Bài: 1.2 Giới thiệu về Ethical Hacking - Information Security Threats và Attack Vectors

Xem bài học trên website để ủng hộ Kteam: 1.2 Giới thiệu về Ethical Hacking - Information Security Threats và Attack Vectors

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!

Information Security Threats và Attack Vectors

Động cơ, mục đích, mục tiêu của những cuộc tấn công bảo mật

Trong thế giới của bảo mật thông tin, một **kẻ tấn công** (**attacker**) tấn công mục tiêu theo ba phần. "**động cơ hoặc mục tiêu**" (**Motive or Objective**) khiến cho kẻ tấn công tập trung vào tấn công một hệ thống riêng biệt. một thành phần khác được kẻ tấn công sử dụng phổ biến đó là **Phương pháp** (**Method**) nhằm có được quyền truy cập vào hệ thống đích. Ý định của kẻ tấn công cũng được các điểm yếu của hệ thống làm cho thành hiện thực. Ba thành phần đã nêu là những " viên gạch " chính mà một cuộc tấn công cần.

Động cơ và **mục tiêu** (Motive and Objective) của cuộc tấn công vào một hệ thống có thể phụ thuộc vào thứ có giá trị bên trong hệ thống đặc thù đó. Lý do vì sao thì có thể là do "đạo đức" hoặc cũng có thể là do "vô đạo đức". Tuy nhiên, điều dẫn tới nhiều mối hiểm nguy cho hệ thống, đó là **tin tặc** (**hacker**) cần phải có mục tiêu để đạt được. Một vài động cơ đặc trưng đứng sau các cuộc tấn công là nhằm đánh cắp thông tin, lôi kéo dữ liệu, chia rẽ, truyền bá tư tưởng chính trị hoặc tôn giáo, tổn hại đến danh tiếng của mục tiêu hoặc trả thù. Cách thức tấn công và những điểm yếu thì thường đi bên cạnh nhau. kẻ xâm nhập áp dụng hàng tá công cụ, hàng đống công nghệ - từ công nghệ cũ kỹ tới công nghệ hiện đại để khai thác điểm yếu trong hệ thống hoặc điều lệ bảo mật để tạo ra các lỗ hổng và hiện thực hóa mục đích của mình.

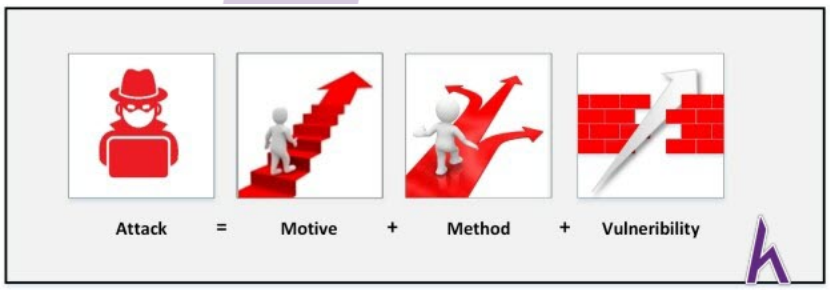

Figure 1-3 Information Security Attack

Những cuộc tấn công thông tin lừa đảo hàng đầu

Mối đe dọa điện toán đám mây

Điện toán đám mây là xu hướng phổ biến nhất được sử dụng ngày nay. điều đó không có nghĩa là mối nguy hiểm đe dọa điện toán đám mây hoặc bảo mật đám mây bớt hơn. Phần lớn những vấn đề tương tự tồn tại trong môi trường máy chủ truyền thống cũng tồn tại trong điện toán đám mây. Có thể thấy, bảo vệ an toàn cho điện toán đám mây để bảo vệ dịch vụ và dữ liệu là vô cùng quan trọng.

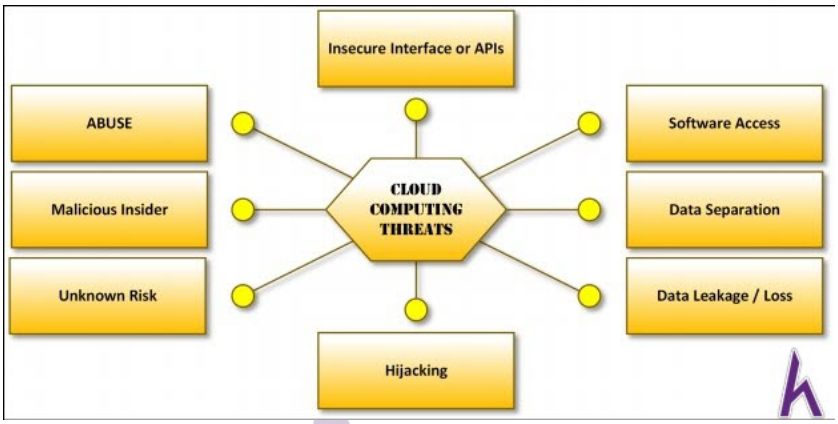

Figure 1-4 Cloud Computing Threats

Dưới đây là một số **mối hiểm nguy tồn tại** trong điện toán đám mây:

- Trong môi trường của điện toán đám mây, một mối nguy hiểm phổ biến đe dọa bảo mật là một **lỗ hổng dữ liệu** nhỏ bé cũng có thể **gây ra thất thoát dữ liệu**. Thêm vào đó, lỗ hổng đó khiến tin tặc có được những quyền truy cập xa hơn để truy cập được những bản ghi cho phép chúng có quyền tiến vào nhiều bản ghi vượt quá đám mây. Trong trường hợp xấu nhất, chúng làm tổn hại chỉ một đối tượng, dẫn tới cả một chuỗi những bản ghi bị hư hại.
- **Thất thoát dữ liệu** là một trong những mối nguy hiểm phổ biến tiềm tàng khiến cho an ninh đám mây bị tổn thương. Nguyên nhân có thể bắt nguồn từ nguyên nhân vô tình hoặc cố ý. Có thể là khối lượng nhỏ, cũng có thể là khối lượng lớn, tuy nhiên, việc mất một lượng dữ liệu lớn là một điều cực kỳ tồi tệ và tất nhiên, vô cùng tốn kém.
- Một mối đe dọa đến điện toán đám mây phổ biến khác đó là **chiếm quyền kiểm soát** của tài khoản qua đám mây và các loại dịch vụ. Thiết bị vận hành trong đám mây sở hữu phần mềm: **flaws** (thiếu sót), **weak encrypt** (mã hóa yếu ớt), **loopholes** (lỗ hổng lách luật) và những điểm yếu cho những kẻ xâm nhập kiểm soát.

Ngoài ra, còn có hàng tá mối đe dọa khác đến điện toán đám mây:

- **APIs** (**A**pplication **P**rogramming **I**nterface) không được bảo mật.
- Dịch vụ bị từ chối
- Nội bộ độc hại
- Bảo mật kém
- Nhiều khách hàng

Advanced Persistent Threats

APT là quá trình ăn cắp thông tin qua quá trình kéo dài liên tục. Thông thường, APT tập trung vào các tổ chức tư nhân hoặc các động cơ chính trị. Quá trình của APT phụ thuộc vào các công nghệ vừa phức tạp vừa hiện đại nhằm khai thác điểm yếu trong một hệ thống. Từ "**persistent**" biểu thị quá trình của việc ra lệnh từ phía bên ngoài và điều khiển hệ thống. Trong quá trình đó, dữ liệu từ một mục tiêu được giám sát và thu thập về liên tục. Quá trình "**threat**" chỉ những kẻ tấn công với mục đích phá hoại, làm tổn hại.

Ta có thể nêu ra các đặc điểm của APT, đó là:

Đặc điểm	Mô tả
Mục tiêu (objectives)	Động cơ hoặc đích đến của mối đe dọa
Tính chất đúng lúc (Timeliness)	thời gian thăm dò và xâm nhập mục tiêu
Tài nguyên	Mức độ hiểu biết và công cụ
Chịu rủi ro	Sự chịu đựng để không bị phát hiện
Kỹ năng và cách thức	Công cụ và công nghệ được sử dụng trong trường hợp
Hành động	Tính chuẩn xác hoạt động đe dọa
điểm bắt đầu tấn công	Số điểm bắt đầu
Những con số liên quan	Bao gồm những con số trong và ngoài hệ thống
Nguồn hiểu biết	Nhận thức những thông tin liên quan tới mối đe dọa

Viruses và Worms (bọ)

"**Virus**" trong bảo mật mạng và thông tin dùng để mô tả phần mềm độc hại. Phần mềm này được phát triển để tự mình phát tán, tái tạo và bám vào các file (Tệp tin) khác. Khi đã bám được vào các file đó, chúng sẽ truyền dẫn qua các hệ thống khác. Những "virus này cần người sử dụng tương tác với để gây ra và bắt đầu các hoạt động độc hại trên **hệ thống chúng cư trú** (resident System)

Khác với Virus, "**worm**" có khả năng tự tái tạo mình. Khả năng này giúp cho hoạt động phát tán của chúng diễn ra trên resident system một cách cực kỳ nhanh chóng. Chúng sinh sôi, phát triển ở nhiều dạng khác nhau từ những năm 1980. Sự xuất hiện của một vài loại "**worm**" mang tính chất tàn phá nguy hiểm, gây ra cuộc tấn công khiến DoS lụi tàn.

Mobile Threats (Mối nguy hiểm di động)

Với sự xuất hiện của công nghệ điện thoại di động, đặc biệt là điện thoại thông minh (Smartphone) đã làm tăng sự tập trung của những kẻ tấn công lên các thiết bị di động. Bởi điện thoại thông minh được sử dụng rộng rãi trên toàn cầu, những kẻ tấn công đã chuyển sự chú ý của mình qua đánh cắp công việc và thông tin qua các thiết bị di động. Những mối đe dọa phổ biến đối với thiết bị di động là:

- Rò rỉ dữ liệu (Data leakage)
- Mạng wifi không an toàn (Unsecured wifi)
- Lừa đảo mạng (Network Spoofing)
- Tấn công " phishing " (Phishing Attack)
- Phần mềm gián điệp (Spyware)
- Mật mã bị hỏng (Broken Cryptography)
- Thời kỳ chỉnh lý không phù hợp (Improper Session Handling)

Insider Attack (Tấn công nội bộ)

Một cuộc **tấn công nội bộ** là một loại tấn công diễn ra trên một hệ thống, trong phạm vi một tổ hợp mạng và được thực hiện bởi một người đáng tin cậy. Người dùng đáng tin cậy được hiểu như là **Insider** (nội bộ), có quyền ưu tiền và được ủy quyền để truy cập vào tài nguyên mạng.

Figure 1-5 Insider Threats

Botnets

Sự kết hợp chức năng của Robot với mạng máy tính phát triển một "**Botnet**" liên tục thực hiện lặp đi lặp lại một nhiệm vụ. Đó chính là nền tảng cơ bản của một "bot". Ta biết đến "bot" như những **con ngựa thồ** (work-horse) của Internet. Như đã nói, "bot" thực hiện những tác vụ lặp đi lặp lại. Thông thường, Botnet được kết nối với **Internet Relay Chat** (chat chuyển tiếp) . Những loại botnet này là hợp pháp và mang lại lợi ích.

Một botnet có thể được sử dụng cho những mục đích tốt đẹp nhưng cũng có những botnet được tạo ra trái phép với mục đích gây hại. Những botnet xấu này có khả năng **chiếm được quyền truy cập** vào hệ thống bằng cách **sử dụng những script và code độc hại hoặc bằng cách trực tiếp "hack" hệ thống** hoặc qua " Spider". Chương trình Spider luồn lách qua internet và tìm kiếm những lỗ hổng bảo mật. Bots phơi bày hệ thống trên trang web của hacker bằng cách liên lạc mới máy chủ. Máy chủ được cảnh báo khi hệ thống bị nắm quyền điều khiển. Những kẻ tấn công điều khiển tất cả những bot từ xa qua máy chủ.

Phân loại các mối đe dọa bảo mật an toàn thông tin

Các mối đe dọa đến việc bảo mật thông tin được nêu dưới đây:

Network Threats (Đe dọa mạng)

Những thành phần chính của cơ sở cấu trúc mạng là **đường truyền** (routes), **khóa** (switches) và **tường lửa** (firewalls). Những thiết bị này không chỉ thực hiện việc truyền dẫn và vận hành mạng, mà chúng còn điều khiển và bảo vệ những ứng dụng, những máy chủ đang hoạt động khỏi các cuộc tấn công hoặc xâm nhập. Thiết bị với cấu trúc càng nghèo nàn, những kẻ xâm nhập càng có cơ hội để khai thác. Điểm yếu thường thấy của mạng máy tính bao gồm thiếu cài đặt thiết lập, truy cập mạng "thoáng", mã hóa và mật khẩu yếu, thiết bị thiếu những bản vá bảo mật mới nhất. Những mối đe dọa mạng cao cấp nhất bao gồm:

- Thông tin tập trung (information gathering)
- "Đánh hơi" và nghe trộm (Sniffing & Eavesdropping)
- Lừa đảo, giả mạo (Spoofing)
- Chiếm quyền kiểm soát của một "session" (Session hijacking)
- Tấn công xen giữa (Man-in-the-middle attack)
- Nhiễm độc DNS & ARP (DNS & ARP poisoning)
- Tấn công Password-based (Password-based Attacks)
- Tấn công từ chối dịch vụ (Denial-of-Services Attacks)
- Tấn công phá mã khóa (Compromised Key Attacks)
- Tấn công tường lửa và IDS (Firewall&IDS Attacks)

Host Threats(Mối đe dọa đến host)

Host threats tập trung vào những phần mềm, ứng dụng hệ thống được cài đặt hoặc hoạt động vượt quá hệ thống đó như Window 2000, .NET Framework, SQL Server, và nhiều thứ khác. Những cấp độ nguy hiểm đến host bao gồm:

- Tấn công bằng phần mềm độc hại (Malware Attacks)

- Lần mò dấu vết (Footprinting)
- Tấn công mật khẩu (Password Attack)
- Tấn công từ chối dịch vụ (Denial-of-Services Attacks)
- Mã thực thi phá hoại (Arbitrary code execution)
- Truy cập không được phép (Unauthorized Access)
- Leo thang đặc quyền (Priviledge escalation)
- Tấn công "cửa sau" (Backdoor Attacks)
- Tấn công bảo mật vật lí (Physical Security Threats)

Application Threats (Mối đe dọa ứng dụng)

Để phân tích các mối đe dọa một các tốt nhất, ta phân chúng vào các loại tổn thương của ứng dụng:

- Dữ liệu không phù hợp / phê duyệt đầu vào (Improper Data/ Input Validation)
- Tấn công xác thực và ủy quyền (Authentication& Authorization Attack)
- Bảo mật bị mất định hình (Security Misconfiguration)
- Hỏng hóc bộ quản lý "session" (Broken Session Management)
- Lỗi tràn bộ nhớ đệm (Buffer Overflow issues)
- Tấn công mật mã (Cryptography Attacks)
- SQL injection
- Xử lý lỗi và quản lý trường hợp ngoại lệ không phù hợp (Improper error handling & exception Management)

Các dạng tấn công vào một hệ thống

Tấn công hệ thống vận hành

Trong tấn công hệ thống vận hành, những kẻ tấn công luôn tìm kiếm những điểm yếu của hệ thống vận hành. Nếu chúng tìm được bất cứ điểm yếu nào, chúng sẽ khai thác nó để tấn công hệ thống này. Có một vài điểm yếu thường thấy trong một hệ thống vận hành đó là:

- **Tràn bộ nhớ đệm** (Buffer Overflow vulnerabilities)

  Buffer Overflow là một loại tấn công hệ điều hành phổ biến có liên quan đến tấn công khai thác phần mềm. Trong buffer overflow, khi một ứng dụng hoặc một chương trình không được xác định rạch ròi ranh giới nhưsự hạn chế hay **khu vực chức năng trước khi được xác định** (pre-defined functional area) khả năng của dữ liệu để xử lý hoặc loại dữ liệu có thể được đưa vào. Buffer Overflow gây ra hàng loạt các vấn đề như **Từ chối dịch vụ** (Denial of Service – DOS), khởi động lại, những truy cập không giới hạn và đóng băng.

- **"Bugs" trong hệ điều hành**

  Trong tấn công khai thác phần mềm và "**bugs**" trong phần mềm, kẻ tấn công cố gắng khai thác những điểm yếu trong phần mềm. Điểm yếu này có thể là nhầm lẫn của nhà phát triển trong khi phát triển **mã chương trình** (program code). Những kẻ này có thể khám phá ra lỗi sai đó, sử dụng chúng để truy nhập vào hệ thống.

- **Hệ điều hành không bản vá** (Unpatched operating system)

  Unpatched Operating System cho phép thực thi các hoạt động độc hại, hoặc hệ thống không thể hoàn toàn ngăn chặn những phương tiện độc hại xâm nhập vào. Những xâm nhập trái phép thành công nhằm phá hoại có thể gây nhiều ảnh hưởng tồi tệ đến những thông tin nhạy cảm, mất mát dữ liệu và cản trở việc vận hành bình thường.

Misconfiguration Attacks

Khi một thiết bị mới đang được cài đặt trên mạng nội bộ, **người quản lí** (Administrator) sẽ phải thay đổi cấu hình còn thiếu sót. Nếu thiết bị đó được để dưới dạng cấu hình còn thiếu sót, thiếu độ tin cậy khi sử dụng, bất cứ người dùng nào dù không có quyền truy cập vào thiết bị cũng chỉ cần kết nối mạng để truy cập vào.

Đó không phải là món hời đối với những đối tượng xâm nhập khi truy cập vào thiết bị bởi những lỗi cấu hình đã quá phổ biến, mật khẩu thì yếu và chẳng có điều lệ bảo mật nào khả dụng trên thiết bị có thiếu sót.

Application-Level Attacks (Tấn công Application-level)

Trước khi phát hành một ứng dụng, nhà phát hành phải chắc chắc, kiểm tra và xác nhận từ giới hạn của chính nó, từ giới hạn của nhà sáng chế hoặc nhà phát triển. Trong tấn công Application level Attack, một hacker có thể sử dụng:

- Tràn bộ nhớ đệm (Buffer overflow)
- Nội dung đang hoạt động (Active content)
- Lỗ hổng Cross-site script
- Từ chối dịch vụ (Denial of service)
- SQL injection
- Chiếm quyền session (Session hijacking)
- Phishing

Shrink Wrap Code Attacks (Tấn công Shrink Wrap Code)

Tấn công bằng "**Shrink wrap code**" là loại tấn công mà hacker sử dụng để có quyền truy cập vào một hệ thống. Trong loại tấn công này, hacker khai thác những lỗ hổng trong hệ điều hành không có bản vá, có những thiết bị hoặc phần mềm được định hình kém. Muốn hiểu được tổn thương "shrink wrap", ta xem xét một hệ thống vận hành có lỗi bug trong phiên bản gốc của phần mềm. Người bán hàng có thể phát hành các bản cập nhật, nhưng trong khoảng thời gian giữa việc phát hành bản vá của anh ta cho tới khi hệ thống của khách hàng được cập nhật là khoảng thời gian then chốt nhất. Trong khoảng thời gian quyết định này, những hệ thống không có bản vá dễ bị tổn hại bởi tấn công Shrinkwrap. Tấn công Shrinkwrap còn bao gồm làm tổn thương đến hệ thống được cài đặt với phần mềm gắn với những trang kiểm tra và script sửa lỗi không an toàn. Nhà phát triển phải bắt buộc loại bỏ những script này trước khi phát hành.

Information Warfare(Chiến tranh thông tin)

Chiến tranh thông tin là một khái niệm của chiến tranh, bước vào cuộc chiến để có được những thông tin có giá trị nhất." **Information warfare**" hay "**Infor war**" mô tả cách sử dụng công nghệ thông tin và công nghệ giao tiếp (ICT). Lý do chủ yếu của chiến tranh thông tin là nhằm có được lợi ích để cạnh tranh với các đối thủ. Dưới đây, ta phân chiến tranh thông tin thành hai loại.

Defensive Information Warfare (Chiến tranh bảo vệ thông tin)

Đây là khái niệm được sử dụng để chỉ những hành động bảo vệ thông tin khỏi bị đánh cắp và hoạt động tình báo. **Defensive information warfare** bao gồm:

- Bảo vệ (Protection)
- Ngăn chặn (Deterrence)
- Chỉ ra và báo động (Indication&warning)
- Phát hiện (Detection)
- Chuẩn bị cho những trường hợp khẩn cấp (Emergency Preparedness)
- Phản hồi (Response)

Offensive Information Warfare (Chiến tranh tấn công thông tin)

Khái niệm này liên kết với quân đội. **Offensive warfare** là cuộc vận hành mang tính chất hung hãn được sử dụng để chống lại kẻ địch thay vì chờ đợi những kẻ tấn công bắt đầu cuộc chiến. Truy cập vào khu vực của chúng để chiếm đoạt thay vì mất đi lãnh địa của mình là khái niệm nền tảng của offensive warfare. Lợi ích chính của offensive warfare đó là nhận dạng đối thủ, những chiến lược của chúng và nhiều thông tin khác. **Offensive information warfare** ngăn chặn hoặc giảm bớt nguy cơ thông tin bị đem ra sử dụng theo nguyên tắc: **nguyên vẹn, sẵn sàng và tuyệt mật**.