Bài: 5.1 Phân tích lỗ hổng bảo mật (Vulnerability Analysis)

Xem bài học trên website để ủng hộ Kteam: 5.1 Phân tích lỗ hổng bảo mật (Vulnerability Analysis)

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!

Phân tích lỗ hổng bảo mật (Vulnerability Analysis)

Tóm tắt

Phân tích lỗ hổng bảo mật là một phần của công đoạn quét, đóng vai trò trọng yếu trong quy trình hacking. Ở chương này, chúng ta sẽ tìm hiểu các khái niệm về đánh giá lỗ hổng bảo mật, các công đoạn của việc đánh giá lỗ hổng bảo mật, các kiểu đánh giá, công cụ và những vấn đề quan trọng khác.

Khái niệm về đánh giá lỗ hổng bảo mật

Đây là nhiệm vụ cơ bản **penetration tester** phải thực hiện để tìm ra các lỗ hổng bảo mật trong một môi trường hệ thống. Việc đánh giá lỗ hổng bảo mật bao gồm tìm ra những điểm yếu, lỗi thiết kế hay bất cứ vấn đề bảo mật nào có thể khai thác để sử dụng hệ điều hành, ứng dụng hay website sai mục đích. Những lỗ hổng gồm có sai sót cấu hình, cấu hình mặc định, lỗi tràn bộ đệm (buffer overflow), lỗi hệ điều hành, dịch vụ mở (open services) và các lỗ hổng khác.

Hiện nay **quản trị viên hệ thống** và **pentester** có nhiều công cụ khác nhau để quét lỗ hổng bảo mật trong một hệ thống mạng. Những lỗ hổng được tìm thấy chia thành ba loại khác nhau dựa trên mức độ an ninh của nó, ví dụ thấp, trung bình hay cao. Bên cạnh đó, chúng cũng được phân loại dựa trên quy mô khai thác như gần hay xa.

Đánh giá lỗ hổng bảo mật

Đánh giá lỗ hổng bảo mật là quá trình kiểm tra, tìm tòi, nhận diện các biện pháp an toàn cũng như lỗ hổng của hệ thống và ứng dụng. Các hệ thống và ứng dụng được kiểm tra để nhận định tính hiệu quả của các tầng bảo mật hiện thời trong việc chống lại các tấn công và lạm dụng. Đánh giá lỗ hổng bảo mật cũng giúp nhận diện những lỗ hổng có thể khai thác, sự thiếu tầng bảo mật và những thông tin máy quét có thể phát hiện.

Các loại đánh giá lỗ hổng bảo mật

- **Đánh giá chủ động**: Đánh giá chủ động bao gồm việc trực tiếp gửi yêu cầu đến live network và kiểm tra các phản hồi. Nói ngắn gọn, quá trình đánh giá này yêu cầu thăm dò máy chủ mục tiêu.
- **Đánh giá thụ động**: Đánh giá thụ động bao gồm việc nghe trộm gói tin (packet sniffing) để tìm ra lỗ hổng, running services, open ports và các thông tin khác. Đây là quá trình đánh giá không can thiệp vào máy chủ mục tiêu.
- **Đánh giá từ bên ngoài**: Đây là quá trình đánh giá mà mục tiêu hacking là tìm ra lỗ hổng để khai thác từ bên ngoài.
- **Đánh giá từ bên trong**: Đánh giá từ bên trong bao gồm việc tìm ra lỗ hổng bảo mật bằng cách quét hệ thống mạng nội bộ và cơ sở hạ tầng mạng.

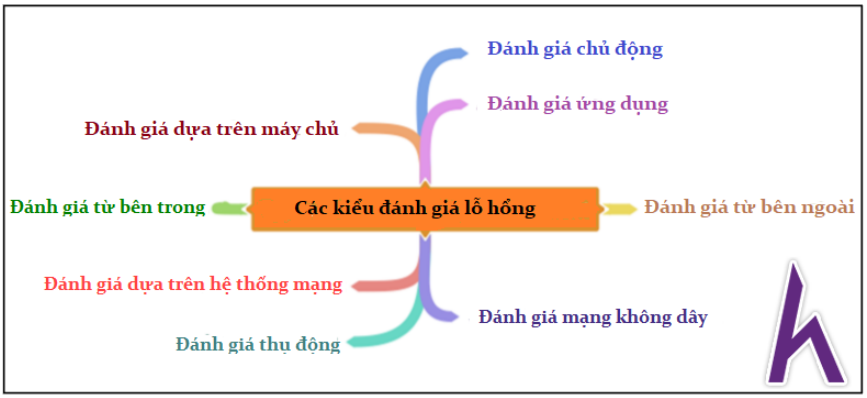

Figure 5-01 Types of Vulnerability Assessment

Chu trình đánh giá lỗ hổng bảo mật

Chu trình đánh giá lỗ hổng bảo mật bao gồm các công đoạn sau đây:

Tạo đường cơ sở

Tạo đường cơ sở là một công đoạn phải thực hiện trước trong chu trình đánh giá lỗ hổng bảo mật. Ở công đoạn này, **pentester** hay **quản trị viên hệ thống** phải nhận diện bản chất của hệ thống, ứng dụng và dịch vụ. Người đang thực hiện đánh giá sẽ tạo một bản kiểm nghiệm tất cả các tài nguyên và tài sản để dễ dàng quản lí và dành ưu tiên đánh giá. Bên cạnh đó, anh ta cũng lập bản vẽ cơ sở hạ tầng mạng, tìm hiểu kiểm soát an ninh, chính sách cũng như tiêu chuẩn mà tổ chức phải tuân thủ. Tóm lại, đường cơ sở giúp lên kế hoạch đánh giá một cách hiệu quả, lập thời gian biểu cho các công đoạn cũng như quản lí chúng theo thứ tự ưu tiên.

Đánh giá lỗ hổng bảo mật

Đánh giá lỗ hổng bảo mật tập trung vào đánh giá mục tiêu. Quá trình đánh giá bao gồm **thăm dò** và **điều tra** các biện pháp an toàn như physical security hay các chính sách an ninh. Công đoạn này đánh giá mục tiêu về các phần sai sót cấu hình, cấu hình mặc định, lỗi hay các lỗ hổng bằng cách thăm dò từng thành phần riêng biệt hoặc sử dụng các công cụ đánh giá. Khi quét xong, các dữ liệu tìm thấy được xếp hạng dựa trên mức độ ưu tiên. Cuối công đoạn, báo cáo đánh giá lỗ hổng bảo mật sẽ cho thấy tất cả các lỗ hổng được phát hiện, phạm vi cũng như mức độ ưu tiên của chúng.

Figure 5-02 Vulnerability Assessment Lifecycle

Đánh giá rủi ro

Đánh giá rủi ro bao gồm việc kiểm tra các lỗ hổng bảo mật và đánh giá ảnh hưởng của chúng lên hệ thống mạng hay tổ chức.

Giảm thiểu rủi ro

Công đoạn này bao gồm việc **giảm thiểu rủi ro** của những lỗ hổng bảo mật đã tìm thấy. Những lỗ hổng có mức độ ưu tiên được tiếp cận đầu tiên vì chúng có thể gây ra những ảnh hưởng nghiêm trọng.

Xác thực

Công đoạn **xác thực** để bảo đảm rằng tất cả các lỗ hổng bảo mật đã được loại bỏ.

Quan sát

Quan sát **network traffic** và **system behaviors** để phát hiện kịp thời nếu có xâm nhập.

Các giải pháp đánh giá lỗ hổng bảo mật

Các cách tiếp cận đánh giá lỗ hổng bảo mật khác nhau

Giải pháp dựa trên sản phẩm và giải pháp dựa trên dịch vụ

Giải pháp dựa trên sản phẩm được áp dụng cho mạng nội bộ của một tổ chức hoặc một hệ thống mạng riêng, nhưng thường là hệ thống mạng riêng.

Giải pháp dựa trên dịch vụ là bên thứ ba, cung cấp an ninh và kiểm nghiệm cho hệ thống mạng. Những giải pháp này có thể được áp dụng ở bên trong hoặc bên ngoài hệ thống. Trong trường hợp giải pháp này tiếp cận với mạng nội bộ thì có thể dẫn đến rủi ro về an toàn.

Đánh giá dạng cây và đánh giá hệ quả

Đánh giá dạng cây là phương pháp mà người kiểm nghiệm áp dụng những chiến lược khác nhau cho mỗi thành phần của môi trường hệ thống. Ví dụ, xem xét một hệ thống mạng của tổ chức trong đó có những máy móc riêng biệt, kiểm nghiệm viên có thể tiếp cận máy móc dùng hệ điều hành Windows khác với cách tiếp cận máy chủ dùng hệ điều hành Linux.

Đánh giá hệ quả là một phương pháp khác dựa vào bản kiểm kê của giao thức mạng trong môi trường hệ thống. Ví dụ, nếu kiểm nghiệm viên tìm được một giao thức, người này sẽ thăm dò các ports và services liên quan đến giao thức đó dựa trên đánh giá hệ quả.

Thực hiện đánh giá lỗ hổng bảo mật tốt nhất

Sau đây là một số bước cần thực hiện để việc đánh giá lỗ hổng bảo mật đạt hiệu quả. Quản trị viên hệ thống hay kiểm nghiệm viên cần áp dụng những bước sau:

- Trước khi sử dụng bất cứ công cụ nào để đánh giá lỗ hổng bảo mật, kiểm nghiệm viên phải hiểu rõ mọi chức năng của công cụ, từ đó tìm được công cụ phù hợp nhất để thu thập thông tin cần thiết.
- Đảm bảo công cụ sử dụng không gây tổn hại hoặc vô hiệu hóa những dịch vụ đang chạy của hệ thống mạng.
- Xác định rõ source location của máy quét để thu hẹp phạm vi focus.
- Quét thường xuyên để xác định lỗ hổng.

Hệ thống đánh giá lỗ hổng

Hệ thống đánh giá lỗ hổng chung (CVSS)

Hệ thống đánh giá lỗ hổng chung là một cách để nhận biết những tính chất cơ bản của lỗ hổng và đưa ra con số cụ thể cho mức độ nghiêm trọng của nó. Những con số này được sắp xếp vào các nhóm với một số đại diện định tính (ví dụ như low, medium, high và critical). Điều này giúp tổ chức đánh giá và dành thứ tự ưu tiên xử lí lỗ hổng một cách đúng đắn nhất.

Mức độ an toàn	Điểm đánh giá tương đương
Không (None)	0.0
Thấp (Low)	0.1 – 3.9
Trung bình (Medium)	4.0 – 6.9
Cao (High)	7.0 – 8.9
Nghiêm trọng (Critical)	9.0 – 10.0

Table 5-01 CVSSv3 Scoring

Để tìm hiểu thêm về CVSS-SIG, hãy vào website

> https://www.first.org.

Hệ thống lỗ hổng và phơi nhiễm thông thường (CVE)

CVE là một nền tảng khác mà bạn có thể tìm kiếm thông tin về lỗ hổng ở đó. **CVE** cung cấp danh sách các lỗ hổng an minh mạng đã phát hiện cùng với số nhận dạng và mô tả.

Dữ liệu lỗ hổng quốc gia Mỹ (NVD) vừa được thành lập bởi Viện Tiêu chuẩn và Kỹ thuật quốc gia (NIST). NVD dựa trên những thông tin thu được từ dữ liệu đầu vào CVE để cung cấp thêm các thông tin nâng cao cho mỗi đầu vào, ví dụ như thông tin sửa chữa, điểm nghiêm trọng và đánh giá ảnh hưởng. Bên cạnh đó, NVD cũng cung cấp những công cụ tìm kiếm nâng cao, ví dụ như tìm bằng OS, bằng tên nhà cung cấp, tên sản phẩm, hoặc/ và số hiệu version; hay bằng kiểu lỗ hổng, độ nghiêm trọng, quy mô khai thác và ảnh hưởng.

Để tìm hiểu thêm về CVE, vào website http://cve.mitre.org.

Quét lỗ hổng

Trong thời đại công nghệ phát triển như hiện nay, việc tìm kiếm các lỗ hổng bảo mật trong một môi trường hệ thống nhất định đã trở nên dễ dàng hơn nhờ các công cụ khác nhau. Các công cụ từ tự động đến thủ công đều sẵn có để giúp đỡ việc tìm kiếm.

Máy quét lỗ hổng là công cụ tự động được thiết kế chuyên dụng cho tìm kiếm lỗ hổng, điểm yếu, vấn đề cần giải quyết trong một hệ điều hành, mạng, phần mềm hay ứng dụng. Những công cụ quét này có thể thăm dò kĩ lưỡng scripts, open ports, banners, running services, configuration errors (lỗi cấu hình) và các khu vực khác.

Những công cụ quét lỗ hổng này bao gồm:

- Nessus
- OpenVAS
- Nexpose
- Retina
- GFI LanGuard
- Qualys FreeScan, và nhiều công cụ khác.

Không chỉ chuyên gia bảo mật mà cả những kẻ có ý định tấn công hệ thống mạng cũng sử dụng những công cụ trên để tìm ra rủi ro và lỗ hổng.

Các công cụ quét lỗ hổng

1. GRI LanGuard

GFI LanGuard là một phần mềm vá lỗ hổng (patch management) và an ninh mạng, làm nhiệm vụ cố vấn an ninh thế giới ảo. Phần mềm này cung cấp:

- Patch Management dành cho Windows®, Mac OS® and Linux®
- Patch Management dành cho những ứng dụng bên thứ ba
- Quét lỗ hổng bảo mật cho máy tính và thiết bị di động
- Kiểm kê thông minh hệ thống mạng và phần mềm
- Web reporting console
- Tìm những lỗ hổng mới nhất và missing updates

2. Nessus

Nessus Professional Vulnerability Scanner là phần mềm quét lỗ hổng bảo mật toàn diện nhất do **Tenable Network Security** sáng lập. Máy quét này tập trung đánh giá lỗ hổng và cấu hình. Phần mềm này cho phép người dùng tùy biến, đặt thời gian biểu việc quét cũng như xuất báo cáo.

3. Qualys FreeScann

Công cụ này cho phép quét lỗ hổng bảo mật online. Nó cung cấp bản tóm tắt những tiêu chuẩn pháp lý và an ninh của hệ thống mạng và web cùng với đề nghị. **Qualys FreeScan** có hiệu quả với:

- Quét lỗ hổng bảo mật cho server và app.
- Vá
- Kiểm nghiệm OWA SP Web Application

- Kiểm nghiệm SCAP Compliance

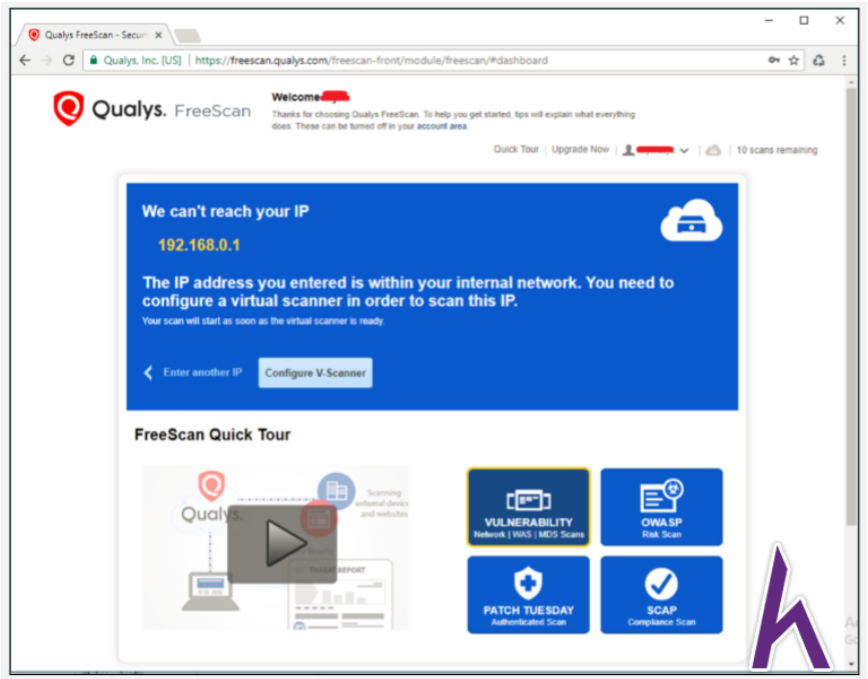

Figure 5-05 Qualys FreeScan Vulnerability Scanning Tool

Vào trang web http://www.qualys.com để mua công cụ quét lỗ hổng hoặc đăng kí trial version. Để quét mạng nội bộ, Qualys cung cấp Virtual Scanner. Máy quét này có thể được ảo hóa để phù hợp với tất cả môi trường máy chủ ảo. Bảng số liệu sau đây là kết quả quét lỗ hổng trên một mục tiêu hệ thống.

Công cụ quét lỗ hổng dành cho điện thoại

Danh sách các công cụ quét lỗ hổng cho điện thoại được liệt kê trong danh sách dưới:

- Retina CS for Mobile: http://www.byondtrust.com
- Security Metrics Mobile Scan:http://www.securitymetrics.com
- Nessus Vulnerability Scanner: http://www.tenable.com

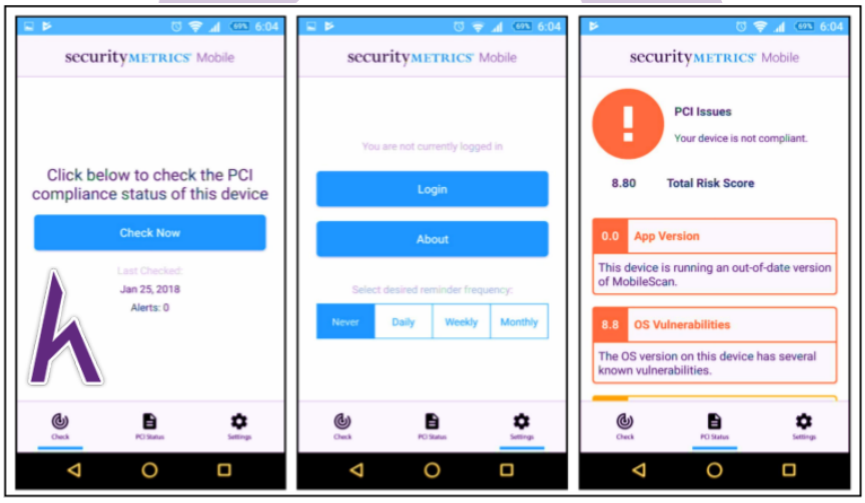

Figure 5-07 Security Metrics Mobile Scan