Từ Điển Chuyên Ngành

Hỗ Trợ Công Nghệ Thông Tin

Khóa 5: Bảo mật trong CNTT

Từ và Định nghĩa

A

Adware (phần mềm quảng cáo): loại phần mềm hiển thị quảng cáo và thu thập dữ liệu.

Availability (tính sẵn sàng): thông tin có thể dễ dàng truy cập được đối với những người cần nó.

B

Backdoor (cửa hậu): một lối xâm nhập bí mật vào hệ thống của những kẻ tấn công.

Bot: máy tính bị cài đặt phần mềm tự động thực hiện các nhiệm vụ qua mạng internet.

Botnet: một mạng lưới các máy kết nối Internet bị kẻ tấn công sử dụng thực hiện một số chức năng phân tán

Brute-force attack (tấn công vét cạn): một phương pháp tấn công đoán mật khẩu hoặc chuỗi khóa cho đến khi tìm được một cái đúng.

C

Cipher (phép mã hóa): phép biến đổi để chuyển một thông điệp từ bản rõ thành dạng thông điệp bị cắt xén và không thể đọc hiểu.

Confidentiality (tính bảo mật): giữ mọi thứ được giấu kín.

Cryptology (mật mã học): ngành nghiên cứu cách thức thực hiện mã hóa và ẩn thông điệp.

D

Daemon process: tiến trình chạy nền bên dưới.

E

Encryption (mã hóa): hành động lấy một thông điệp và thực hiện phép biến đổi trên nó để được một thông điệp mới không thể hiểu nội dung.

Exploit (khai thác): tận dụng lỗ hổng của hệ thống để tấn công.

H

Handshake process (quá trình bắt tay): quá trình trao đổi dữ liệu giữa máy khách và điểm truy cập để chia sẻ khóa cho quá trình mã hóa thông điệp giao tiếp.

Hashing (băm): thao tác nhận đầu vào dữ liệu bất kỳ và ánh xạ nó thành đầu ra có kích thước cố định.

I

Integrity (tính toàn vẹn): giữ cho dữ liệu chính xác và không bị can thiệp.

Internet Protocol Security (IPsec): một giao thức VPN mã hóa gói IP và đóng gói nó bên trong một gói Ipsec.

K

Keylogger: chương trình ghi lại mọi thao tác bàn phím của người dùng.

L

Layer 2 Tunnel Protocol (L2TP): một giao thức đường hầm cho phép đóng gói các giao thức khác hoặc các lưu thông mà không được hỗ trợ bởi mạng hiện tại.

M

Malware (phần mềm độc hại): loại phần mềm nhằm đánh cắp thông tin nhạy cảm, xóa, hoặc sửa đổi các tập tin.

O

OpenVPN: một VPN sử dụng thư viện OpenSSL để xử lý việc trao đổi khóa và mã hóa dữ liệu cùng với các kênh điều khiển.

P

PCI-DSS: một tiêu chuẩn bảo mật thẻ thanh toán mà các công ty cần đề ra cho mục tiêu bảo mật khi hỗ trợ khách hàng thanh toán bằng thẻ tín dụng, nó bao gồm 6 mục tiêu lớn.

Pretty Good Privacy (PGP): một ứng dụng mã hóa cho phép xác thực dữ liệu cùng với quyền riêng tư từ các bên thứ ba dựa trên mã hóa bất đối xứng.

Privacy policy (chính sách quyền riêng tư): các hướng dẫn việc truy cập và sử dụng dữ liệu nhạy cảm, những thông tin cá nhân của người dùng.

R

Ransomware: loại phần mềm nhằm đánh cắp thông tin nhạy cảm, xóa, hoặc sửa đổi các tập tin.

Rootkit: loại phần mềm có quyền sửa đổi ở cấp quản lý đối với hệ điều hành.

S

SSH (Secure shell): một giao thức mạng thiết lập các giao tiếp giữa các máy tính một cách bảo mật thường dùng để điều khiển máy tính và thực thi các lệnh.

Security goal (mục tiêu bảo mật): những yêu cầu về một kiến trúc bảo mật mà doanh nghiệp mong muốn đạt được để cân bằng giữa mức độ an ninh của hệ thống và năng suất của người dùng.

Social engineering attack (tấn công phi kỹ thuật): cách thức tấn công nhằm vào con người để lừa đảo quyền truy cập thông tin cá nhân hoặc lừa nạn nhân thực hiện điều nào đó.

Spyware (phần mềm gián điệp): loại phần mềm theo dõi người dùng như màn hình, phím bấm, webcam, v.v...

Steganography: thuật ngữ mô tả quá trình che giấu thông tin khỏi những người quan sát nhưng không mã hóa nó.

T

Threat (mối đe dọa): những mối nguy hiểm tiềm tàng có thể xảy ra.

Threat modeling (mô hình hóa mối đe dọa): xác định các mối đe dọa có thể xảy ra đối với hệ thống, sau đó gán độ ưu tiên tương ứng với mức độ nghiêm trọng và xác suất xảy ra.

Trojan: loại phần mềm độc hại nhưng tự ngụy trang thành một dạng phần mềm vô hại khác.

V

VPN (Virtual Private Network): kỹ thuật cho phép mở rộng một mạng riêng hay mạng cục bộ đến những máy không được đặt trong mạng này.

Virus: loại phần mềm có khả năng gắn vào mã thực thi của một chương trình, tự sao chép chính chúng và thực hiện các công việc gây nguy hại.

Vulnerability scanner (quét lỗ hổng bảo mật): quá trình tìm các lỗ hổng bảo mật có thể có trong hệ thống.

W

Worms (sâu máy tính): loại phần mềm có thể sống độc lập và lây lan qua các kênh như mạng máy tính

Z

Zero-day (lỗ hổng Zero-day): lỗ hổng mà nhà phát triển chưa biết nhưng kẻ tấn công lại phát hiện ra.