MODULE 1

Những Nội Dung Chính Trong Chương Này

Các Thuật Ngữ Về An Toàn Thông Tin
Những Kỹ Thuật Tấn Công
Các Giai Đoạn Tấn Công
Hacktivism Là Gì
Phân Loại Hacker
Hành Động Của Ethical Hacker
Mục Tiêu Của Những Kẻ Tấn Công
Những Kỹ Năng Cần Thiết Để Trở Thành Ethical Hacker
Tìm Kiếm Các Lổ Hỗng Bảo Mật
Quy Trình Tấn Công Thử Nghiệm
Tạo Bản Kế Hoạch Đánh Giá Bảo Mật
Blackbox Và Whitebox
Các Kiểu Tấn Công Của Ethical Hacker
Ethical Hacking Report
Tính Hợp Lệ Của Việc Tấn Công

Khi nhắc đến hacker có lẽ hầu hết chúng ta đều liên tưởng đến các trang web bị tấn công và thay đổi giao diện, việc sử dụng trái phép thẻ tín dụng hay hình ảnh của một nhóm người mang mặt nạ là các thành viên thuộc nhóm hacker Anonymous, xa hơn nữa là những thông tin mật bị đánh cắp và đăng tải trên trang web Wikileak mà chương trình truyền hình đã đưa tin. Như vậy, một cách không chính thức mọi người đều cho rằng hacker là những kẻ xấu chuyên phá hoại và ăn trộm định danh, thông tin bí mật trên mạng internet, và điều này hoàn toàn sai đặc biệt là trong lĩnh vực CEH.

CEH viết tắt của Cetified Ethical Hacker là chứng chỉ công nhận những hacker thiện chí hay còn gọi là hacker mũ trắng, những người có kỹ năng của một hacker nhưng hành động của họ hoàn toàn trong sáng, không vi phạm pháp luật mà còn đóng góp cho vấn đề bảo mật, an toàn thông tin.

Các Thuật Ngữ Về An Toàn Thông Tin

Để có thể nhận thức được các mối nguy hiểm chúng ta cần hiểu một số thuật ngữ sau trong lĩnh vực an toàn thông tin, đó là *threat, remote exploit, local exploit, vulnerability, target of evaluation, attack.*

Threat là các mối đe dọa đối với sự an toàn của thông tin bao gồm hacker, virus, sự cố máy tính như hư hỏng phần cứng, lỗi phần mềm cho đến những nguyên nhân do thiên tai, hỏa hoạn cũng là các threat.

Vulnerability là những điểm yếu về bảo mật của hệ thống như thiếu các bản vá lỗi bảo mật, sử dụng chính sách mật khẩu yếu … đều là các điểm nhạy cảm có khả năng bị các *threat* khai thác gây mất an toàn thông tin.

Exploit là quá trình khai thác các điểm yếu bảo mật để đánh cắp thông tin, tiến trình này có thể được thực hiện bởi những tác nhân bên trong hay bên ngoài hệ thống.

Remote exploit là quá trình khai thác các lỗ hỗng bảo mật từ xa ở trên máy tính khác hay từ internet.

Local exploit là quá trình khai thác những điểm yếu bảo mật ngay trên hệ thống để tiến hành leo thang nâng quyền hạn của một tài khoản, hay bẻ khóa mật khẩu của ứng dụng.

Target of evaluation là những mục tiêu có khả năng chứa các lổ hỗng bảo mật có thể bị tấn công. Các mục tiêu nay có thể là một máy chủ, máy trạm,những ứng dụng hay các trang web.

Attack là thuật ngữ chỉ tiến trình tấn công vào mục tiêu.

Những Kỹ Thuật Tấn Công

Có nhiều công cụ và phương pháp để tìm kiếm các lổ hỗng bảo mật, tiến hành khai thác, tấn công hệ thống. Những kỹ thuật này bao gồm trojan, backdoor, sniffer, rootkit, khai thác lỗi tràn bộ đệm Buffer Overflow hay SQL Injection … mà chúng ta sẽ thảo luận trong các phần sau. Thông thường hacker sẽ tập trung tìm kiếm các lổ hỗng bảo mật của những thành phần :

Hệ Điều Hành : Nhiều hệ thống được cài đặt và cấu hình mặc định, nghĩa là không có sự thay đổi hay tùy biến để nâng cao tính an toàn. Ngoài ra, những máy tính không được cập nhật các bản vá hay cài đặt các chương trình sữa lỗi bảo mật cũng là mồi ngon của các kẻ tấn công.

Ứng Dụng : Mỗi máy tính có nhiều ứng dụng được cài đặt, nếu những chương trình này có lổ hỗng bảo mật cũng có thể bị hacker tấn công chiếm quyền điều khiển từ xa.

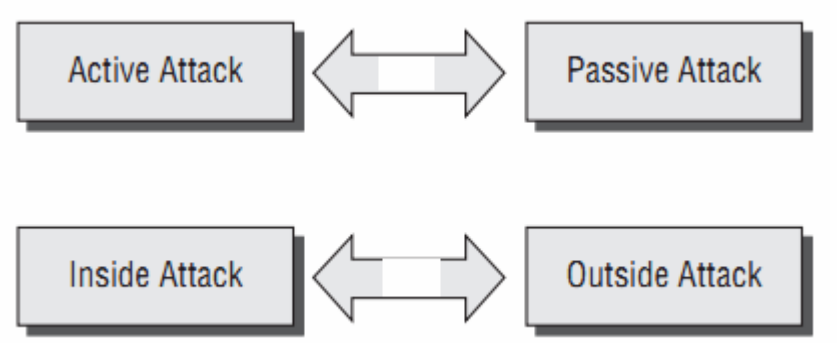
Shrink-wrap Code : Đây là các thành phần mở rộng của ứng dụng mà nhiều người dùng không hề hay biết, nhưng hacker sẽ biết rất rõ các thành phần này ví dụ như chức năng macro trong ứng dụng MS Word cho phép các hacker chạy những chương trình độc hại trong ứng dụng xử lý văn bản này. Hay các lỗi Active X cho phép hacker chạy lệnh từ xa thông qua trình duyệt của nạn nhân

Lỗi Cấu Hình : Việc cấu hình sai là một trong những nguyên nhân chính khiến hệ thống bị tấn công, ví dụ các lỗi liên quan đến việc gán quyền không chặt chẽ có thể cho phép hacker hay người dùng bất kì sao chép và chạy những chương trình trái phép.

Bên cạnh các kỹ thuật trên, những cuộc tấn công được chia làm hai trạng thái hoạt động là *passvie* (bị động) và *active* (chủ động). Những cuộc tấn công bị động thường khó dò tìm hơn vì không tương tác trực tiếp vào hệ thống hay đường truyền mà chỉ âm thầm thu thập các thông tin, dữ liệu. Nghe lén hay *sniffing* là dạng tấn công thuộc loại này, những hacker nghe lén dữ liệu được gọi là sniffer và thường tập trung vào tính riêng tư của thông tin.

Trong khi đó dạng tấn công chủ động có sự tương tác trực tiếp vào hệ thống xác thực hay đường truyền làm thay đổi tính toàn vẹn, ảnh hưởng đến khả năng đáp ứng của dữ liệu. Những dạng tấn công thuộc loại này như DDoS, Scan Port …

Bên cạnh sự phân loại tấn công dựa trên trạng thái hoạt động thì chúng ta còn xác định chúng theo vị trí địa lý là ở phía bên trong hay bên ngoài hệ thống tương ứng với các thuật ngữ là *insise* hay *outside*. Những kẻ tấn công *inside* là các *insider* thường là nhân viên hay những người có mối liên quan trực tiếp đối với tổ chức, vì vậy tác động của dạng tấn công này rất lớn và nguy hiểm. Theo một số thông kê thì có tới 80 % tác nhân gây mất mát thông tin là những thành viên bên trong của hệ thống. Tuy nhiên, những thành viên bên ngoài lại có những mối nguy hiểm khác vì họ thường đông đảo hơn, có trình độ kỹ thuật cao và mục tiêu tấn công của họ thường nhắm vào những hệ thống ít được bảo vệ hay có sự giao tiếp với môi trường công cộng (còn được gọi là môi trường không tin cậy) như các máy chủ cơ sở dữ liệu, trang web.

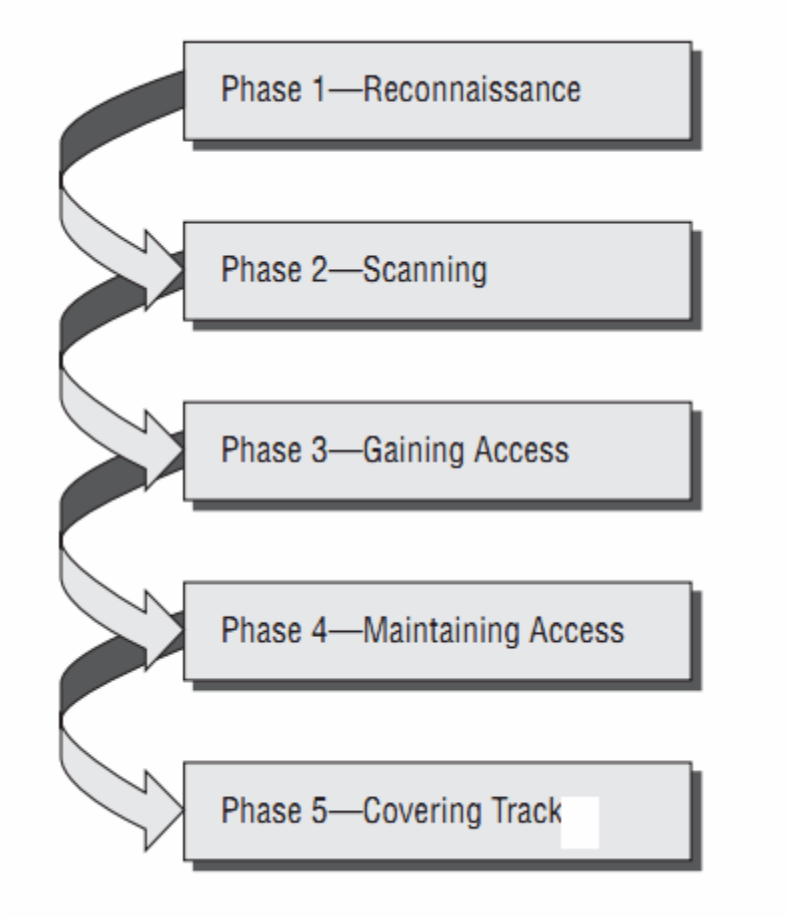


Hình 1.1 – Phân loại các dạng tấn công dựa trên trạng thái hoạt động và vị trí địa lý.

Trong bài thi lấy chứng chỉ CEH có nhiều câu hỏi liên quan đến các dạng tấn công này, do đó chúng ta cần ghi nhớ các đặc điểm chính của mỗi loại tấn công để có thể đưa ra câu trả lời chính xác nhất.

Các Giai Đoạn Tấn Công

Một cuộc tấn công được chia làm năm giai đoạn là Reconnaissance, Scaning, Gaining Access, Maintaining Access, và Covering Track một số tài liệu còn gọi là Clear Track như hình 1.2



Hình 1.2 - Năm giai đoạn tấn công.

Phase 1 : Passive và Active Reconnaissance

Reconnaissance là giai đoạn thu thập thông tin. Và *passive reconnaissance* là quá trình thu thập dữ liệu của một mục tiêu hay tổ chức mà không biết thông tin gì về tổ chức trên. Quá trình passive reconnaissance có thể chỉ đơn giãn là theo dõi thông tin hoạt động của một tòa nhà công sở để ghi nhận lại giờ giấc làm việc của nhân viên, tuy nhiên quá trình này thường được thực hiện thông qua các chương trình tìm kiếm như Google hay cơ sở dữ liệu Whois. Công đoạn này còn được gọi là *information gathering* hay thu thập thông tin trong toàn bộ tiến trình tấn công của hacker. Một trong các phương pháp thu thập thông tin một cách bị động như *social engineering* và dumpster diving mà chúng ta sẽ trình bày ở các chương sau.

Hình thức tấn công sniffing hay nghe lén là một trong những ví dụ điển hình nhất cho passive reconnaissance, với phương pháp này hacker có thể thu thập được nhiều thông tin giá trị như dãy địa chỉ IP, tên miền của tổ chức, các máy chủ ẩn danh hay những dịch vụ đang hoạt động trên mạng. Nghe lén thông tin tương tự như các hệ thống giám sát trong tòa nhà hoặc các thiết bị thu âm chuyên dùng để đánh cắp thông tin cuộc gọi, các cuộc nói chuyện của mục tiêu mà chúng ta thường thấy trên phim ảnh.

Ngược lại, *active reconnaissance* là quá trình thu thập thông tin của mục tiêu theo hình thức chủ động, lúc này hacker sẽ tác động trực tiếp lên đối tượng để ghi nhận các dữ liệu phản hồi. Một ví dụ của tình huống *active reconnaissance* là khi kẻ tấn công tiến hành dò quét mạng để xác định các máy đang hoạt động hay những dịch vụ đang chạy trên một hệ thống nào đó thông qua các công cụ như Nessus, Supperscan. Vì mang tính chất chủ động nên kết quả thu thập được sẽ nhanh chóng và khả quan hơn so với *passive reconnaissance* nhưng *acvtive reconnaissance* dễ bị phát hiện, dò tìm hơn.

Cả hai hình thức *passive reconnaissance* và *active reconnaissance* thường được các kẻ tấn công sử dụng để tìm kiếm thông tin hữu ích về máy chủ web hay hệ điều hành đang sử dụng. *Reconnaissance* cũng được thực hiện bởi các chuyên gia bảo mật trong tiến trình tấn công thử nghiệm gọi là *penetration test* hay *pentest*. Tuy nhiên, *pentest* là hành động hợp pháp nên người thực hiện là *penetration tester* thường sử dụng *active reconnaissance* để nhanh chóng thu nhận kết quả.

Phase 2 : Scanning

Scanning là quá trình thuộc giai đoạn thu thập thông tin *reconnaissance* . Các hacker tiến hành *scanning* bằng các chương trình quét lỗi hệ thống, quét địa chỉ IP hay các cổng đang mở bằng ứng dụng *Nmap*, *là Acunetix Web Vulnerability Scanner*, hay *Angry Ip Scan*. Chúng ta sẽ thảo luận chi tiết về *scanning* trong **Module 3 Scanning Network**.

Phase 3 : Gaining Access

Gaining access là quá trình thâm nhập mục tiêu khi quá trình khai thác và tấn công thành công. Lúc này hacker sẽ xâm nhập vào hệ thống và tiến hành các hành động đánh cắp tập tin mật khẩu hay phá hủy dữ liệu, chạy những chương trình nguy hiểm, leo thang đặc quyền để có thể truy cập vào các khu vực thông tin bí mật. Muốn thâm nhập thành công hacker cần sử dụng thông tin mà tiến trình *reconnaissance* và *scanning* thu thập được, dựa trên các thông tin này hacker sẽ xác định phương án tấn công hợp lý như sử dụng mã khai thác lỗi tràn bộ đệm (buffer overflow), hay chiếm quyền sử dụng của phiên làm việc của người dùng (session hijacking) mà chúng ta sẽ trình bày trong các **Module 11 Session Hijacking** và **Module 17 Buffer Overflow** của giáo trình.

Phase 4: Maintaining Access

Một khi đa xâm nhập hệ thống thành công hacker thường cài đặt chương trình gián điệp để có thể duy tri sự kiểm soát, nghe lén thông tin người dùng nhập vào từ bàn phím hay mơ các công hậu để có thể quay lại vào các lần sau, công đoạn này được gọi là maintaining access. Những mã độc nguy hiểm các hacker dùng để cấp vào máy tính bị

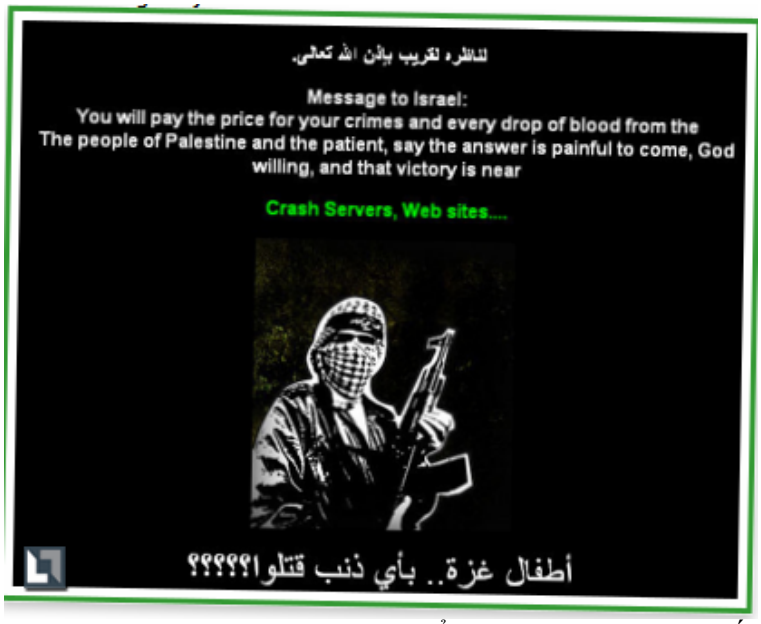
tấn công được gọi là trojan hay backdoor, các khái niệm này sẽ được trình bày trong module 6 của giáo trình CEH.

Phase 5: Covering Track

Covering track hay clear track là hành động xóa dấu vết của các hacker để tránh bị phát hiện. Các hành động này có thể là xóa tập tin nhật kí của ứng dụng hay hệ thống, xóa các chương trình đã được cài đặt, ẩn các tiến trình nguy hiểm.

Hacktivism Là Gì

Hacktivism là hành động tấn công vì một mục tiêu xã hội hay mang tính chất chính trị. Thông qua hành động tấn công của mình hacker sẽ đưa ra một thông điệp đến các cơ quan quản lý hay một tổ chức như tình huống *hacker* Việt Nam và *hacker* Trung Quốc tấn công vào các trang web của cơ quan quản lý của hai nước để đưa ra các thông tin về chủ quyền biển đảo Hoàng Sa – Trường Sa. Hay gần đây nhất là nhóm hacker Luzsec đã tấn công vào máy chủ của công ty bảo mật BKIS và yêu cầu tha bổng cho một hacker xâm nhập vào một trang web của cơ quan này nhằm đưa ra các cảnh báo bảo mật. Những hacker tấn công vì mục tiêu nhất định thường là một nhóm các hacker, hay đôi khi chỉ là cá nhân riêng lẽ nhưng đa phần các hành động này là sai trái và không hợp lệ. Hình 1.3 minh họa một hacktivism điển hình.



Hình 1.3 – Một thông điệp mà hacker để lại trên trang web bị tấn công

Các bạn cần lưu ý thuật ngữ *hacktivism* là một trong những chủ đề thường hay xuất hiện trong các câu hỏi của kì thi chứng chỉ CEH, vì vậy chúng ta cần đặc biệt lưu ý khái niệm trên với định nghĩa bằng tiếng Anh là *"Hactivism refers to hacking for a cause"*

Phân Loại Hacker

Chúng ta thường nghe gọi nhóm này là hacker mũ đen, nhóm khác là hacker mũ trắng hay những khái niệm tương tự khác. Vậy thì có tất cả bao nhiêu loại "mũ" mà những hacker có thể "đội" và ý nghĩa của chúng như thế nào? Sau đây chúng ta sẽ tìm hiểu về các khái niệm trên.

- **Black Hat** (Mũ đen)
    - Là những cá nhân hay nhóm hacker sử dụng kỹ năng và kiến thức của mình để xâm nhập trái phép và các hệ thống, thực hiện các hành vi phá hoại hay đánh cắp dữ liệu. Nhóm này còn được gọi là **'Cracker**' hay **'Attacker'**.
- **White Hat** (Mũ trắng)
    - Là các cá nhân có kỹ năng của một hacker và sử dụng chúng cho các mục đích bảo mật thông tin hay phòng chống hacker. Những chuyên viên kiểm định bảo mật *'Security Analyst'* hay các chuyên gia an toàn thông tin, *penetration tester* là những hacker thuộc nhóm này.
- **Gray Hat** (Mũ xám)
    - Là người hoạt động trong cả hai lĩnh vực của hacker mũ đen và hacker mũ trắng.

Ethical Hacker Và Attacker

Trong các dạng hacker thì hacker mũ đen hay *attacker* là nhóm nguy hiểm nhất.Và những hacker thuộc nhóm này được chia làm các dạng khác nhau tùy thuộc vào vị trí tiến hành tấn công hay công cụ mà họ sử dụng. Còn các ethical hacker được xem như những hacker thiện chí và họ là những chuyên gia bảo mật đích thực.

- **Ethical Hacker**

  Là các hacker thiện chí, sử dụng kiến thức và kỹ năng của mình phục vụ cho tiến trình bảo mật và an toàn thông tin, chỉ tiến hành tấn công hay xâm nhập vào một hệ thống khi được sự cho phép của chủ nhân hệ thống đó. Các phương pháp và kỹ thuật mà *ethical hacker* áp dụng cũng giống như cách thức mà các hacker mũ đen thực hiện.

- **Internal Attacker**

Đây là những kẻ tấn công từ bên trong hay hacker nội bộ, có thể là các nhân viên trong công ty, các cộng tác viên hay những người làm chung một tòa nhà, cao ốc văn phòng. Do có những thuận lợi về mặt vật lý nên những hacker thuộc nhóm này rất dễ đánh cắp thông tin của người dùng như email, mật khẩu hoặc đột nhập các máy chủ, máy trạm trên mạng.

- **Electronic Activist, Hacktivist**

  Thuật ngữ này chỉ những hành động phá hoại như thay thế nội dung của trang web hay cố tình thâm nhập trái phép vào hệ thống vật dẫn, đường truyền của công ty, tổ chức.

- **Data Thief**

  Những kẻ tấn công thuộc nhóm này chuyên đánh cắp những thông tin riêng tư của người dùng, ví dụ các *attacker* đánh cắp tài khỏan của game thủ bằng thủ đọan cài *keylogger* trên những máy tính ở các phòng game, internet. Để ngăn ngừa việc bị phát hiện, các *attacker* thuộc dạng *Data thief* thường tiến hành *cover track*, nghĩa là xóa các dấu vết được lưu trong tập tin nhật kí.

- **Script kiddie**

  Đa số các kẻ tấn công là *script kiddie*, họ là những người chỉ biết sử dụng các công cụ, đọan mã được xây dựng sẵn để tiến hành khai thác và tấn công những hệ thống bị lỗi mà không am hiểu về các chi tiết kỹ thuật. Nhóm này rất nguy hiểm vì mức độ hiểu biết của chúng luôn tỉ lệ nghịch với khả năng phá hoại.

- **Electronic Vandal**

  Các *attacker* thuộc nhóm này chỉ muốn phá hoại các dư liệu, hệ thống hay dịch vụ mà không cần một mục tiêu nào cả. Các hành động đôi khi chỉ để vui đùa, giải trí hoặc vì mục đích phô trương, trình diễn.

- **Cyberterrorist**

  Các attacker thuộc nhóm này có hành động giám sát, xem trộm những thông điệp cá nhân hay của tổ chức hơn là tiến hành đánh cắp hay thay đổi dữ liệu.

Hành Động Của Ethical Hacker

Ethical hacker hay hacker thiện chí đều có phương pháp thực hiện tương tự như những kẻ tấn công "thiếu thiện chí" nhưng mục tiêu của họ thì hoàn toàn khác. Ethical hacker tìm kiếm các điểm yếu bảo mật và xác định cách thức để thâm nhập vào mục tiêu nhằm đánh giá mức độ thiệt hại do các lổ hỗng này gây ra, từ đó đưa ra cảnh báo cùng những

phương án gia cố, kiện toàn bảo mật thích hợp. Tiến trình này thường được gọi là *penetration test* hay các cuộc tấn công thử nghiệm mà chúng ta đã trình bày ở trên. Công cụ hàng đầu hay được sử dụng để tiến hành *penetration test* các trang web *là Acunetix Web Vulnerability Scanner* với thông điệp quảng cáo mà ta thường thấy là **IS YOUR WEBSITE HACKABLE ?** như trong hình minh họa.

Ngoài mục tiêu thì một trong những điểm khác biệt quan trọng giữa *ethical hacker* và những hacker thông thường là hacker thiện chí chỉ hành động trên các hệ thống mà họ có thẩm quyền hay được sự cho phép, ủy quyền của người chủ hệ thống. Nhiều hacker tại Việt Nam nhầm lẫn về khái niệm này trong quá trình thi lấy chứng chỉ CEH cũng như hành động của họ trong việc tìm kiếm lỗi. Một số người đã chủ động dò lỗi của trang web, thâm nhập vào và sau đó gởi yêu cầu vá lỗi cho chủ nhân của hệ thống, đây là hành động không hợp lệ vì chưa có sự cho phép của chủ nhân thì bất kì sự xâm nhập nào cũng đều là trái phép. Tuy nhiên, nếu chỉ dừng lại ở hành động dò quét lỗi và gởi thông báo riêng về các lỗi được phát hiện thì hoàn toàn hợp lệ, ngoại trừ một số máy chủ hay dãy địa chỉ IP tuyệt mật như của NASA hay Bộ Quốc Phòng Mỹ thì ngay cả việc quét IP cũng không được phép.

Mục Tiêu Của Những Kẻ Tấn Công

An toàn thông tin bao gồm bốn yếu tố sau :

- Confidentiality
- Integrity
- Availability
- Authenticity

Mục tiêu của việc triển khai các giải pháp bảo mật, áp dụng chính sách an ninh là để bảo vệ bốn đặc tính cơ bản trên. Ngược lại, điều mà các kẻ tấn công nhắm tới là phá vỡ các yêu tố cơ bản này của thông tin. Khi một hacker tấn công theo hình thức nghe lén dữ liệu trên đường truyền để trộm mật khẩu của hộp thư điện tử hay tài khoản ftp thì lúc này họ đang phá vỡ tính riêng tư, bí mật của dữ liệu. Đặc tính này được gọi là *Confidentiality*.

Còn trong trường hợp hacker đánh cướp *session* (trình bày trong **Module 11 Session Hijacking**) để chiếm phiên làm việc đã qua xác thực của người dùng thi họ đang tấn công và cơ chế xác thực của hệ thống, đây chính là cơ chế *Authenticity*. Một tình huống thông dụng khác tấn công vào cơ chế xác thực là giả mạo địa chỉ MAC của thiết bị mạng còn được gọi là *MAC address spoofing*, dạng tấn công này sẽ vượt qua cơ chế kiểm soát

của các *router* hay hệ thống kiểm soát truy cập trên mạng không dây dựa trên địa chỉ vật lý thông qua phương pháp giả mạo địa chỉ MAC của một máy tính hợp lệ.

Vậy khi nào các hacker sẽ làm mất tính sẵn sàng hay *Availability* của dữ liệu và dịch vụ ? Ví dụ một trang web cung cấp thông tin hay dịch vụ cho người dùng bị tấn công từ chối dịch vụ bằng cách gởi một số lượng rất lớn những yêu cầu kết nối, làm cho hệ thống không thể đáp ứng các yêu cầu truy cập khác thì tính sẵn sàng hay khả dụng của trang web đã bị vô hiệu.

Trong trường hợp dữ liệu truyền sau khi bị chặn bắt sẽ được thay đổi và gởi về cho các máy tính client hay server như giả mạo chứng chỉ điện tử (*fake certificate*) thì hacker đang tác động vào tính toàn vẹn hay *Integrity* của thông tin. Hoặc hình thức tấn công *Bit-flipping* còn được gọi là *integrity attack,* chuyên chặn các dữ liệu truyền hay thông tin trên máy tính và thay đổi nội dung làm cho quản trị viên không thể xác nhận được dữ liệu đúng như mục tiêu của người gởi. Một ví dụ của tấn công *Bit-flippin*g là đánh vào cơ chế mã hóa cipher (mã hóa theo dòng) làm thay đổi *ciphertext* mặc dù hacker không hề hay biết plaintext là gì (plaintext là dữ liệu gốc, dữ liệu này sau khi được áp dụng một thuật toán mã hóa sẽ cho ra ciphertext, các khái niệm này sẽ được trình bày trong **Module 18 Cryptography**). Với dạng tấn công này hacker có thể thay đổi nội dung thông điệp từ "Tôi nợ anh 10.000.000 VND " thành "Tôi nợ anh 1.000.000 VND"

> *Các bạn lưu ý, bốn yếu tố nên tảng này thường xuyên xuất hiện trong các câu hỏi trắc nghiệm của bài thi lấy chứng chỉ CEH. Ví dụ như các bạn hãy xác định các chữ CIA là viết tắt của những từ nào trong danh sách Confidentiality, Authenticity, Integrity và Availability. Đáp án sẽ là* ***Confidentiality***, ***Integrity*** *và* ***Availability*** *với các mô tả chi tiết sau đây :*
>
> *C: Confidentiality là đặc tính riêng tư, bí mật của thông tin. Một trong những mục tiêu quan trọng nhất của bảo mật thông tin là bảo đảm sự riêng tư của dữ liệu. Điều này có nghĩa là dữ liệu hay thông tin của người nào thì chỉ người đó được biết và những người khác không được quyền can thiệp vào. Trong thực tế, chúng ta thường thấy khi phát lương ngoài bì thư hay đề chữ* ***Confidentiality*** *nhằm không cho các nhân viên biết mức lương của nhau để tránh sự đố kỵ, so sánh giữa họ. Hoặc trong những khu vực riêng của một cơ quan hay tổ chức nhằm ngăn chặn người lạ xâm nhập với bảng cấm "không phận sự miễn vào" cũng là một hình thức bảo vệ tính riêng tư. Đối với dữ liệu truyền để bảo vệ tính riêng tư thì chúng thường được mã hóa hay sử dụng các giao thức truyền thông an tòan như SSH.*
>
> *I: Integrity là tính tòan vẹn của dữ liệu. Mục tiêu tiếp theo trong bảo mật thông tin là bảo vệ tính tòan vẹn cho dữ liệu. Nhằm bảo đảm khi dữ liệu truyền đi không bị thay đổi bởi một tác nhân khác, ví dụ khi một email quan trọng được gởi đi thì thường được áp dụng các thuật tóan bảo vệ tính tòan vẹn như message digest (sẽ tham khảo trong Module 18) ngăn ngừa bị một tác nhân thứ ba thay đổi bằng cách chặn bắt thông điệp trên.*

A: Availability là tính khả dụng và sẵn sàng đáp ứng nhu cầu người dùng của thông tin, dịch vụ. Nghĩa là dữ liệu cần phải luôn luôn đáp ứng được nhu cầu của người dùng ví dụ như dịch vụ email của doanh nghiệp phải luôn luôn có khả năng phục vụ nhu cầu gởi và nhận email, nếu do sự cố nào đó mà quá trình trao đổi thông tin qua email không diễn ra được thì hệ thống bảo mật của chúng ta đã bị gãy đổ do đã đánh mất khả năng đáp ứng nhu cầu của người dùng.

An Toàn Thông Tin, Chức Năng Của Người Dùng Và Tính Tiện Dụng

Ba đặc trưng này tạo nên một tam giác bảo mật mà bất kì chuyên gia an ninh thông tin nào cũng phải cân nhắc khi áp dụng các quy tắt và giải pháp an toàn cho hệ thống của mình. Trong vai trò quản trị hệ thống hay một người phụ trách về bảo mật thông tin chúng ta đều muốn thắt chặt chính sách an ninh, triển khai những hệ thống bảo vệ mạnh mẽ, chặt chẽ nhất để ngăn ngừa sự tấn công của hacker, hay tiến trình lây lan của virus.

Nhưng điều này có thể làm hạn chế chức năng sử dụng của người dùng, và gây khó khăn cho họ trong nhiều thao tác. Ví dụ trong vài trò quản trị hệ thống mạng cho một tập đoàn trước đây tôi đã triển khai hệ thống tường lữa trên nền ISA Server Firewall ngăn tải về những tập tin *exe* để phòng bị nhiễm virus, nhưng điều này đã gây khó khăn cho bộ phận kỹ thuật vì họ cần cài đặt nhiều công cụ và ứng dụng cho các phòng lab, và rất nhiều chương trình này được tải về từ internet. Để khắc phục tình trạng trên, tôi phải tạo thêm một ngoại lệ cho nhóm *Technical Support* mặc dù điều đó có thể tạo ra một khe hở cho sự lây nhiễm mã độc hại. Ở một tình huống khác, khi áp dụng chính sách bảo mật cao nhất cho toàn vùng được quản trị bởi *Domain Controller*, yêu cầu người dùng đặt mật khẩu bắt buộc phải có sự kết hợp của kí tự đặc biệt, chữ hoa, chữ thường kèm theo đó là độ dài trên 16 kí tự đã làm cho họ gặp khó khăn ngay từ khâu đặt mật khẩu.

Vì vậy, khi triển khai một giải pháp an toàn thông tin cho tổ chức các bạn cần lưu ý đến nhũng chức năng sẽ bị hạn chế của người dùng, các ảnh hưởng đến tính tiện lợi trong quá trình sử dụng để có biện pháp xử lý đem đến sự cân bằng, ổn định cho toàn bộ hệ thống. Để khắc phục các tình trạng trên thì chúng ta nên có những chương trình đào tạo thích hợp nâng cao nhận thức cho người sử dụng trong vấn đề bảo mật thông tin, kèm theo đó là các biện pháp chế tài thích hợp nhằm ngăn ngừa việc sử dụng tài nguyên không hợp lệ.

Những Kỹ Năng Cần Thiết Để Trở Thành Ethical Hacker

Để trở thành một *ethical hacker* các bạn cần có những kỹ năng của một hacker mũ đen đó là kiến thức về hệ thống mạng và máy tính, có khả năng quản trị và hiểu rõ hệ thống Windows , Linux. Chúng ta cần nắm vững cách khai thác một lổ hổng bảo mật và phương pháp khắc phục sự cố vì mục tiêu của chúng ta là "tấn công để phòng thủ" chứ không phải "tấn công để phá hoại". Ngoài ra, để có thể hiểu rõ các mã khai thác, hay biên soạn các công cụ, kịch bản dùng cho việc thử nghiệm thì *ethical hacker* nên có kiến thức

về lập trình, mặc dù các hacker ngày nay có nhiều công cụ hỗ trợ viết các đoạn mã hiểm độc một cách dễ dàng như sử dụng công cụ tạo kịch bản Auto IT hay những chương trình chuyên dụng để tạo ra *trojan, virus, worm*.

Bên cạnh những kiến thức và kỹ năng đã trình bày thì những hacker thiện chí cần có chứng chỉ CEH, đây là chứng nhận rõ ràng và hợp lệ nhất dành cho một ethical hacker.

Tìm Kiếm Các Lổ Hỗng Bảo Mật

Một trong các công đoạn quan trọng của quá trình tấn công mà các hacker mũ đen và mũ trắng cần phải tiến hành là tìm kiếm các lổ hỗng bảo mật để qua đó có thể xâm nhập vào hệ thống. Những công cụ thường dùng trong quá trình này như là MBSA chuyên tìm kiếm các thiếu sót trong việc cài đặt các bản vá lỗi hay bản cập nhật hệ thống dành cho các ứng dụng và hệ điều hành của Microsoft hay công cụ Nessus có khả năng tìm kiếm lổ hỗng bảo mật của cả hệ điều hành Windows và Linux, Mac hoặc những thiết bị phần cứng như bộ định tuyến Cisco. Ngoài ra, đối với các ứng dụng đặc biệt như trang web còn có những công cụ dành riêng cho việc tìm kiếm lỗi đó là W3AF hay Acunetix Web Vulnerability Scanner.

Trong vai trò của một ethical hacker chúng ta cần nắm rõ chức năng và cách thức sử dụng của những công cụ tìm kiếm lỗi bảo mật hàng đầu để có thể phát hiện lỗi, đưa ra giải pháp khắc phục hay hạn chế những tác hại do các rũi ro về an toàn thông tin mang lại.

Quy Trình Tấn Công Thử Nghiệm

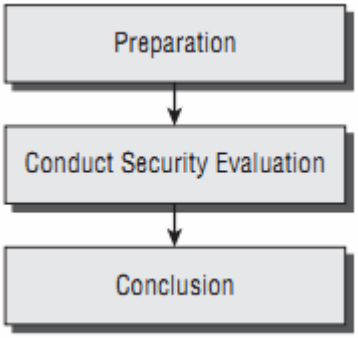
Khác với hacker thông thường những ethical hacker tấn công hệ thống để đánh giá tính bảo mật thông tin. Vì vậy khi thực hiện công việc *penetration test* hay *security audit* phải tuân theo quy trình chặt chẽ, cần chú ý điến tác động mà việc thử nghiệm tấn công. Khi thực hiện công việc các ethical cần đặc biệt chú ý nhu cầu và ý kiến của người sử dụng.

Sau đây là các bước hướng dẫn trong quá trình kiểm định bảo mật hệ thống :

1. Trao đổi với client (người sử dụng cuối) để thảo luận về tính cần thiết của việc thử nghiệm và biện pháp xử lý sự cố có thể gặp trong quá trình thực hiện.
2. Chuẩn bị văn bản lấy chữ kí xác nhận của người dùng gọi là *nondisclosure agreement* (NDA) trước khi thực hiện công việc nhằm bảo đảm tính hợp lệ của việc tấn.
3. Thành lập nhóm làm việc gồm các ethical hacker và lên kế hoạch thực hiện với thời gian cụ thể.
4. Thực hiện kiểm định theo quy trình đề ra.
5. Phân tích kết quả của quá trình kiểm tra và chuẩn bị báo cáo.
6. Trình bày báo cáo với khách hàng.

Tạo Bản Kế Hoạch Đánh Giá Bảo Mật

Như đã trình bày, đa số ethical hacker hoạt động như các chuyên gia bảo mật đó là tiến hành kiểm định hệ thống, đánh giá rũi ro, thử nghiệm tấn nên khi thực hiện công việc cần phải được tiến hành khoa học theo ba bước Preparation (chuẩn bị), Conduct (xây dựng quy trình) và Conclusion (thảo luận) như hình 1.4



Hình 1.4 – Các giai đoạn trong quá trình kiểm định bảo mật

- **Preparation** – Đây là giai đoạn chuẩn bị, trong bước này các bản hợp đồng sẽ được kí kết nhằm bảo vệ chính bản thân các Ethical Hacker khi có những rắc rối xảy ra ví dụ như vi phạm vào các điều luật an tòan thông tin, ngòai ra bản hợp đồng còn quy định những phạm vi hay tài nguyên mà Ethical hacker được quyền khảo sát và tấn công thử nghiệm.

- **Conduct** – Trong giai đọan này các bản kế hoạch về quá trình khảo sát, báo cáo mang tính chất kỹ thuật sẽ được trình bày và tiến hành quá trình ethical hacking.

- **Conclusion** – Cuối cùng là những kết luận về tình trạng an toàn của hệ thống, các lỗi bảo mật nào có thể bị khai thác và giải pháp khắc phục như thế nào….

Các Kiểu Tấn Công Của Ethical Hacker

Ethical hacker có thể sử dụng nhiều phương pháp khác nhau để đánh giá tính an toàn của hệ thống thông qua việc tấn công thử nghiệm, những phương pháp này bao gồm :

- **Remote network** – Giả lập các cuộc tấn công từ xa hay từ hệ thống internet.

- **Remote dial-up network** – Tiến hành các cuộc tấn công vào hệ thống modem hay các kết nối dial-up của hệ thống như máy chủ VPN .

- **Local network** – Giả làm nhân viên của tổ chức và thực hiện các cuộc tấn công lên các tài nguyên để tìm ra các điểm sơ hở trong chính sách bảo mật hay điểm nhạy cảm của hệ thống.

- **Stolen equipment** – Giả lập mộttình huống đánh cắp tài nguyên để dự đóan các thiệt hại và tác động của nó lên quá trình kinh doanh. Đã có tình huống một sân bay của Úc bị hacker giả làm nhân viên bảo trì đánh cắp ổ cứng làm hệ thống điều khiển và vận hành bị tâ liệt trong vòng 2 giờ.

- **Social engineering** – Quá trình này dùng để kiểm tra sự hiểu biết của người dùng và các kiến thức về an tòan thông tin, phòng chống bị các đối tượng xấu giả mạo, đánh lừa nhằm lất cắp thông tin quan trọng.

- **Physical entry** – Trong mô hình này các ethical hacker sẽ tiến hành tấnc ông trực tiếp và cáo thành phần vật lý của hệ thống như các máy chủ, hệ thống lưu điện v.v nhằm kiểm tra xem các tài nguyênnày có được đặt dưới sự bảo vệ tốt hay không.

Các Mô Hình Thử Nghiệm Tấn Công

Có hai mô hình thử nghiệm tấn công hay *penetratiom test* (gọi tắt là *pentest*) là **black box** tương ứng với tình huống tấn công hay *pentest* từ bên ngoài hệ thống. Ngược lại khi ethical hacker tiến hành tấn công mạng máy tính từ vị trí bên trong của tổ chức sẽ được gọi là **white box**.

Ethical Hacking Report

Kết quả của tiến trình *penetration test* hay kiểm điểm anh toàn thông tin được gọi là *ethical hacking report*, bản báo cáo này bao gồm thông tin chi tiết các hoạt động tấn công thử nghiệm, mô hình tấn công và các phương pháp đã sử dụng, nội dung được so sánh tương ứng với từng giai đoạn trong *Conduct Security Evaluation*. Trong bản báo cáo này các lổ hỗng cần được mô tả chi tiết kèm theo những hướng dẫn hay khuyến nghị về phương pháp phòng chống. Do tính chất quan trọng nên những bản báo cáo quá trình tấn công thử nghiệm cần được gởi bằng định dạng *hard-copy* nhằm bảo đảm an toàn.

Thông tin lỗi kèm theo phải được giữ bí mật nhằm tránh bị kẻ xấu lợi dụng tấn công, khai thác nếu không những tài liệu này sẽ trở nên phản tác dụng.

Hiểu Rõ Tính Hợp Lệ Của Việc Tấn Công

Là một hacker thiện chí chúng ta cần nắm rõ những vấn đề liên quan đến luật định và tính hợp pháp của quá trình tấn công. Bất kì hành động tấn công thử nghiệm, kiểm định bảo mật hay *penetration test* nào cũng cần có sự xác nhận và đồng ý của đơn vị chủ quản bằng các văn bản hay công văn. Những ethical hacker cần phải biết rõ các hình phạt được quy định bởi luật pháp tại nơi mình cư trú của hành vi tấn công trái phép, thận trọng khi ứng dụng kỹ năng trong quá trình tấn công, cũng như nhận thức đầy đủ về hậu quả nếu như áp dụng các phương pháp không đúng đắn.

Có hai bộ luật của Mỹ liên quan đến tội phạm máy tính mà chúng ta cần phải quan tâm là 18 U.S.C. § 1029 Federal Law và 18 U.S.C. § 1030 U.S. Federal Law. Mặc dù CEH là một chứng chỉ quốc tế nhưng việc nắm rõ hai bộ luật này là điều cần thiết để thi đạt chứng chỉ trên. Các bạn cần lưu ý là ngay cả những ethical hacker cũng có thể bị khởi kiện nếu vi phạm các điều luật này.

Để giải quyết các khe hở của luật pháp đối với tội phạm công nghệ cao các nhà làm luật của Mỹ đã xây dựng bộ luật ***Cyber Security Enhancement Act of 2002*** quy định các hình phạt dành cho các kẻ tấn công tương ứng với bất kì hành động phá hoại, xâm phạm thông tin trái phép.

U.S Code hay *Code of Laws of the United States* là bộ luật của Mỹ bao gồm 51 chương, tại chương 18 (Title 18) về "*Crimes and Criminal Procedure*.", điều 1029 là "*Fraud and related activity in connection with access devices,*" quy định rõ những việc sử dụng trái phép các tài sản bao gồm thiết bị, vật dụng trong lĩnh vực truyền thông có giá trị trên *1000 USD* là vi phạm pháp luật.

Trong điều 1030 "*Fraud and related activity in connection with computers*," ngăn cấm việc truy cập trái phép vào các máy tính hay có những hành động gây thiệt hai về thông tin. Bao gồm cả các hành động phát tán và lan truyền virus hay xâm nhập bất hợp pháp máy tính cá nhân.

Riêng tại Việt Nam, từ điều 67 đến điều 72 quy định về luật công nghệ thông tin như

> Điều 67. Trách nhiệm bảo vệ quyền, lợi ích hợp pháp của người sử dụng sản phẩm, dịch vụ công nghệ thông tin
>
> Điều 68. Bảo vệ tên miền quốc gia Việt Nam ".vn"
>
> Điều 69. Bảo vệ quyền sở hữu trí tuệ trong lĩnh vực công nghệ thông tin
>
> Điều 70. Chống thư rác
>
> Điều 71. Chống vi rút máy tính và phần mềm gây hại
>
> Điều 72. Bảo đảm an toàn, bí mật thông tin

Kết Luận

Qua phần đầu tiên của giáo trình chúng ta đã nắm được những khái niệm quan trọng như *threat, exploit, attack* và phân biệt sự khác nhau giữa ethical hacker và hacker thông thường. Bên cạnh đó, các bạn đã nắm về quy trình *penetration test* cùng với những vấn đề liên quan đến luật pháp. Trong các chương tiếp theo chúng ta sẽ thảo luận về tiến trình tấn công của hacker và những kỹ thuật tấn công chi tiết.