Bài: 1.3 Giới thiệu về Ethical Hacking - Khái niệm hack, phân loại và các giai đoạn

Xem bài học trên website để ủng hộ Kteam: 1.3 Giới thiệu về Ethical Hacking - Khái niệm hack, phân loại và các giai đoạn

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!

Khái niệm hack, phân loại và các giai đoạn

Tin tặc (Hacker)

Hacker là một kẻ đủ trí thông minh để có thể **ăn cắp thông tin** như dữ liệu công việc, dữ liệu cá nhân, thông tin tài chính, thông tin thẻ tín dụng, tên người dùng và mật khẩu từ những hệ thống hắn **không được cho phép**. Hắn sử dụng quyền kiểm soát không chính thức trên hệ thống đó bằng nhiều công cụ và công nghệ.

Hacker có kỹ năng tốt, có khả năng để phát triển những phần mềm, nhất là phần mềm "khám phá". Mục đích của hắn có thể vô pháp, có lúc vì hứng thú, có lúc vì được trả tiền để làm vậy.

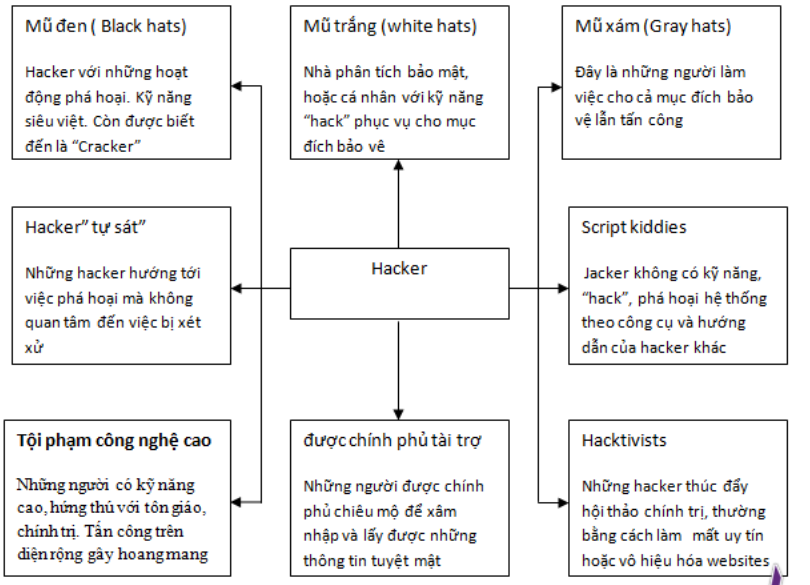

Figure 1-6 Types of Hacker

Hacking

"**Hacking**" trong lĩnh vực an toàn thông tin là từ để chỉ **sự khai thác điểm yếu** của một hệ thống, **phá hoại bức tường bảo mật** để **chiếm quyền kiểm soát**, **điều khiển tài nguyên** hệ thống. Mục đích của hack có thể bao gồm làm giảm đi tài nguyên trên hệ thống, phá vỡ đặc điểm và dịch vụ của hệ thống nhằm đạt được mong muốn. Hack cũng có thể được dùng để ăn cắp thông tin sử dụng cho nhiều mục đích khác như gửi đến những người tham gia, cá nhân giới hạn hoặc công khai những thông tin nhạy cảm.

Các công đoạn hack

1. Thăm dò (Reconnaissance)

1. Quét (Scanning)
2. Có được quyền truy cập (Gaining access)
3. Duy trì truy cập (Maintaining Access)
4. Xóa dấu vết (Clearing tracks)

Thăm dò

Đây là bước đầu chuẩn bị sẵn sàng của những kẻ tấn công bằng cách thu thập thông tin về mục tiêu trước khi bắt đầu tấn công bằng nhiều công nghệ và công cụ khác nhau. Ngay cả khi thông tin có quy mô lớn, việc thu thập thông tin về mục tiêu khiến cho âm mưu của kẻ tấn công sẽ dàng thành hiện thực hơn và hỗ trợ chúng xác định được phạm vi của mục tiêu

Trong việc **thăm dò bị động** (Passive Reconnaissance), hacker **có được thông tin về mục tiêu mà không cần tương tác trực tiếp** với mục tiêu. Có thể nêu ra một ví dụ về thăm dò bị động là thông qua tìm kiếm trên các phương tiện truyền thông cộng đồng để lấy được thông tin của mục tiêu.

Thăm dò chủ động (Active Reconnaissance) là việc **giành lấy thông tin từ mục tiêu một cách trực tiếp**. Ví dụ về thăm dò chủ động đó là qua cuộc gọi, qua emails, helpdesk hoặc cục công nghệ.

Quét

Trước công đoạn tấn công là công đoạn "**quét**" (**scanning**). Trong công đoạn này, kẻ tấn công quét hệ thống bằng những thông tin đã có trong quá trình ban đầu (thăm dò). Công cụ scan là Dialler, máy quét như Port scanners, Network mappers, công cụ máy chủ như ping, hoặc thậm chí là những máy quét điểm yếu. Khi công đoạn này diễn ra, kẻ tấn công lấy được thông tin của cổng giao tiếp (port) bao gồm trạng thái, thông tin về cách vận hành của thiết bị, loại máy móc, và nhiều thông tin khác.

Đạt được quyền truy cập

Đây là công đoạn khi hacker chiếm được quyền kiểm soát một hệ thống, một thiết bị hoặc mạng máy tính. Quyền kiểm soát này định rõ mức độ truy cập của hệ thống vận hành, của thiết bị, của mạng máy tính.

Để có được quyền truy cập trái phép, kẻ tấn công dùng các công nghệ như phá mật khẩu, từ chối dịch vụ, chiếm quyền sử dụng trong phiên làm việc của người dùng, sử dụng mã khai thác lỗi tràn bộ nhớ đệm và nhiều thứ khác được sử dụng. Sau khi truy cập hệ thống, kẻ tấn công sẽ làm cho quyền ưu tiên của mình leo thang để kiểm soát hoàn toàn các dịch vụ, các quá trình và phá hoại hệ thống kết nối tức thời.

Duy trì truy cập/ leo thang quyền lợi

Quá trình duy trì truy cập là khi một kẻ tấn công **cố gắng duy trì việc xâm nhập, điều khiển hệ thống đã bị phá hoại**. Tương tự, hắn cố gắng ngăn quyền sở hữu của mình rơi vào tay hacker khác. Bằng cách sử dụng **Backdoor**, **rootkits** hoặc **trojans** để cầm giữ quyền làm chủ.

Một kẻ tấn công có thể ăn cắp thông tin qua việc đăng tải thông tin lên các hệ thống từ máy chủ ở xa, tải xuống bất cứ tệp tin nào của hệ thống, điều khiển dữ liệu và nhận dạng. Dùng chính hệ thống bị phá hoại, kẻ tấn công sẽ tiếp tục bắt đầu tấn công những hệ thống khác.

Xóa dấu vết

Kẻ tấn công phải giấu đi nhận dạng của mình bằng việc che đậy dấu vết. **Che đậy dấu vết** là những hành vi kẻ tấn công thực hiện nhằm che giấu các hành vi phá hoại của mình. đối với một kẻ tấn công, đây là công đoạn cần thiết nhất để đạt được ý định của hắn. Bằng cách tiếp tục xâm nhập vào hệ thống đã bị làm hư hại, giữ cho bản không bị phát hiện và đoạt được điều hắn muốn mà không để lại bất kỳ bằng chứng nào có thể tố cáo hắn. Để điều khiển những dấu hiệu và chứng cứ, hắn sẽ chép đè lên hệ thống, lên thiết bị cùng những khóa log liên quan khác để tránh bị nghi ngờ.