Topic Planning Pentest service

# Overview

Mục tiêu: Thảo luận và xây dựng kế hoạch thực hiện dịch vụ pentest.

Nội dung chính:

1. Giới thiệu khái quát về Pentest và dịch vụ Pentest.

2. Thông tin về thị trường Pentest của thế giới và VN.

3. Lựa chọn triển khai loại hình Pentest (theo phân loại và nhu cầu từ phía dự án).

4. Quy trình thực hiện dịch vụ Pentest chung.

5. Những vấn đề trước mắt và việc cần làm tiếp theo để khởi động dịch vụ Pentest.

# Content

## 1. Giới thiệu dịch vụ Pentest

Pentesting (kiểm thử xâm nhập) giúp đánh giá khả năng 1 hệ thống có thể được bảo vệ như thế nào như network, app, system từ các cuộc tấn công trong và ngoài hệ thống. Giúp đảm bảo tính Bảo mật (Confidentiality), toàn ven (Integrity) và sẵn sáng (Availability) cho các dịch vụ đang được vận hành ở tổ chức.

**Lợi ích** của việc triển khai pentest cho hệ thống CNTT:

- Tìm ra lỗ hổng: Để tìm ra lỗ hổng, điểm yếu của phần mềm, hệ thống thì pentester có vai trò thực hiện tấn công vào hệ thống như Hacker hay user xấu để biết được họ tấn công từ đâu, như thế nào vào hệ thống và sau đó báo cáo cho tổ chức đồng thời đưa ra các giải pháp khắc phục.

- Cho thấy nguy cơ gây mất ATTT thực tế: Việc kiểm thử còn cho thấy nguy cơ gây hại đến hệ thống và pentester có thể phát hiện và khuyến nghị tổ chức, góp phần hạn chế rủi ro mất ATTT.

- Hạn chế các khả năng bị tấn công thực: Việc pentest đóng vai trò quan trọng vì việc này giúp nhìn ra cách thức tấn công của Hacker trong lẩn ngoài doanh nghiệp từ đó mà tổ chức có thể đưa ra những phương án để phòng thủ.

- Bảo vệ danh tiếng của Công ty.

**Pentesting service delivery model**:

In-house pentesting: Tổ chức có team pentest trong họ.

Pentesting-as-a-service: Pentest sử dụng dịch vụ cloud cho phép dịch vụ liên tục.

Outsource pentesting service: Tổ chức thuê một bên khác để thực hiện kiểm thử

Crowded pentesting service: Tổ chức nhờ một bên thứ ba có thể tổ chức pentest dạng cộng đồng như chương trình bug bounty.

**Type of Pentesting Assessment**

Goal-oriented/Object-oriented pentesting approach: Là loại pentest dựa trên tiêu chí là đạt được mục tiêu, kiểm thử một đối tượng nào đó. VD: chiếm quyền điều khiển một server, tạo DOS vào server,..,..

Compliance Pentesting approach: pentest dựa trên các điều khoản bảo mật cần tuân thủ của một hệ thống, tổ chức xem tổ chức đó có đạt chuẩn hay không hay trong các điều khoản có lỗ hổng để hacker vượt rào.

Redteaming-oriented pentesting approach: pentest được thực hiện mô phỏng sự tấn công thật của hacker đối với hệ thống.

**Strategies of Pentesting:**

Black box: Pentester thực hiện tấn công với thông tin giới hạn về hệ thống, gần như không có, vị trí gần như 1 hacker tấn công từ bên ngoài.

Gray box: Pentester biết một phần thông tin về hệ thống, có thể có account và quyền nhất định.

White box: Pentester có gần như mọi thông tin và quyền truy cập của hệ thống. Vị trí gần như là 1 employee của tổ chức.

**Cost and Comprehensiveness:**

|  |  |  |
| --- | --- | --- |
| **Type of Pentesting** | **Cost** | **Comprehensive** |
| Black box | $$ | X |
| Gray box | $ | XX |
| White box | $$$ | XXX |

**Type of Methods to test**

Automated pentesting: Sử dụng tool để auto test và scan để thẩm định kết quả.

Manula pentesting: test được thực hiện thông qua chủ yếu là sức người của đội ngũ pentest.

**Common Areas of Pentesting**

Network pentesting

Web application pentesting

Social engineering pentesting

Wireless Network pentesting

Mobile device pentesting

Cloud pentesting.

**Phases of pentesting service**

Graphical user interface, application, Teams

Description automatically generated

Pre-Attack Phase -> Attack Phase ->Post-Attack Phase

## 2. Thị trường Pentest chung

Nguyên nhân khiến thị trường Pentest tăng

- Sự phát triển web app, mobile app đang gia tăng mạnh

- Quy trình chuyển đổi số dần phổ biến, lan rộng.

- Pentest là hình thức chủ động phòng ngừa hiệu quả.

## 3. Lựa chọn triển khai loại hình Pentest

Type of Pentesting Assessment: Redteaming-oriented pentesting approach

Strategies of Pentesting: Full option

Type of Methods to test: Full option

Areas of Pentesting: Web app

## 4. Quy trình thực hiện dịch vụ Pentest

Diagram

Description automatically generated

Shape, arrow, polygon

Description automatically generated

Table

Description automatically generated

## 5. Khởi động dịch vụ Pentest như thế nào

\* Khó khăn trước mắt:

…

\* Cần thiết:

- Cần quy trình chuẩn và phù hợp vào tình hình thực tế.

- Cần xác định nguồn lực để từ đó thiết lập kế hoạch phù hợp và mở rộng nguồn lực trong tương lai.

# Reference

CPENT modules

<https://www.alliedmarketresearch.com/penetration-testing-market-A07473>

https://cystack.net/vi/blog/pentest-la-gi-nhung-dieu-can-biet-ve-kiem-thu-xam-nhap