Duy trì truy cập nói đến việc kẻ tấn công cố gắng giữ lại quyền sở hữu hệ thống.
- Kẻ tấn công sử dụng các hệ thống đã chiếm được để bắt đầu các cuộc tấn công tiếp theo.
- Kẻ tấn công có thể giữ quyền sở hữu hệ thống của mình khỏi những kẻ tấn công khác bằng backdoors, rootkits, hoặc trojan.
- Kẻ tấn công có thể thực hiện tất cả các thao tác với dữ liệu của hệ thống đang sở hữu.

Các giai đoạn tấn công: xóa dấu vết

- Kẻ tấn công tiến hành xóa các bản ghi trên máy chủ, hệ thống và các ứng dụng để tránh bị nghi ngờ..
- Mục đích:
  - Là các hoạt động để che giấu hành vi tấn công của kẻ tấn công.
  - Tiếp tục truy cập vào hệ thống của nạn nhân vì không bị chú ý và phát hiện, xóa bằng chứng liên quan đến bản thân.

Các loại tấn công (1)

- Tấn công vào hệ điều hành
  - Kẻ tấn công tìm kiếm các lỗ hổng của hệ điều hành và khai thác chúng để truy cập vào hệ thống mạng. Các lỗ hổng như :
  - ❑Lỗ hổng tràn bộ đệm
  - ❑Lỗi trong hệ điều hành
  - ❑Hệ điều hành chưa vá lỗi
- Tấn công cấp ứng dụng
  - -Phần mềm ứng dụng đi kèm với nhiều chức năng nên dễ phát sinh lỗi
  - -Phát hành gấp rút nên thiếu thời gian thử nghiệm

Các loại tấn công (2)

- Tấn công vào cấu hình sai
  - Khi một hệ thống bị lỗi cấu hình, như sự thay đổi trong quyền truy cập vào tập tin, thì nó đã trở nên không an toàn.
  - Các quản trị viên sẽ thiết lập các cấu hình thiết bị trước khi triển khai trong mạng. nếu không có những thiết lập mặc định này thiết bị sẽ dễ dàng bị tấn công.
- Tấn công gói tin nhỏ
  - Khi cài đặt các hệ điều hành hoặc phần mềm ứng dụng thì bản mẫu sẽ có các mặc định để việc quản lý trở nên dễ dàng hơn. Khi chúng ta thay đổi các mặc định đó thì sẽ lộ ra các lỗ hổng để cho nhưng kẻ tấn công có thể khai thác và tấn công vào các gói tin nhỏ.

Vấn đề về kiểm thử xâm nhập mạng

- Không có mạng nào là an toàn tuyệt đối.
- Giúp đưa ra các chiến lược theo chiều sâu. Tức là việc phân tích, xâm nhập vào mạng của chính mình và tiếp xúc cũng như tính toán về chúng.
- Kiểm thử xâm nhập mạng là cần thiết bởi vì nó cho phép phòng chống các cuộc tấn công từ hacker bằng cách dự đoán các cách tấn công mà họ có thể sử dụng để xâm nhập vào một hệ thống.
- Phòng thủ chiều sâu:
  - Phòng thủ chiều sâu là một chiến lược an ninh trong đó một số lớp bảo vệ được đặt trên toàn bộ hệ thống thông tin
  - Nó giúp ngăn chặn các cuộc tấn công vì khi kẻ tấn công qua một lớp thì sẽ gặp lớp phòng thủ tiếp theo

Kiểm thử xâm nhập mạng

- Ưu điểm
  - Là một phần quan trọng của đánh giá nguy cơ, kiểm toán, quản trị hệ thống,..
  - Được sử dụng để nhận diện rủi ro làm các hoạt động khắc phục hậu quả và làm giảm nguy cơ an toàn hệ thống thông qua việc giải quyết các lỗ hổng
- Hạn chế
  - Chỉ khi các doanh nghiệp biết hệ thống của họ có lỗi họ mới thuê kiểm tra hệ thống của mình và cũng chỉ có một lần duy nhất.
  - Chỉ có các tổ chức cần có bảo vệ mạng mới có nhu cầu

Nghiên cứu lỗ hổng (1)

- **Định nghĩa**
  - Quá trình phát hiện ra các lỗ hổng trong thiết kế để tấn công hoặc lợi dụng hệ điều hành và các ứng dụng của nó.
  - Các lỗ hổng thường được phân loại dựa trên mức độ nghiêm trọng (thấp, trung bình, cao) và phạm vi khai thác (cục bộ hoặc từ xa).
- **Mục đích**
  - Để xác định và sửa chữa các lỗ hổng mạng
  - Để bảo vệ mạng khỏi bị tấn công bởi những kẻ xâm nhập
  - Thu thập thông tin về các loại virus
  - Để có được thông tin giúp giải quyết các vấn đề an ninh
  - Để tìm ra các điểm yếu và cảnh báo người quản trị mạng trước khi bị tấn công
  - Để biết làm sao khôi phục được các thiết bị sau khi bị tấn công.

Nghiên cứu lỗ hổng (2)

- Kiểm thử xâm nhập là một phương pháp chủ động đánh giá sự an toàn của mạng hoặc hệ thống thông tin bằng cách mô phỏng các cuộc tấn công từ một nguồn độc hại.
- Tích cực phân tích những điểm yếu thiết kế sai sót kĩ thuật và các lỗ hổng.
- Trong một cuộc kiểm tra :
  - Hộp đen mô phỏng một cuộc tấn công từ một người không có kiến thức về hệ thống
  - Hộp trắng mô phỏng một cuộc tấn công từ một người có thông tin/ kiến thức về hệ thống.
- Kết quả được gửi toàn bộ trong một báo cáo để người sử dụng có thể kiểm tra về điều hành, quản lý và kĩ thuật

Nghiên cứu lỗ hổng (3)

- Tại sao phải tiến hành kiểm thử xâm nhập
  - Xác định các mối đe dọa đối với hệ thống thông tin của một tổ chức.

  → Xác định, giải quyết các lỗ hổng và điểm yếu trong đầu tư an ninh để cung cấp lại tốt hơn.
  - Cung cấp cho một tổ chức với một sự bảo đảm – một đánh kỹ lưỡng và toàn diện về an ninh bao gồm chính sách, thủ tục, thiết kế, và thực hiện.

  → Đạt được và duy trì chứng nhận theo quy định nghành công nghiệp.
  - Cung cấp các sản phẩm tốt nhất tuân theo các quy định của pháp luật và công nghiệp.

  → Tập trung vào các lỗ hổng có mức độ nghiêm trọng cao. Nhấn mạnh các vấn đề bảo mật ứng dụng cho các nhà phát triển và các nhà quản lý.
  - Cung cấp một phương pháp chuẩn bị toàn diện để có thể ngăn chặn các cuộc tấn công.

  → Đánh giá hiệu quả của các thiết bị an ninh mạng như firewall, route, và web server.

Phương pháp xâm nhập thử nghiệm