Bài: 1.9 Giới thiệu về Ethical Hacking - Thử nghiệm độ an toàn

Xem bài học trên website để ủng hộ Kteam: 1.9 Giới thiệu về Ethical Hacking - Thử nghiệm độ an toàn

Mọi vấn đề về lỗi website làm ảnh hưởng đến bạn hoặc thắc mắc, mong muốn khóa học mới, nhằm hỗ trợ cải thiện Website. Các bạn vui lòng phản hồi đến Fanpage How Kteam nhé!

Thử nghiệm độ an toàn

Tổng quan

Trong môi trường **ethical hacking**, khái niệm được sử dụng phổ biến nhất là "**pentester**". **Pentester** là các nhà thử nghiệm độ an toàn (penetration tester) được chủ sở hữu cho phép để hack thiết bị.

Quá trình thử nghiệm an toàn đánh giá mức độ bảo mật, **giá trị "hack"** (hack value), cái đích của việc đánh giá (TOE), các cuộc tấn công, khai thác, điểm yếu zero-day và những thành phần khác như các mối đe dọa, các yếu điểm, chuỗi daisy.

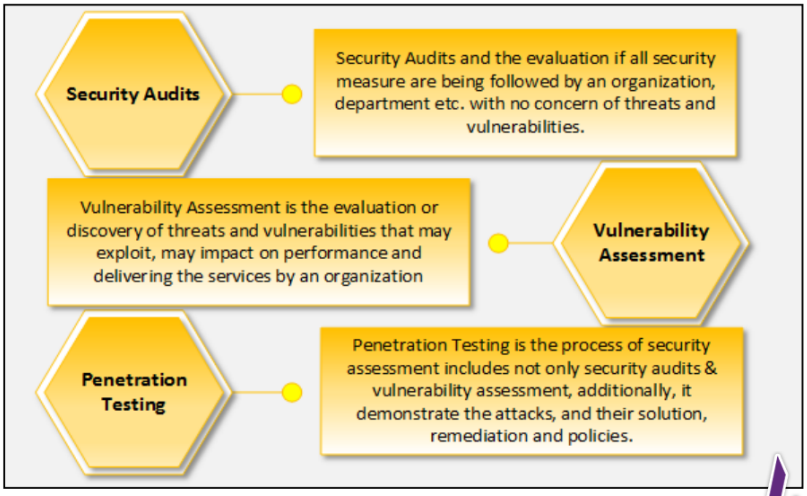


Figure 1-13 Comparing Pentesting

Impotant for Penetration testing (Tầm quan trọng của thử nghiệm độ an toàn)

Nếu bạn muốn chuẩn bị sẵn sàng trước một cuộc tấn công, bạn phải đủ thông minh, để nghĩ và hành động như hắn. Hacker có kỹ năng rất cao, có thông tin chi tiết về phần cứng, phần mềm, mạng và những thông tin có liên quan khác.

Sự cần thiết và quan trọng của việc **thử nghiệm an toàn** trong thế giới đương đại – nơi vô vàn các mối đe dọa như **tấn công từ chối dịch vụ** (denial of service), danh tặc (identity theft), đánh cắp dịch vụ, đánh cắp thông tin tồn tại quá phổ biến, hệ thống thử nghiệm an toàn đảm bảo cho việc chống lại các mối nguy hiểm độc hại bằng cách ước đoán phương thức.

Vài lợi ích và điều cần thiết cho thử nghiệm độ an toàn là tiết lộ điểm yếu của hệ thống và triển khai bảo vệ bằng cách thức giống với cách kẻ tấn công cố gắng có được quyền truy cập.

- Xác định mối nguy hiểm vị trí dễ tổn thương đến tài sản của tổ chức
- Cung cấp điều lệ, quy trình, thiết kế và kiến trúc dự kiến một cách toàn diện.
- Chuẩn bị cách sửa chữa nhằm bảo vệ chúng trước khi bị hacker lợi dụng để phá vỡ hệ thống bảo mật.
- Nhận định những gì kẻ tấn công có thể truy cập để đánh cắp
- Nhận định những thông tin có thể bị đánh cắp và công dụng của thông tin đó
- Kiểm tra và làm cho việc bảo mật có hiệu lực, nhận định sự cần thiết cho mỗi bước bảo vệ bổ sung.

- Điều chỉnh và nâng cấp việc triển khai kiến trúc bảo mật hiện tại.
- Làm giảm chi phí bảo mật IT bằng cách làm tăng vốn đầu tư vào bảo mật (Return on Security Investment – ROSI)

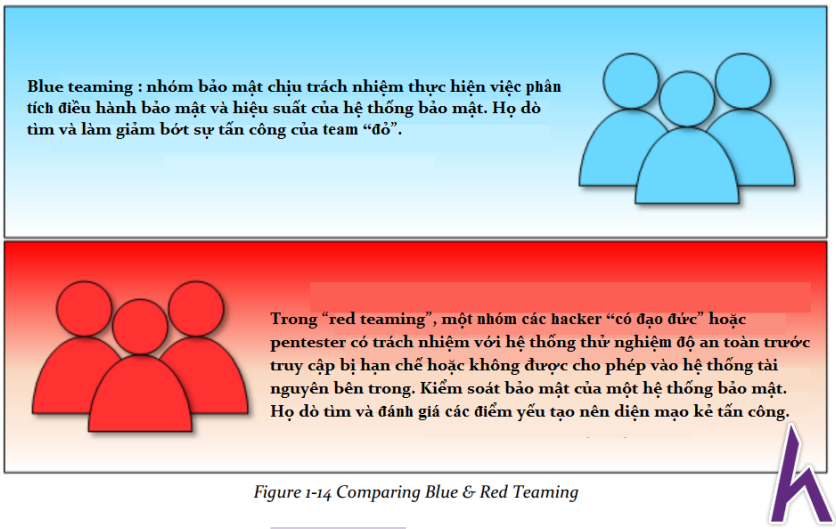


Figure 1-14 Comparing Blue & Red Teaming

Các kiểu đánh giá bảo mật

Ba kiểu đánh giá bảo mật đều rất quan trọng, vì pentester có thể yêu cầu thực hiện bất cứ kiểu nào trong số ba kiểu đó:

Hộp đen

Black box là một kiểu đánh giá bảo mật mà pentester thử nghiệm "mù" hoặc thử nghiệm "mù" kép, có nghĩa trong trường hợp không có bất kỳ kiến thức nào về hệ thống hoặc thông tin của mục tiêu.

Black box được thiết kế để **biểu diễn mô phỏng kẻ tấn công** trong tình huống cuộc tấn công gặp phải sự chống trả.

Hộp xám

Gray box là kiểu thử nghiệm trong đó các pentester có rất ít hiểu biết về hệ thống hoặc các thông tin gì về mục tiêu như địa chỉ IP, hệ điều hành hoặc thông tin mạng sẽ bị hạn chế.

Gray box được thiết kế nhằm **biểu diễn mô phỏng tình huống trong nội bộ** có được những thông tin này và chống lại cuộc tấn công khi các pentester có thông tin cơ bản, tuy giới hạn về mục tiêu được nhắm tới.

Hộp trắng

White box là kiểu thử nghiệm trong đó pentester có hoàn toàn nắm bắt được những thông tin và hiểu biết về hệ thống. Kiểu thử nghiệm này được thực hiện bởi đội ngũ bảo mật hoặc đội kiểm tra thông tin để thực hiện việc kiểm tra.

Các giai đoạn của thử nghiệm độ an toàn

Quá trình thử nghiệm độ an toàn gồm ba giai đoạn

1. Giai đoạn trước cuộc tấn công
2. Giai đoạn cuộc tấn công diễn ra
3. Giai đoạn sau cuộc tấn công

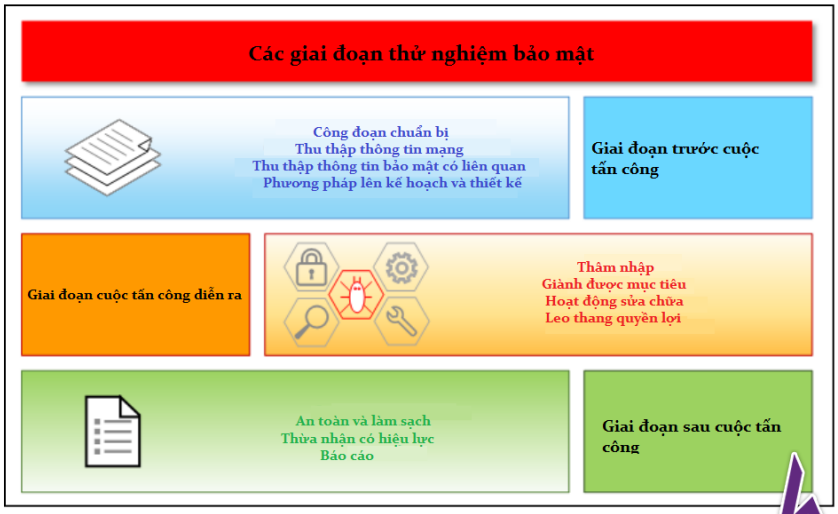


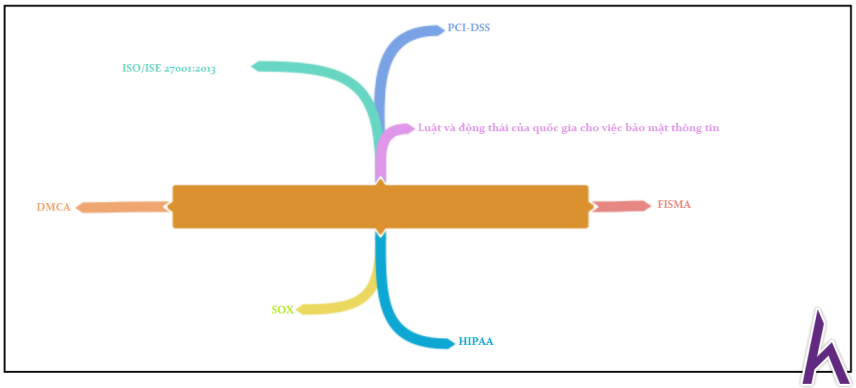
Figure 1-15 Penetration Testing Phases

Phương pháp thử nghiệm bảo mật

Có vài hệ phương pháp có thể áp dụng cho **thử nghiệm bảo mật** hoặc **độ an toàn**. Những tổ chức với các phương pháp thử nghiệm dẫn đầu đó là:

- Open Web Application Security Project (OWASP)
- Open Source Security Testing Methodology Manual (OSSTMM)
- Information Systems Security Assessment Framework (ISAF)
- EC-Council Licensed Penetration Tester (LPT) Methodology

MinMap



Luật & tiêu chuẩn bảo mật an ninh dữ liệu thẻ thanh toán

Payment Card Industry Data Security Standard (PCI-DSS)

PCI-DSS là một tiêu chuẩn bảo mật thông tin toàn cầu được đưa ra bởi "**PCI Security Standards Council**", khả dụng cho các tổ chức phát triển, tăng cườngvà đánh giá tiêu chuẩn bảo mật trong việc giữ thông tin của chủ thẻ và tiêu chuẩn cho việc bảo mật tài khoản giao dịch.

PCI Security Standards Council phát triển tiêu chuẩn bảo mật cho ngành công nghiệp thẻ tín dụng, cung cấp công cụ cần thiết cho sự vận hành của những tiêu chuẩn đó như huấn luyện (training), chứng nhận (certification), định mức (assessment) và quét (scanning).

Những thành viên sáng lập nên hội đồng này là:

- American Express, Discover Financial Service
- JCB International
- MasterCard
- Visa Inc

Tiêu chuẩn bảo mật dữ liệu PCI giải quyết an toàn dữ liệu chủ thẻ cho việc ghi nợ, tín dụng, trả trước, ví điện tử, thẻ ATM và POS. Một cái nhìn tổng quan của PCI-DSS cung cấp

- An ninh mạng
- Sự điều hành truy cập mạnh mẽ
- Bảo mật dữ liệu chủ thẻ
- Thường xuyên điều chỉnh và đánh giá mạng
- Chương trình sửa chữa tổn thương
- Luật bảo vệ thông tin

ISO/IEC 27001:2013

Tổ chức quốc tế về tiêu chuẩn hóa (ISO) và **ủy ban Kỹ thuật điện tử quốc tế** (IEC) là những tổ chức được phát triển trên toàn cầu và duy trì những tiêu chuẩn đã đặt ra. Tiêu chuẩn **ISO/IEC$_{27001:2013}$** đảm bảo những yêu cầu cho việc thi hành, duy trì cùng với sự phát triển của một hệ thống quản lý bảo mật thông tin. Tiêu chuẩn này là bản chỉnh sửa (bản thứ hai) từ bản **ISO/IEC$_{27001:2005}$** .

ISO/IEC$_{27001:2013}$ bao gồm những điểm chính sau đây trong an toàn thông tin:

- Thi hành và duy trì yêu cầu bảo mật
- Quy trình quản lý an toàn thông tin
- Cam kết quản lí rủi ro hiệu quả
- Trạng thái của hoạt động quản lý an toàn thông tin
- Tuân theo luật

Đạo luật về Trách nhiệm giải trình & Cung cấp thông tin bảo hiểm y tế (HIPAA)

Đạo Luật về Trách Nhiệm Giải Trình và Cung Cấp Thông Tin Bảo Hiểm Y Tế được thông qua vào năm 1996 bởi Quốc hội. **HIPAA** vận hành với bộ ý tế và nhân sinh (HHS) nhằm phát triển và duy trì nguyên tắc giữ bí mật thông tin sức khỏe .

Luật an toàn của HIPAA đảm bảo những thông tin nào cần được bảo mật, thêm vào đó là bảo vệ những thông tin sức khỏe điện tử.

HIPAA nhận định thông tin an toàn điện tử, những luật lệ chung, phân tích rủi ro và quản lý. Phương pháp hành chính bảo vệ bao gồm bảo vệ vật lý, bảo vệ bằng công nghệ đảm bảo tính bí mật, tính nguyên vẹn và tính khả dụng của những thông tin sức khỏe được bảo vệ điện tử (ePHI)

Những lĩnh vực chính của an toàn thông tin mà HIPAA phát triển và duy trì tiêu chuẩn cùng với các nguyên tắc là:

- Giao dịch điện tử và đặt mã tiêu chuẩn (Electronic Transaction and Code sets Standards)
- Luật riêng tư (Privacy Rules)
- Luật an toàn (Security Rules)
- Yêu cầu nhận dạng quốc gia (national Identifier Requiments)
- Luật bắt buộc (enforcement Rules)

Đạo luật Sarbanes Oxley (Sarbanes Oxley Act (SOX))

Những yêu cầu then chốt hoặc điều khoản tổ chức của Sarbanes Oxley được thể hiện ở 11 tiêu đề dưới đây:

Title	Majors
Title I	Public company accounting oversight board
Title II	Auditor independence
Title III	Corporate responsibility
Title IV	Enhanced financial disclosures
Title V	Analyst conflicts of interest
Title VI	Commission resources and authority
Title VII	Studies and reports
Title VIII	Corporate and criminal fraud accountability
Title IX	White-collar crime penalty enhancements
Title X	Corporate tax returns
Title XI	Corporate fraud and accountability