0913.0966.77

[quangth@mta.education](mailto:quangth@mta.education)

**Đánh giá an ninh mạng**

LAN >< WAN

-3 kỹ thuật biến đổi sang bit 0 1

fm

am

pm

-Model network OSI vs

IPX/SPX

SNA

Apple Talk

**Bài 1: Tổng quan đánh giá an ninh mạng**

1. Khái niệm

-Đánh giá an ninh mạng: Là quá trình nhằm xác định được trạng thái rủi ro của hệ thống

2. Phương pháp đánh giá

3. Phương pháp luận

4. Kế hoạch hành động

5. Kỹ thuật thực hiện

a. Outsiders-Black box

b. Associates- Gray box

c. Insiders- White box

**3.Nghiên cứu**

# NIST-SP800

# NSA

* IAM
* IEM

# Pete Herzog

* Open source security testing methodology manual

\*Tiêu chuẩn có 3 loại:

-Định tính – ISO 17799, ISO 27000

-Định lượng -> Công cụ || +Tìm kiếm các rủi ro của an ninh (đặc biệt lỗ hổng)

+Dựa trên chất lượng dịch vụ (hiệu năng)

-Tổng hợp

# NIST SP800-30

->Đánh giá rủ ro

-Tiến hành theo từng bước

B1: System Characterization (khảo sát hệ thống) thu thập được nhiều thông tin nhất về hệ thống: phần cứng, dữ liệu, con người, dịch vụ, …

B2: Threat Identification (mối đe dọa): Chỉ ra đối tượng gây ra mối đe dọa

B3: Vuluerability Identification (Chỉ ra các lỗ hổng): Xem lại tất cả các hệ thống an ninh, rà soát kiểm tra lỗ hổng của từng đối tượng một -> lấy kết quả đánh giá xem đã phù hợp chưa

B4: Control Analysis (Phân tích điều khiển): xem xét lại các quy trình vào/ra, đường đi dữ liệu, các đối tượng sử dụng

B5: Likelihood Determination (Xác định những kịch bản có khả năng xảy ra)

B6: Impact analysis (Phân tích tác động): Thử xem các kịch bản có thể xảy ra hay không -> tính ra tỉ lệ tác động

B7: Risk Determination (Chỉ ra các rủi ro): chỉ ra các rủi ro có thể xảy ra là bao nhiêu %

B8: Control Recommendation (Đề xuất kiểm soát): Đề xuất ra 1 loạt các vấn đề để giảm thiểu rủi ro

B9: Results Documentation (Xây dựng giải pháp)

# NIST SP800-42

B1: Security Testing and the System Development Life Cycle

-Đánh giá mô hình phát triển, chu trình hệ thống mạng

B2: Security Testing Techniques

-Chuẩn bị các kỹ thuật để đánh giá

+Kiểm tra quyền

+Quét toàn bộ lỗ hổng mạng

+Phá mật khẩu

+Rà soát Log

+Kiểm tra tính toàn vẹn

+Phát hiện mã độc, virus

+…

B3:

# NSA

# IEM

#OSSTMM

1. Process security Testing

-Thu thập các hiện trạng

-Lấy các yêu cầu

-Các phản hồi

-Đưa ra 1 số các giải pháp

-Đánh giá các khu vực an toàn

3. Internet Technology Security Testing (19 nội dung đánh giá)

4. Communications Security Testing (các hệ thống tổng đài)

-PBX review

-Voicemail

-FAX

-…

5. Wireless security Testing (đánh giá các hệ thống không dây)

-Đánh giá về điện từ trường, hồng ngoại

-Bluetooth

-Bàn phím, chuột, loa

-Các thiết bị cầm tay không dây

-Các thiết bị bộ đàm

6. Physical security Testing (đánh giá về các hệ thống vật lý)

-Phòng cháy nổ, khóa, …

**4. Kỹ thuật đánh giá**

**-**Flaw-hypothesis (hypothesis testing)-> tìm lỗ hổng bằng cách giả định các trường hợp

**-**Penetration Testing (pentest) -> tấn công thử

-Attack Trees testing (attack tree) -> tổ hợp các lỗ hổng để ra lỗ hổng lớn hơn (7+8 -> 9)

\*6 nội dung

-Topology

-Technical Testing (chọn công cụ, kỹ thuật phù hợp)

-Network Devices: Toàn bộ các trang thiết bị mạng

-Servers: Hệ thống server

-Application: Toàn bộ ứng dụng

-Các chính sách, quy trình

**5. Tiêu chuẩn**

**BTVN:Tìm hiểu**

1. Các tiêu chuẩn đánh giá

2. Các kỹ thuật đánh giá

3. Các bộ công cụ để đưa ra đánh giá

4. Các kịch bản đánh giá

**Bảo vệ hệ thống (protecting systems)**

1. Hệ điều hành

\*Update

-Security Patch: vá lỗi

-Hotfix: được sử dụng để khắc phục cho 1 chức năng nào đó theo nhu cầu của người sử dụng

-Service pack:

\*BufferOverflow

- 2 cách (DEP: ngăn chặn thực thi dữ liệu, ASLR: ngẫu nhiên hóa chức năng bộ nhớ)

\*Configure (4 bước)

-Security policy

-Configuration baseline

-Security template

-Deployment: nên được triển khai theo Group Policy

**Bộ tiêu chuẩn gồm các phần gì?**

**Các phần nào áp dụng vào thực tế?**

Template for iso

Bài tập 2: Đánh giá định lượng

Thực thi cho 1 đánh giá theo 1 công cụ hoặc 1 bộ tiêu chuẩn (OWASP/NMAP/Fowd Stone)

* Kết luận đánh giá

**Đánh giá Mạng Không Dây (IEEE 802.11)**

Vesion: a/b/g/n

b - 11 Mbps

a/g/n – 54Mbps

n > 54 Mbps

WEP/WPA -> Personal/Interprise

Local: Token Ring

Internet: CSMA,CSMA/CD

Wireless: CSMA/CA

\*WEP

\*WPA/WPA2

**Enterprise Wireless Security (**IEEE 802.1x/802.11i)

**Nội dung thi đánh giá an ninh mạng:**

-Đánh giá là gì?

-2 cách đánh giá: định tính và định lượng

-Tìm được bộ qui chuẩn đánh giá

1. Định tính -> Mỗi người 1 bài -> Sửa lại -> In ra quyển

2. Định lượng -> Thực hành -> Video để mô tả -> Hiểu biết về vấn đề đó

-Kỹ thuật pentest

-Đánh giá mảng pentest owasp

(4-5 cái)

-owasp 4.0 release : https://www.owasp.org/images/1/19/OTGv4.pdf

+Tiêu chuẩn, mục cụ thể

+Tools

+Minh chứng

* Việc đánh giá có giá trị -> tăng cường an ninh