Module 19
Penetration Test

Những Chủ Đề Chính Trong Chương Này

Security Assessment Là Gì ?

Các Mô Hình Penetration Test

Các Bước Của Quá Trình Penetration Test

Công Cụ Tiến Hành Penetration Test

Security Assessment Là Gì ?

"Biết người biết ta trăm trận trăm thắng" là câu thành ngữ nổi tiếng của binh pháp Tôn Tử, vì vậy trong nhiều tài liệu về an toàn thông tin hay trích dẫn câu nói này với tiêu đề "Know Your Enemy" . Thật vậy, để có thể bảo mật thông tin và phòng chống các cuộc tấn công của hacker thì chính những người chịu trách nhiệm về an ninh cần phải nắm rõ những cách thức mà hacker sẽ tiến hành để tấn công vào hệ thống. Nói cách khác, chúng ta cần phải đột nhập vào hệ thống của mình như là một hacker, quá trình này được gọi là penetration test (gọi tắt là pentest) còn những người thực hiện chính là các penetration tester.

Trước tiên penetration tester hay những chuyên gia an ninh mạng cần tiến hành đánh giá mức độ bảo mật thông tin, ước lượng các rũi ro có thể xảy ra cho hệ thống mạng, Quá trình này được gọi là Security Assessment. Đây cũng là một bước trong tiến trình kiểm định bảo mật mà chúng ta hay gọi bằng thuật ngữ security audit và cuối cùng là thực hiện penetration test. Đây là các công việc quan trọng cần được thực hiện bởi những chuyên gia có kinh nghiệm và tiến hành theo quy trình khoa học để đem lại hiệu quả cao nhất.

Trong quá trình kiểm định bảo mật hay đánh giá các điểm yếu của hệ thống chúng ta cần quét các lớp mạng để tìm ra những lỗ hỗng của hệ thống tồn tại trong các dịch vụ hay máy trạm, máy chủ, xác định các hệ thống đang hoạt động cùng những dịch vụ đang chạy trên các cổng tương ứng, và có hay không những lỗi cấu hình như gán quyền sai, sử dụng thông tin cấu hình mặc định là các default password có thể bị các hacker lợi dụng để xâm nhập hệ thống và đánh cắp dữ liệu. Sau đó, các hacker thiện chí hay pentration tester sẽ dựa trên những thông tin này để thực hiện một cuộc tấn công thực sự vào hệ thống nhằm kiểm tra xem mức độ thiệt hại và khả năng chịu đựng các cuộc tấn công trên.

Các Mô Hình Penetration Test

Có hai mô hình pentest là white-box và black-box tương ứng với vị trí của pentration tester là ở bên trong hay bên ngoài hệ thống mục tiêu.

Ở mô hình black-box các penetartion tester sẽ như là các hacker black-hat thực sự nằm bên ngoài hệ thống, do đó việc đánh giá bảo mật cần phải tiến hành theo đúng quy trình hacking mà chúng ta đã thảo luận từ Module 2 trở đi đó là tìm kiếm và tập trung tất cả những thông tin liên quan đến mục tiêu từ các nguồn trên internet như cơ sở dữ liệu Whois, tiến hành thu thập thông tin DNS, sử dụng Google để tìm kiếm nâng cao với các tùy chọn liên quan đến trang web của tổ chức, các địa chỉ email công bố trên các diễn đàn công cộng. Sau đó là quét lỗi nhằm xác định các lổ hỗng bảo mật hay các khiếm khuyết liên quan đến ứng dụng đang chạy rồi từ đó xác định phương pháp tấn công thông qua internet nhằm vào mục tiêu.

Quá trình pentest theo mô hình black-box có thể gây ra một số vấn đề ảnh hưởng đến quá trình hoạt động của hệ thống, do đó trước khi tiến hành các bạn cần sao lưu những dữ liệu quan trọng cẩn thận hay có một chế độ bảo đảm tính liên tục của hệ thống nhằm tránh

những tác động tiêu cực. Vì pentest là một quá trình tấn công hợp lệ, cần có sự đồng ý của đơn vị chủ quản nên những người quản lý có quyền đưa ra những ngoại lệ mà penetration tester không nên thử nghiệm tấn công, tất cả những điều này sẽ được quy định rõ trong bản yêu cầu dịch vụ Service Level Argeement (SLA).

Ngược lại với mô hình back-box, khi các penetration tester đánh giá bảo mật và thử nghiệm tấn công từ phía bên trong mạng nội bộ sẽ được gọi là white-box, và khác với tình huống tấn công từ bên ngoài những mối đe dọa từ bên trong sẽ có những thuận lợi hơn do cùng hệ thống nên có sự tương tác trực tiếp về vật lý với máy chủ, máy trạm hay thông tin liên lạc của người dùng. Các tài liệu thống kê cho rằng những nguyên nhân mất mát dữ liệu từ bên trong mạng nội bộ nhiều đến mức ngạc nhiên, lên đến 80 % , và tại Việt Nam chúng ta cũng đã thấy các tình huống những nhân viên bị nghĩ việc đã cố tình phá hoại dữ liệu, tấn công trang web để làm xâu hình ảnh của đơn vị chủ quản trước đây của mình. Chính vì vậy chúng ta cần đánh giá cặn kẽ những mối nguy hiểm đến từ bên trong để có hình thức đối phò và đề phòng thích hợp.

Nếu công ty hay tổ chức chỉ muốn đánh giá và kiểm định vấn đề an toàn thông tin thì những tình huống tương ứng khi thực hiện ở bên trong và bên ngoài hệ thống là internal assessment và external assessment. Để đạt được hiệu quả cao tổ chức cần tuyển dụng những nhân viên có chuyên môn trong lĩnh vực an ninh mạng hay thuê bên ngoài thực hiện công việc này. Các chuyên gia có chứng chỉ kiểm định bảo mật quốc tê CISA là những người thích hợp.

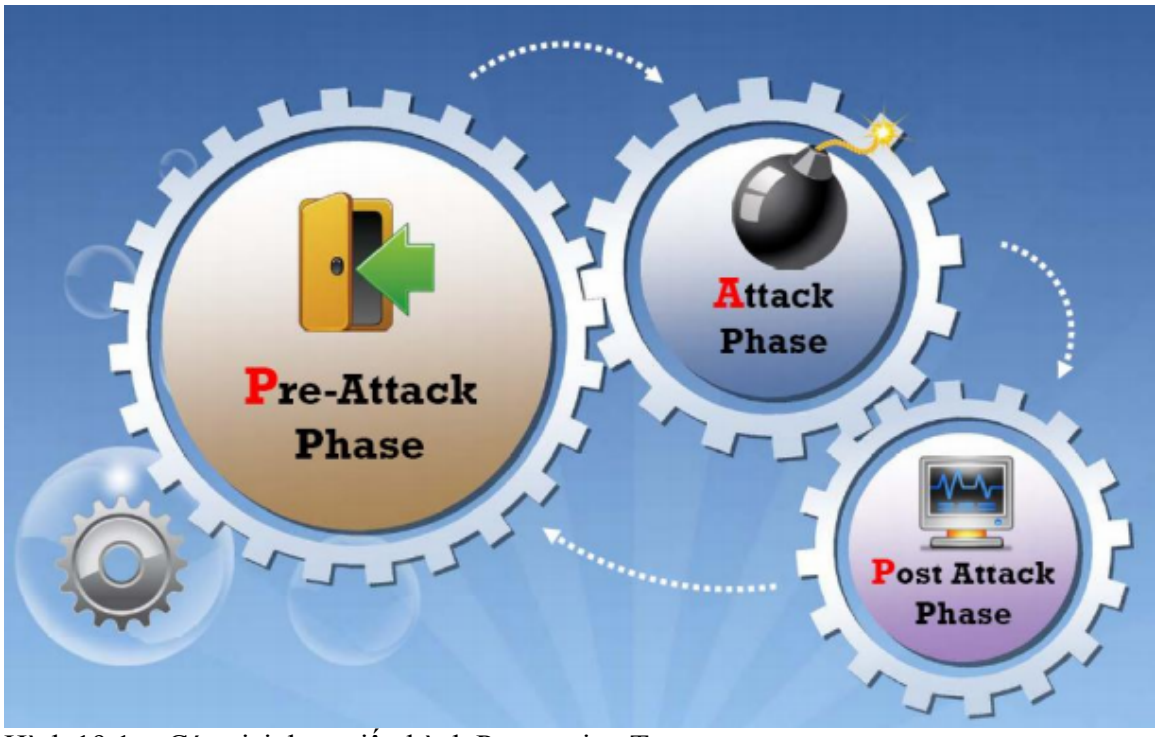
Về mặt công cụ thì các hacker dù là black hat hay white hat, ở bên trong hay bên ngoài hệ thống cũng đều sử dụng nhưng công cụ như nhau. Có thể đó là những ứng dụng thương mại với nhiều chức năng mạnh mẽ và thường là rất dễ sử dụng, đôi khi tiến hành các thao tác thăm dò và khai thác hoàn toàn tự động như Core Impact hoặc các công cụ chuyên tìm kiếm lỗi của ứng dụng Web như Web Acunetix. Ngoài ra, những chương trình miễn phí hay mã nguồn mở cũng là các công cụ được nhiều chuyên gia bảo mật và ngay cả các hacker tin dùng như Nessus – Công cụ mạng và bảo mật số 1 thế giới hiện nay được đánh giá bởi hơn 2600 hacker, hay Metasploit Framwork mà chúng ta đã có dịp tham khảo những chức năng mạnh mẽ của chúng qua các ví dụ minh họa. Tuy nhiên, việc sử dụng những công cụ audit tự động nay cũng có một số điểm hạn chế như phát hiện sai khi chưa kịp cập nhật thông tin nhận dạng của các lổ hỗng, do đó chúng ta cần update những chương trình này đầy đủ và kết hợp giữa các ứng dụng kiểm định tự động với các phương pháp thủ công thông qua việc hoạch định, lập lịch cũng như đánh giá các rũi ro dựa trên tình hình thực tế của hệ thống hay khảo sát nhu cầu của người dùng.

Tuy nhiên, trong quá trình kiểm định và pentest thủ công chúng ta cần thuê các chuyên gia giàu kinh nghiệm để đạt được hiệu quả cao nhất. Những người có kỹ năng hacking như CEH và có kiến thức về kiểm định bảo mật (ví dụ có chứng chỉ CISA) là những chuyên gia đáng tin cậy để tổ chức, doanh nghiệp thuê làm pentest và audit hệ thống.

Các Bước Của Quá Trình Penetration Test

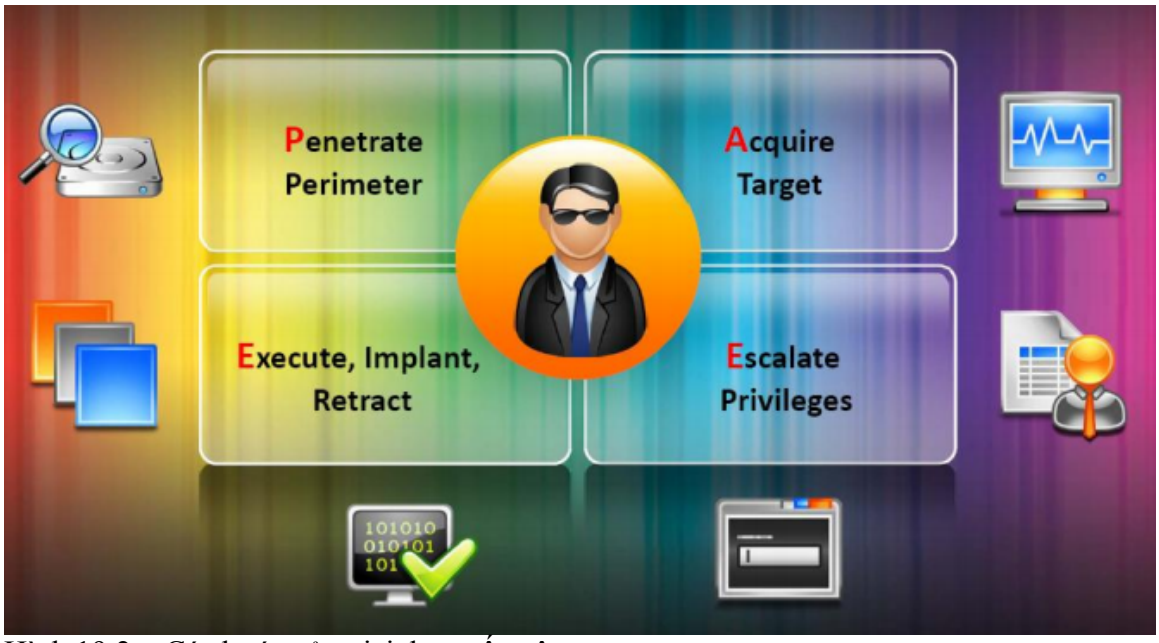
Quá trình Penetration Test gồm có ba giai đoạn đó là :

- Giai đoạn Pre-attack
- Giai đoạn tấn công
- Giai đoạn tổng kết Post-attack



Hình 19.1 - Các giai đoạn tiến hành Penetration Test

Trong giai đoạn Pre-attack chúng ta cần tập hợp các thông tin liên quan đến hệ thống từ các nguồn dữ liệu công cộng từ Whois hay DNS Check tương ứng với giai đoạn Footprinting và Reconnaissance. Sau khi thu thập đầy đủ các thông tin cần thiết thì giai đoạn tấn công thực sự mới bắt đầu, quá trình này sẽ gồm *Penetrating The Perimeter, Acquiring The Target, Escalating Priveledge Và Executing, Implant Và Retracing* với ý nghĩa của từng giai đoạn như sau :



Hình 19.2 – Các bước của giai đoạn tấn công

Penetrating The Perimeter : Công đoạn này gồm có xem xét các bao cáo lỗi, kiểm tra danh sách truy cập Access Control List, đánh giá các bộ lọc giao thức hay những quy tắt được áp đặt trên Firewall đối với các giao thức như SSH, FTP, Telnet. Ngoài ra, người thực hiện cần tiến hành kiểm lỗi tràn bộ đệm, SQL injection, hay tấn công DoS. Bên cạnh đó nên kiểm tra thêm về cấu hình của hệ thống mạng không dây hay các ứng dụng web nội bộ.

Acquiring The Target : Đây là quá trình tận dụng các kết quả đã xác định như những lổ hỗng hệ thống, lỗi bảo mật của ứng dụng để tấn công, xâm nhập vào mục tiêu. Trong giai đoạn này các bạn có thể sử dụng các chương trình khai thác tự động như CORE IMPACT hay ứng dụng chuyên dùng cho các penetration tester là Back Track (phiên bản hiện nay là BackTrack 5).

Escalating Privilege : Sau khi thâm nhập hệ thống hacker sẽ tiến hành nâng quyền với để chiếm quyền quản trị cao nhất. Hành động này được gọi là Escalating privilege hay leo thang mức ưu tiên.

Executing, Implanting, Reacting : Đây là công đoạn cuối cùng của quá trình penetration test. Cần lưu ý các hành động của chúng ta trong các giai đoạn này không được gây ảnh hưởng đến quá trình hoạt động của doanh nghiệp, vì vậy một số tổ chức sẽ yêu cầu chúng ta không tiến hành một số thao tác trong giai đoạn này như việc chạy thử nghiệm một số ứng dụng có khả năng làm lộ những thông tin mật, ảnh hưởng đến hoạt động chung …

Cuối cùng là ***post-attack*** bao gồm việc tạo báo cáo đánh giá chi tiết về những lỗi bảo mật, các rũi ro đối với an toàn thông tin và trình bày những vấn đề này trước khách hàng hay

hội đồng thẩm định. Đưa toàn bộ hệ thống trở về trạng tháo hoạt động trước đây nếu như trong quá trình tiến hành có những sự thay đổi. Một vấn đề cần quan tâm nữa là chúng ta phải đưa ra được các giải pháp nhằm khắc phục các điểm yếu bảo mật đã phát hiện.

Những Công Cụ Tiến Hành Tấn Công Tự Động

Các công cụ dùng để penetration test hay tấn công có rất nhiều loại khác nhau, tùy thuộc nhu cầu và khả năng tài chính của mỗi tổ chức mà chúng ta sẽ dùng bản có phí hay miễn phí, chương trình chạy trên Windows hay Linux …Sau đây là một số ứng dụng cần quan tâm :

Nessus : Đây là ứng dụng được đánh giá là số 1 trong các công cụ bảo mật thông tin, việc đánh giá này được thực hiện trên 3000 hacker và chuyên gia bảo mật. Nessus có khả năng dò tìm những lỗ hổng bảo mật cho nhiều ứng dụng, hệ thống và cả thiết bị khác nhau một cách tự động. Điểm đặc biệt là Nessus hoạt động theo mô hình client – server nghĩa là chỉ cần cài ứng dụng trên một máy và tiền hành quét từ nhiều máy khác nhau.

GFI LANGuard : Một ứng dụng quét lỗi rất mạnh mẽ được nhiều ngân hàng sử dụng, có khả năng phát hiện lỗi dựa trên cơ sở dữ liệu nhận dạng lớn và đặc biệt là GFI LAN Guard có thể vá lỗi trên các máy tính trong hệ thống như bật chức audit, vá lỗi từ xa.

CORE IMPACT : Chương trình dò lỗi và tự động khai thác các mục tiêu.

MBSA : Ứng dụng miễn phí chạy trên hệ thống Windows dùng để dò tìm các bản cập nhật hệ thống, bản vá 1ỗi bảo mật cho hệ điều hành và ứng dụng được phát triển bởi Microsoft như SQL Server, Exchange Server. MBSA được phát triển bởi Microsoft nên khả năng tìm kiếm và quét lỗi trên hệ thống mạng Widnows rất tốt.

BackTrack : Ứng dụng này hoàn toàn miễn phí, và có thể nói là công cụ toàn diện nhất cho các hacker cũng như các penetration tester. Với hơn 200 công cụ từ khai thác, dò lỗi, tấn công và cả dịch vụ honeypot …BackTrack đáp ứng được đây đủ nhu cầu của các penetration tester hay attacker. Các bạn có thể sử dụng BackTrack trên đĩa DVD mà không cần cài đặt, nhưng BackTrack sẽ hoạt động tốt hơn, cũng như có thể lưu lại kết quả, báo cáo nếu các bạn cài ứng dụng này trên đĩa cứng hay cài trên USB và khởi động trực tiếp từ thiết bị này.

Tổng Kết

Như vậy, chúng ta đã năm về khái niệm penetration test cùng các quy trình và mô hình hoạt động của quá trình tấn công thử nghiệm. Những ứng dụng tìm kiếm lỗi và khai thác, tấn công mạnh mẽ. Cần lưu ý penetration test là "tấn công để phòng thủ" cho nên chúng ta cần phải cung cấp báo cáo đầy đủ cho khách hàng, hay tổ chức mà chúng ta tiến hành pentest.

- Liệt kê các lỗi được tìm thấy, những mối nguy hiểm hay rũi ro có thể xảy ra.
- Phân tích kết quả.
- Thảo luận và giải thích về những kết qua đã tìm ra.
- Đo lường mức độ nguy hiểm.
- Lưu giữ lại các tập tin nhật kí, và cung cấp các công cụ lưu giữ chứng cứ nhằm phục vụ công tác điều tra khi có sự cố xảy ra.
- Tạo một bản tóm tắt của toàn bộ quá trình làm việc. Đặt tên và ngày giờ thực hiện.
- Và cuối cùng phải lưu giữa và gởi các kết quả này cho những người có thẩm quyền qua các kênh an toàn, bảo mật cao nhất.