Lỗ hổng (CVE): thực tế đã bị khai thác

Điểm yếu (CWE): có thể bị khai thác

Zero day vuln:

Lỗ hổng

Phân loại: là việc phân chia một tập hợp các tập hợp con theo một tiêu chí phân loại nhất định

Tiêu chí phân loại: là một đặc điểm của các phần tử được chọn để phân biệt các phần tử với nhau

Ví dụ tiêu chí: giới tính, điểm trung bình, đổ tuổi, cân nặng,…

Tiêu chí phân loại:

* Theo nguyên nhân xuất hiện
* Theo thời điểm xuất hiện
* Theo mức độ nguy hiểm

Định tính mức độ nguy hiểm

* Loại c: (thấp): cho phép tấn công từ chối dịch vụ
* Loại b (trung bình): cho phép người dùng cục bộ leo thang đặc quyền hoặc truy cập trái phép
* Loại a (cao): cho phép người dùng từ xa có thể truy cập trái phép vào hệ thống

Nguyên nhân phổ biến:

* Độ phức tạp
* Tính phổ biến
* Mức độ kết nối
* Quản lý mật khẩu kém
* Lỗi hệ điều hành
* Việc sử dụng Internet
* Lỗi phần mềm
* Con người

Định lượng mức độ nguy hiểm (CVSS)

Có 3 nhóm:

* Base Metric Group
  + Exploitability Metrics
    - Attack Vector
    - Attack Complexity
    - Privileges Required
    - User Interaction
  + Impact Metrics
    - Confidentiality Impact
    - Intergrity Impact
    - Availability Impact
* Temporal Metric Group
* Environmental Metric Group

Mỗi đại lượng đều có thể đo được

CWSS

Kiểm thử xâm nhập

* Quá trính kiểm tra và đánh giá hiệu quả của các giải pháp đảm bảo an toàn thông tin được sử dụng trong cty/tổ chức trước các mối đe doạ từ bên trong lẫn bên ngoài
* Người kiểm thử thực hiện các tấn công thực tế để vượt qua các tính năng an toàn của ứng dụng, hệ thống hoặc mạng

Lợi ích:

Xác định được các hiểm hoạ và xác suất tấn công lên tài sản

Xác định được các tấn công tiềm tàng và khả năng ảnh hưởng lên công ty/tổ chức trong trường hợp tấn công thành công

Biện pháp đối phó bổ sung để có thể giảm thiểu

So sánh khái niệm

Security audit

Vuln asessment

Pentesting

Kiểm thử hộp đen

Blind Testing

Double-Blind Testing x

Kiểm thử hộp trắng

Announced Testing

Unannounced Testing

Kiểm thử hộp xám

Footprinting techiques

Search Engines

Web services

Social network sites

Webites, email, DNS, Whois footprinting

Social Engineering

Competitive intelligence