Đánh giá & Kiểm định an toàn hệ thống thông tin

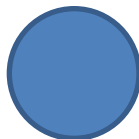
Module 1. Introduction to Pentesting and Methodologies

Thông tin giảng viên

TS. Lại Minh Tuấn

(Khoa ATTT – Học viện Kỹ thuật mật mã)

- Điện thoại: 0907-69-60-66
- Email: lmtuan.1989@gmail.com

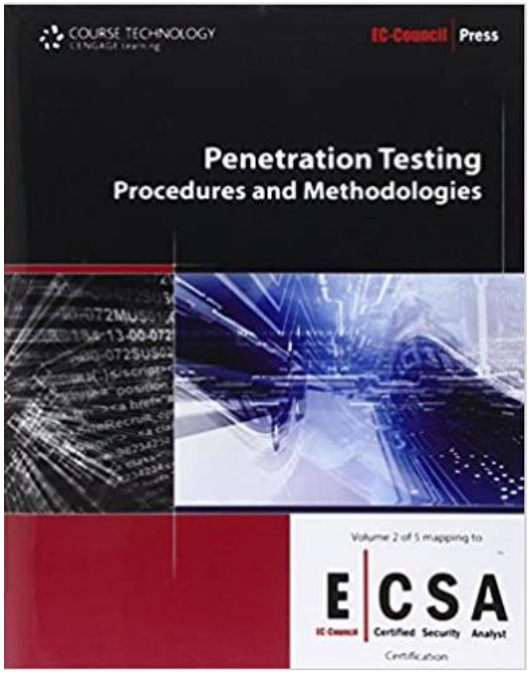


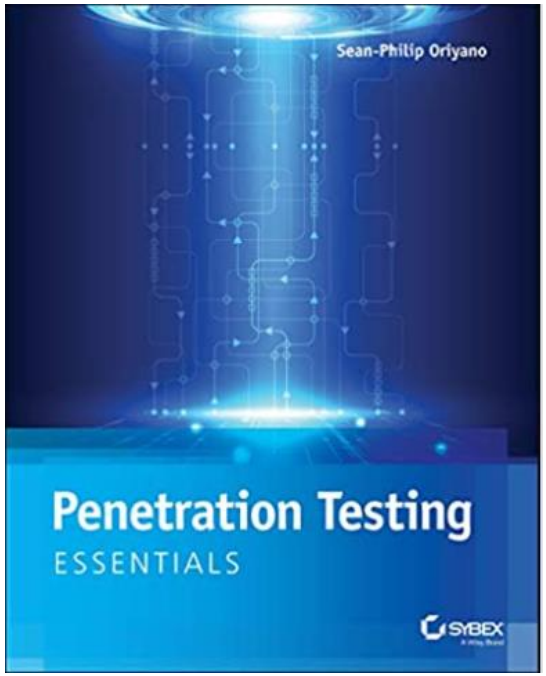
1. Giới thiệu học phần
2. Kiểm thử xâm nhập
3. Lỗ hổng bảo mật

1. Giới thiệu học phần
2. Lỗ hổng bảo mật
3. Kiểm thử xâm nhập

Giáo trình và Tài liệu tham khảo

1. Giáo trình "**Đánh giá & Kiểm định an toàn hệ thống thông tin**", Học viện KTMM, 2013.
2. EC-Council, **Penetration Testing: Procedures & Methodologies**
3. Wil Allsopp**, Advanced Penetration Testing: Hacking the World's Most Secure Networks**
4. Sean-Philip Oriyano, **Penetration Testing Essentials**





Nội dung học phần

1. Tổng quan về kiểm thử xâm nhập, quy trình thực hiện
2. Phương pháp tìm kiếm và thu thập thông tin
3. Phương pháp kiểm thử xâm nhập hệ thống mạng, ứng dụng Web, các thiết bị bảo vệ vành đai mạng…
4. Thực hiện phân tích, đánh giá lỗ hổng bảo mật
5. Tạo báo cáo về kiểm thử xâm nhập

Cấu trúc học phần

- **Thời lượng**: 3tc = 60 tiết
  - 30 tiết lý thuyết
  - 30 tiết thực hành
- **Đánh giá kết quả học tập**
  - Điểm chuyên cần
    - Đi học đầy đủ, đúng giờ
    - Tham gia xây dựng bài
  - Điểm thực hành + BTL
  - Điểm thi kết thúc học phần: Thi tự luận

Bài tập lớn

Danh sách và Yêu cầu

1. Giới thiệu học phần
2. Kiểm thử xâm nhập
3. Lỗ hổng bảo mật

Kiểm thử xâm nhập

- Kiểm thử xâm nhập (Penetration Testing)
  - Quá trình kiểm tra và đánh giá hiệu quả của các giải pháp đảm bảo an toàn thông tin được sử dụng trong công ty/tổ chức trước các mối đe dọa 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

Kiểm thử xâm nhập

- Lợi ích:
  - Xác định được các hiểm họa 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 các mối đe dọa đối với hệ thống.
  - Kiểm tra độ hiểu quả của các giải pháp/ thiết bị bảo mật đang triển khai (firewall, ids…).

So sánh khái niệm

- Security Audit
- Vulnerability Assessment
- Pentesting

Phân loại

- Kiểm thử hộp đen (Blackbox)
- Kiểm thử hộp trắng (Whitebox)
- Kiểm thử hộp xám (Graybox)

Kiểm thử hộp đen

- Người kiểm thử chỉ biết 1 số thông tin giới hạn về đối tượng (ip address, domain…)
- Sau khi kiểm thử có thể đưa ra càng nhiều thông tin về đối tượng càng tốt
- Việc kiểm thử mô tả lại quá trình tấn công trên thực tế và thu thập thông tin của đối tượng qua các kênh khác nhau
- Nhược điểm:
  - Không xác định được toàn bộ lỗ hổng trong hệ thống
  - Mang lại nhiều rủi ro cho hệ thống mạng
  - Các tấn công có thể bị hạn chế do tường lửa hoặc các hệ thống phòng thủ mạng

Kiểm thử hộp đen

- Kiểm thử hộp đen có thể phân thành 02 loại:

- **Blind Testing**
  - Tính thực tế cao do mô phỏng các phương pháp tấn công thực tế
  - Đội kiểm thử hoàn toàn không có thông tin (hoặc có thông tin giới hạn) về đối tượng
  - Tốn thời gian & công sức
- **Double-Blind Testing**
  - Chỉ có 1 vài người trong tổ chức biết về việc thực hiện kiểm thử
  - Hữu ích trong việc kiểm tra các biện pháp kiểm soát an toàn về mặt kĩ thuật, thực thi chính sách an toàn, khả năng phát hiện và ứng phó sự cố của nhân viên trong tổ chức

Kiểm thử hộp trắng

- Người kiểm thử biết tất cả thông tin về đối tượng (hạ tầng, topo mạng, thiết bị bảo mật, IP, chính sách bảo mật…)
- Hỗ trợ khả năng tìm bug và lỗ hổng một cách nhanh chóng
- Đảm bảo khả năng kiểm thử toàn diện đối tượng

Kiểm thử hộp trắng

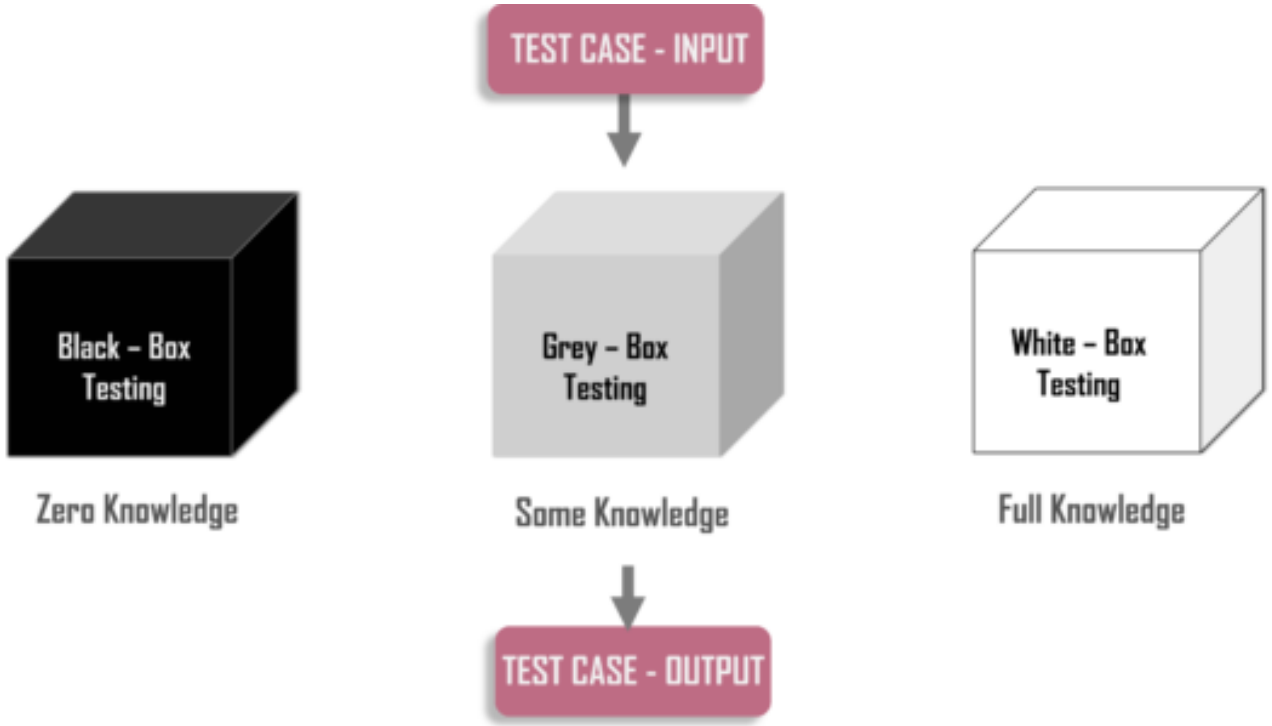
- Kiểm thử hộp trắng có thể phân thành 02 loại:

- **Kiểm thử công khai (Announced Testing)**
  - Thông báo cho mọi người trong tổ chức biết về việc thực hiện kiểm thử, đặc biệt là bộ phận IT
  - Kiểm tra hiện trạng của hệ thống bảo mật trước các lỗ hổng
- **Kiểm thử bí mật (Unannounced Testing)**
  - Không thông báo về việc kiểm thử, chỉ có người quản lý cao nhất biết
  - Kiểm tra hiện trạng của hệ thống bảo mật trước các lỗ hổng và khả năng phản ứng, đối phó sự cố của bộ phận IT

Kiểm thử hộp xám

- Người kiểm thử biết giới hạn thông tin về đối tượng
- Thường mô phỏng lại quá trình tấn công từ các mối đe dọa nội bộ
- Việc thực hiện thường diễn ra khi đội kiểm thử đã thực hiện kiểm thử hộp đen và thu được 1 số thông tin nhất định

So sánh



Dạng kiểm thử	Giá thành	Mức độ toàn diện
Hộp đen	$$	x
Hộp trắng	$$$	xxx
Hộp xám	$	xx

Lựa chọn dạng kiểm thử

- Việc lựa chọn dạng kiểm thử phụ thuộc vào **yêu cầu**, **mục đích**, **thời gian** và **tài nguyên** của tổ chức.
- Kiểm thử hộp đen mô tả lại các cuộc tấn công trên thực tế tuy nhiên kiểm thử hộp xám và trắng có ưu điểm về mặt thời gian, tài nguyên
- Ngoài ra có thể phân loại thành:
  - Kiểm thử tự động (Automated Pentesting)
  - Kiểm thử thủ công (Manual Pentesting)
- Theo MITRE, các công cụ kiểm thử tự động chỉ bao gồm 45% lỗ hổng đã biết, 55% còn lại yêu cầu kiểm thử thủ công.
- Kiểm thử thủ công hạn chế được các kết quả dương tính giả

Đối tượng kiểm thử

1. Network Pentesting

- Xác định các vấn đề an toàn trong thiết kế và thực thi của mạng máy tính
- Một số vấn đề về an toàn thường gặp:
  - Sử dụng giao thức không an toàn
  - Mở cổng hoặc dịch vụ không cần thiết
  - Không cập nhật phần mềm và OS
  - Lỗi cấu hình trên FW, IDS, Server…

Đối tượng kiểm thử

2. Web Application Pentesting

- Xác định các vấn đề an toàn trong thiết kế ứng dụng web và thực tiễn phát triển
- Một số vấn đề về an toàn thường gặp:
  - Lỗ hổng "injection"
  - Lỗ hổng xác thực & phân quyền
  - Quản lý phiên
  - Xử lý lỗi trả về
  - Sử dụng mật mã yếu

Đối tượng kiểm thử

3. SE Pentesting

- Xác định các vấn đề nhận thức về an toàn thông tin đối với con người trong tổ chức
- Một số vấn đề về an toàn thường gặp:
  - Click vào các link, emails độc hại
  - Bị lừa đảo qua emails, điện thoại
  - Để lộ thông tin cho người lạ, rò rỉ các thông tin bí mật
  - Không tuân thủ các chính sách của tổ chức

Đối tượng kiểm thử

4. Wireless Network Pentesting

- Xác định các vấn đề an toàn trong cấu hình mạng không dây
- Một số vấn đề về an toàn thường gặp:
  - Sự tồn tải của các AP giả mạo, AP mở
  - Sử dụng các chuẩn mã hóa yếu
  - Không hỗ trợ các công nghệ mạng không dây

Đối tượng kiểm thử

5. Mobile Device Pentesting

- Xác định các vấn đề an toàn liên quan tới thiết bị di động và việc sử dụng chúng
- Một số vấn đề về an toàn thường gặp:
  - Không thực hiện hoặc thực hiện không đúng chính sách BYOD
  - Sử dụng các thiết bị không rõ nguồn gốc
  - Sử dụng các thiết bị đã bị bẻ khóa
  - Triển khai các cơ chế bảo mật yếu trên thiết bị
  - Kết nối vào các mạng không an toàn

Đối tượng kiểm thử

6. Cloud Pentesting

- Xác định các vấn đề an toàn trên Cloud
- Một số vấn đề về an toàn thường gặp:
  - Không bảo vệ dữ liệu đúng cách
  - Quản lý quyền truy cập
  - Insecure interfaces & APIs
  - Hiểm họa từ bên thứ 3

Quá trình kiểm thử

❑ Xác định phạm vi

- Ai thực hiện
- Phạm vi, thời gian thực hiện
- Thực hiện các công việc chuẩn bị

❑ Thực hiện kiểm thử

- Thu thập các thông tin quan trọng từ đó giúp tìm ra & khai thác các lỗ hổng bảo mật
- Xác nhận lỗ hổng tiềm tàng

❑ Báo cáo kết quả

- Liệt kê & phân loại các lỗ hổng tìm được
- Đưa ra các khuyến nghị
- Hoàn thiện báo cáo

Phương pháp luận kiểm thử

- Ý nghĩa của phương pháp luận:
  - Cung cấp tính thống nhất và có cấu trúc cho việc đánh giá an toàn, từ đó có thể giảm thiểu rủi ro trong quá trình kiểm thử.
  - Giúp dễ dàng trong việc chuyển giao quy trình kiểm thử nếu có sự thay đổi nhân sự đánh giá.
  - Chỉ ra những hạn chế về tài nguyên kết hợp với các đánh giá an toàn.

Pentesting Methodology

- Phương pháp luận bản quyền
  - EC-Council's LPT
  - IBM
  - ISS
  - McAfee Foundstone

Pentesting Methodology

Phương pháp luận mở

- OWASP
  - Web Security Testing Guide (WSTG)
  - Mobile Security Testing Guide (MSTG)
  - Firmware Security Testing Methodology
- Penetration Testing Execution Standard
- PCI Penetration Testing Guide
  - PCI DSS Penetration Testing Guidance
  - PCI DSS Penetration Testing Requirements
- Penetration Testing Framework (PTF)
- Technical Guide to Information Security Testing and Assessment (NIST 800-115)
- Open Source Security Testing Methodology Manual (OSSTMM)

Sinh viên tham khảo thêm trong giáo trình và internet!!!

OWASP Web Application Security Testing

- 4.0 Introduction and Objectives
- 4.1 Information Gathering
- 4.2 Configuration and Deployment Management Testing
- 4.3 Identity Management Testing
- 4.4 Authentication Testing
- 4.5 Authorization Testing
- 4.6 Session Management Testing
- 4.7 Input Validation Testing
- 4.8 Testing for Error Handling
- 4.9 Testing for Weak Cryptography
- 4.10 Business Logic Testing
- 4.11 Client-side Testing
- 4.12 API Testing

Example – LPT Pentesting Methodology

- *Step 1. Information Gathering*
- *Step 2. Scanning & Reconnaissance*
- *Step 3. Fingerprinting & Enumeration*
- *Step 4. Vulnerability Assessment*
- *Step 5. Exploit Reasech & Verification*
- *Step 6. Reporting*

1 Giới thiệu học phần

2 Kiểm thử xâm nhập

3 Lỗ hổng bảo mật

Định nghĩa

- **Lỗ hổng bảo mật** (vulnerability) được hiểu là những **khiếm khuyết trong chức năng, thành phần** của một phần mềm, phần cứng hay một HTTT mà có thể bị lợi dụng để gây hại cho hệ thống.
- **Ví dụ**:
  - Không có cơ chế ngăn chặn duyệt mật khẩu
  - Không kiểm soát dữ liệu đầu vào
  - Lỗi tràn bộ đệm

Điểm yếu ≠ Lỗ hổng

❑Lỗ hổng (Vulnerability)

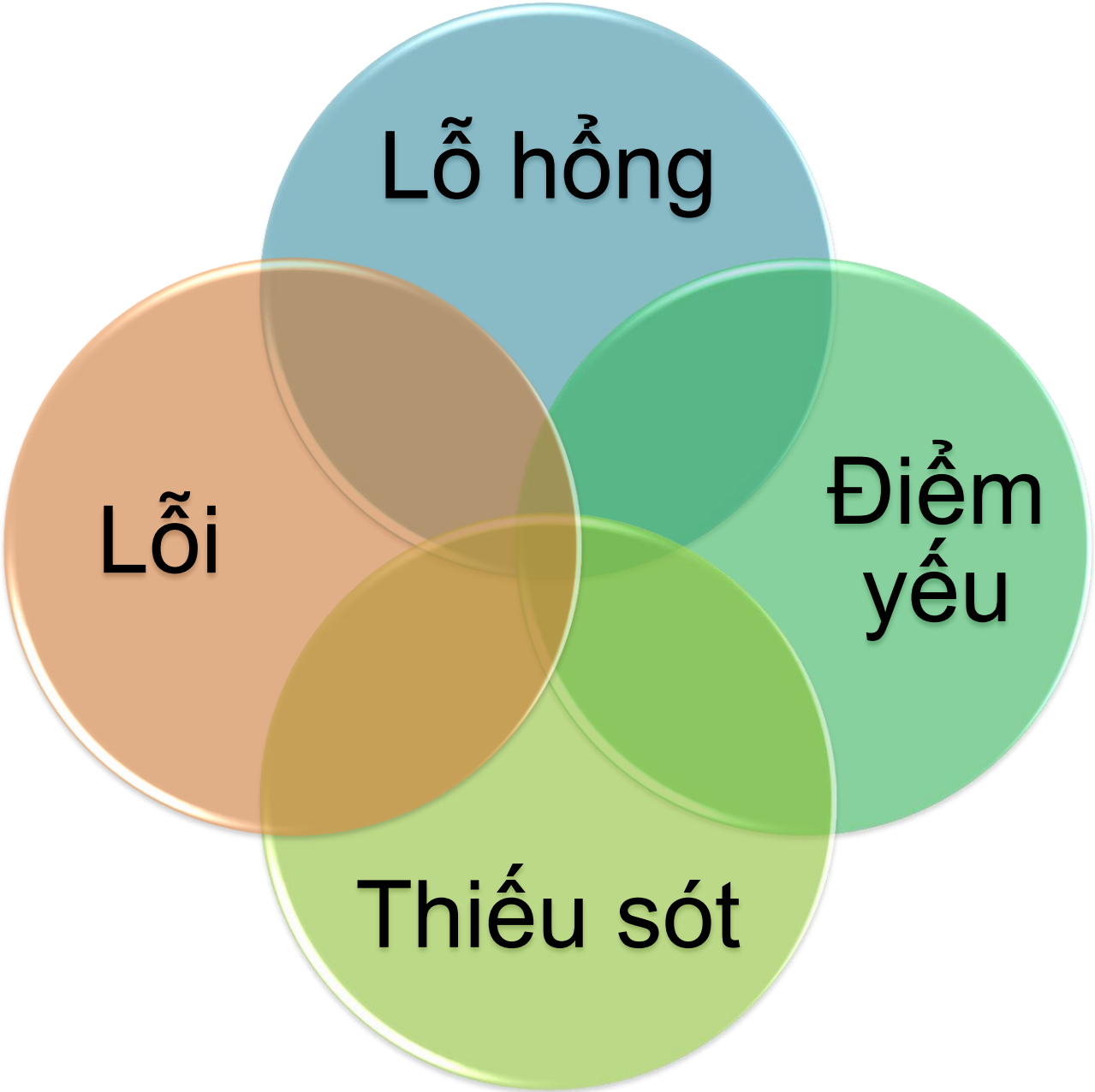
- thực tế đã bị khai thác
- https://cve.mitre.org/
- CVE = Common Vulnerabilities and Exposures

❑Điểm yếu (Weakness)

- Có thể bị khai thác
- https://cwe.mitre.org/
- CWE = Common Weakness Enumeration

Zero-day vulnerability?

Thuật ngữ "lỗ hổng"



Phân loại

- **Phân loại**: là việc phân chia một tập hợp thành 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 phân loại**: Giới tính, Điểm trung bình, Độ tuổi, Cân nặng,...

Phân loại lỗ hổng bảo mật

❑Tiêu chí phân loại

- Theo nguyên nhân xuất hiện
- Theo thời điểm xuất hiện
- Theo mức độ nguy hiểm
  - Định tính
  - Định lượng

Định tính mức độ nguy hiểm

- **Lỗ hổng loại C** (Mức thấp): cho phép tấn công từ chối dịch vụ (DoS)
- **Lỗ hổng loại B** (Mức trung bình): cho phép người dùng cục bộ leo thang đặc quyền hoặc truy cập trái phép.
- **Lỗ hổng loại A** (Mức cao): cho phép người dùng từ xa có thể truy nhập 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

- Common Vulnerability Scoring System, https://www.first.org/cvss/
- Có 3 nhóm đại lượng đặc trưng cho mỗi lỗ hổng
  - Base Metric Group
  - Temporal Metric Group
  - Environmental Metric Group

Base Metric Group

Exploitability Metrics

- Attack Vector
- Attack Complexity
- Privileges Required
- User Interaction

Impact Metrics

- Confidentiality Impact
- Integrity Impact
- Availability Impact

- Scope

Temporal Metric Group

Exploit Code Maturity

Remediation Level

Report Confidence

Environmental Metric Group

Modified Base Metrics

Confidentiality Requirement

Integrity Requirement

Availability Requirement

Định lượng mức độ nguy hiểm

- Mỗi đại lượng đều có thể đo được và nhận một giá trị nhất định
- Có công thức để tính điểm chung cho lỗ hổng từ giá trị của các đại lượng, https://www.first.org/cvss/calculator/3.0
- Thang điểm: 0.0 đến 10.0; điểm càng cao càng nguy hiểm

Định lượng mức độ nguy hiểm

Rating	CVSS Score
None	0.0
Low	0.1 - 3.9
Medium	4.0 - 6.9
High	7.0 - 8.9
Critical	9.0 - 10.0

Demo

Định lượng mức độ nguy hiểm

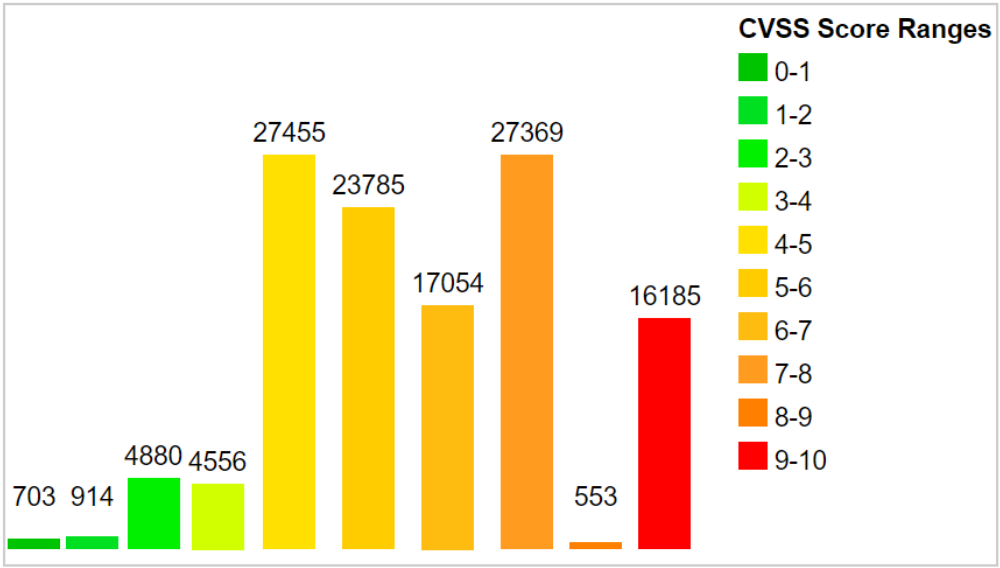
Current CVSS Score Distribution For All Vulnerabilities

Distribution of all vulnerabilities by CVSS Scores

CVSS Score	Number Of Vulnerabilities	Percentage
0-1	703	0.60
1-2	914	0.70
2-3	4880	4.00
3-4	4556	3.70
4-5	27455	22.20
5-6	23785	19.30
6-7	17054	13.80
7-8	27369	22.20
8-9	553	0.40
9-10	16185	13.10
Total	123454	

Weighted Average CVSS Score: **6.6**

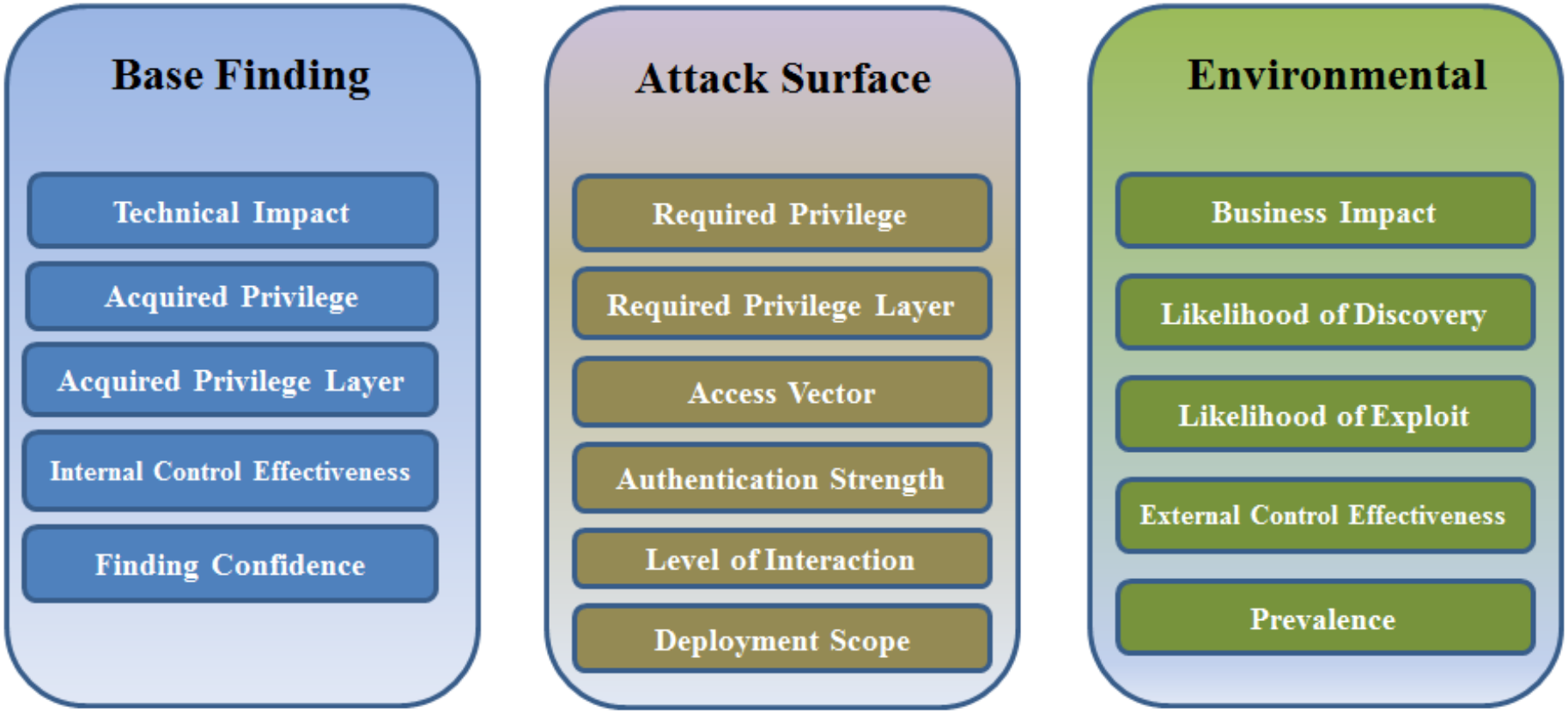
Vulnerability Distribution By CVSS Scores



Common Weakness Scoring System

- CWSS Metric Groups

  https://cwe.mitre.org/cwss/cwss_v1.0.1.html



Top 10 OWASP 2020

- Injection
- Broken Authentication
- Sensitive Data Exposure
- XML External Entities (XXE)
- Broken Access control
- Security misconfigurations
- Cross Site Scripting (XSS)
- Insecure Deserialization
- Using Components with known vulnerabilities
- Insufficient logging and monitoring

Thank you & Any questions?