Bài: 1.1 Giới thiệu về Ethical Hacking - Tổng quan về bảo mật dữ liệu

Xem bài học trên website để ủng hộ Kteam: 1.1 Giới thiệu về Ethical Hacking - Tổng quan về bảo mật dữ liệu

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!

Công nghệ tóm tắt

Tổng quan về bảo mật dữ liệu

Những phương thức, những quá trình bảo mật thông tin cùng với hệ thống thông tin khỏi những truy cập trái phép, rò rỉ thông tin, lạm dụng hoặc thay đổi. Việc bảo mật thông tin đảm bảo dữ liệu được an toàn, nguyên vẹn. Khi một tổ chức không có chính sách và điều luật bảo mật phù hợp – thông tin và dữ liệu mật liên quan đến cơ quan này rất có thể nằm trong vòng nguy hiểm vì thiếu biện pháp bảo vệ. lại nói về một tổ chức, với chính sách và thủ tục bảo mật rõ ràng chặt chẽ, tài sản quý giá của họ sẽ được bảo vệ khỏi truy cập bất hợp pháp, hay lạm dụng.

Trong thế giới hiện đại, hàng triệu người dùng tương tác với nhau mỗi giây phút dưới sự hỗ trợ của các công nghệ, các nền tảng mới nhất. Chỉ 60 giây, nhưng khoảng thời gian này có thể thật "yếu ớt" và, tiêu tốn rất nhiều tiền của đối với tổ chức tư nhân cũng như tổ chức cộng đồng bởi vì mối đe dọa đến từ hàng đống cách thức, từ cổ lỗ đến hiện đại trên toàn cầu. Hệ thống mạng công cộng là lựa chọn nhanh chóng và phổ biến nhất cho những kẻ muốn phát tán mối nguy hiểm ra toàn thế giới. Mã độc, nội dung độc hại, Viruses, Spams, và các lỗ hổng bảo mật luôn ở đâu đó, trực chờ rình rập bạn. Đó là lý do vì sao chúng ta không bao giờ có thể loại bỏ những biện pháp bảo mật mạng, bảo mật hệ thống.

Việc bổ sung những chính sách bảo mật hiệu quả thay cho những biện pháp bảo vệ vừa không cần thiết, vừa tốn tài nguyên lại gây ra những lỗ hổng tạo điều kiện cho những mối đe dọa luôn là thách thức đối với chúng ta. Có ba khái niệm cơ bản mà mục đích bảo mật của ta sẽ xoay quanh:

Data Breach

eBay Data Breach

eBay Data Breach là một trong những ví dụ thực tế thể hiện bảo mật thông tin và dữ liệu quan trọng như thế nào đối với doanh nghiệp. eBay là nền tảng mua bán đấu giá online nổi tiếng, được sử dụng rộng rãi khắp thế giới.Năm 2014, eBay tiết lộ lỗ hổng dữ liệu khổng lồ với những dữ liệu nhạy cảm. ước tính rằng, có dữ liệu của 145 triệu khách hàng đã bị đánh cắp trong cuộc tấn công này. Theo eBay, lỗ hổng dữ liệu đã làm tổn hại những thông tin đề cập dưới đây:

- Tên khách hàng
- Mật khẩu đã được mã hóa

- Địa chỉ bưu điện
- Số điện thoại liên lạc
- Ngày sinh

Những thông tin nhạy cảm này phải được trình bày ở dạng mã hóa mạnh mẽ. Thay vì được trình bày theo chữ cái thông thường, thông tin phải được viết dưới dạng mật mã. eBay quả quyết rằng những thông tin liên quan đến con số cần bảo mật như thông tin thẻ tín dụng không hề bị tổn hại, mặc dù việc đánh cắp nhận dạng cũng như mật khẩu cũng vô cùng nguy hiểm. Cơ sở dữ liệu của eBay bao gồm thông tin tài chính như thẻ tín dụng và nhiều thứ liên quan khác được yêu cầu phải được giữ trong định dạng riêng biệt dưới dạng mật mã.

Những hacker đã làm tổn thương một số lượng nhỏ nhân viên đáng tin cậy qua tấn công "phishing" giữa tháng hai và tháng ba năm 2014 để gây nên nguồn gốc lỗ hổng dữ liệu của eBay. Có lẽ những nhân viên chuyên biệt bị nhắm vào để truy cập vào hệ thống mạng của eBay hoặc có lẽ chính hệ thống mạng của eBay đã hoàn toàn bị giám sát, sau đó bị làm tổn thương. eBay khẳng định, họ đã phát hiện ra cuộc tấn công công nghệ cao (cyberattack) này trong vòng hai tuần

Google Play Hack

Hacker (tin tặc) người Thổ Nhĩ Kỳ, "Ibrahim Balic" đã " hack" Google Play hai lần. Hắn thừa nhận trách nhiệm của mình trong vụ tấn công Google Play. Nhưng đó không phải lần đầu tiên thử nghiệm của hắn. Hắn đứng sau vụ tấn công the Apple's Developer site. Qua thử nghiệm điểm yếu trong Google's Developer console và tìm được một thiếu sót trong hệ thống vận hành Android (Android Operating System), thứ hắn đã thử hai lần để chắc chắn khiến nó "sập" hết lần này đến lần khác.

Với kết quả của việc thử nghiệm điểm yếu, hắn phát triển một thiết bị android để khai thác chính điểm yếu này. Khi bảng điều khiển của nhà phát triển bị "sập", người dùng không thể tải xuống các ứng dụng, các thiết bị trong khi những nhà phát triển không thể đăng tải những ứng dụng, thiết bị của mình

The Home Depot Data Breach

Ngày nay, việc đánh cắp thông tin từ thẻ tín dụng đang trở nên phổ biến. Vào năm 2014, thiết bị bán hàng của Home Depot đã bị tấn công. Ngày 8 tháng 9 năm 2014, một thông báo từ Home Depot đã được phát đi, thừa nhận rằng hệ thống của họ đã xuất hiện lỗ hổng.

Những kẻ tấn công (attacker) đã có được quyền truy cập vào hệ thống đăng nhập từ bên thứ ba được cấp chứng chỉ tin cậy và truy cập vào mạng POS. Khai thác từ lỗ hổng Zero-Day để tạo nên một đường lách xâm nhập hệ thống mạng nội bộ của Home Depot, thiết lập một con đường từ môi trường đối tác thứ ba đến lưới mạng của Home Depot. Sau khi đã truy cập thành công, chúng phát tán **Memory Scraping Malware** nhằm tấn công các điểm đầu cuối của thanh toán. **Memory Scraping Malware** có khả năng rất cao, đã thâu tóm thông tin của hàng triệu thẻ tín dụng.

Home Depot đã có rất nhiều động thái nhằm sửa chữa, chống lại cuộc tấn công này, sử dụng đến thẻ tín dụng EMV Chip-& Pin. Loại thẻ Chip-&Pin này có gắn một con chip bảo mật để đảm bảo

---

Essential Terminology

Hack Value

Dùng để chỉ một giá trị bao gồm sức hấp dẫn, sự hứng thú hoặc thứ gì đó đáng giá. Giá trị biểu thị mức độ hứng thú của hacker đối với mục tiêu

Zero-Day Attack

Zero-Day Attack nghĩa là những mối đe dọa và điểm yếu có thể khai thác nạn nhân trước khi nhà phát triển phát hiện, hoặc gửi và phát hành bản vá nhằm sửa chữa điểm yếu đó.

Vulnerability

Vulnerability có nghĩa là những chỗ yếu ớt, những lỗ hổng, những vấn đề trong bất kỳ hệ thống hoặc trong lưới mạng nào, giúp những tin tặc khám phá, khai thác nhằm vượt qua chúng. Bất kỳ điểm yếu nào cũng có thể là lối vào thuận lợi cho tin tặc xâm nhập vào mục tiêu.

Daisy Chaining

Daisy Chaining là một quá trình thử nghiệm nhiều cách thức tấn công hoặc "hacking" nhằm có được quyền truy cập vào một lưới mạng hay một hệ thống, hết lần này đến lần khác với thông tin giống nhau và thông tin có được từ lần thử nghiệm trước đó.

Exploit

Exploit là lỗ hổng bảo mật của một hệ thống qua Vulnerabilities, Zero-day Attacks hoặc bất kỳ thiết bị "hack" nào khác.

Doxing

Doxing nghĩa là sự công khai hoặc sự sắp đặt thông tin liên quan đến một cá nhân. Thông tin này được thu thập một cách công khai, phần lớn là từ truyền thông xã hội hoặc các nguồn khác.

Payload

Payload nghĩa là phần có thực của thông tin hoặc dữ liệu trong cấu trúc đối lập với siêu dữ liệu (metadata) tự động được sinh ra. Trong an toàn thông tin, Payload là một phần của mã độc, mã khai thác, những thứ gây ra nhiều hoạt động tiềm tàng nguy hiểm như là khai thác, xâm nhập qua hàng rào bảo mật của thiết bị (backdoor) và chiếm quyền kiểm soát.

Bot

Bots là loại phần mềm được sử dụng để điều khiển mục tiêu từ xa và thi hành nhiệm vụ được xác định từ trước. Phần mềm này có khả năng chạy các scripts tự động qua internet. Bên cạnh đó, được biết, bots cũng dành cho Internet Bot hoặc web robot. Những Bots này có thể được sử dụng cho mục đích xã hội như ChatterBots, mục đích tài chính hoặc mục đích cố ý gây tổn hại như Spambots, Viruses, và phát tán bọ, Botnets, tấn công **DDoS**

Những nhân tố của an toàn thông tin

Confidentiality (Tính bảo mật)

Chúng ta luôn muốn chắc chắn rằng những điều nhạy cảm, bí mật được bảo vệ. **Confidentiality** nghĩa là chỉ những người được cho phép mới có quyền được làm việc và xem xét những tài nguyên kỹ thuật số trong cơ sở hạ tầng của ta.

Cũng có thể rút ra ngụ ý rằng, ai chưa được ủy quyền không nên có bất kỳ truy cập nào để tiếp cận dữ liệu. Nói chung, có hai loại dữ liệu: dữ liệu di động (data in motion) – chúng di chuyển qua lại trong lưới mạng và dữ liệu tĩnh (data at rest), khi dữ liệu được lưu trữ ở bất kỳ phương tiện media nào (ví dụ như máy chủ, ổ cứng, đám mây). đối với dữ liệu di động, ta cần chắc chắn rằng chúng đã được mã hóa trước khi được gửi qua mạng. Có một lựa chọn khác chúng ta có thể sử dụng cùng với mật mã là sử dụng mạng riêng biệt cho dữ liệu nhạy cảm. đối với dữ liệu tĩnh, ta có thể áp dụng mật mã lại nơi lưu trữ để trong trường hợp bị đánh cắp, người khác không thể đọc được những dữ liệu này.

Integrity (Tính toàn vẹn)

Ta sẽ không hề muốn dữ liệu của mình bị những kẻ chưa được tin tưởng ủy thác truy cập được và sử dụng. Sự toàn vẹn của dữ liệu đảm bảo rằng chỉ những ai có được cấp quyền mới có thể thay đổi dữ liệu.

Availability (Tính sẵn sàng)

Availability gắn với hệ thống và dữ liệu. Nếu người được cấp quyền không thể lấy được dữ liệu do lỗi mạng thông thường hoặc do cuộc tấn công từ chối dịch vụ (DOS attack). Khi đó, trong trường hợp công việc còn có liên quan đến, đây vẫn là vấn đề. điều này cũng có thể dẫn tới mất mát doanh thu hoặc ghi chép lại một số kết quả quan trọng

Ta có thể dùng từ "**CIA**" để nhớ lấy ba khái niệm bảo mật cơ bản và quan trọng nhất

CIA	Risk	Control
Confidentiality	Mất quyền riêng tư Truy cập trái phép vào dữ liệu Ăn cắp dữ liệu cá nhân	Mật mã. Xác thực. Kiểm soát truy cập
Integrity	Thông tin không còn đáng tin hoặc không chính xác Gian lận	Maker-Checker. Bảo đảm chất lượng Sổ kiểm tra
Availability	Đứt đoạn công việc Mất an toàn bảo mật khách hàng Mất thu nhập	Tiếp tục công việc. Lên kế hoạch và kiểm tra Lưu trữ dự phòng

Authenticity (Tính xác thực)

Authentication (chứng minh xác thực) là quá trình nhận dạng người dùng hoặc thiết bị để cấp quyền ưu tiên, truy cập và đảm bảo các luật, các điều lệ đặt ra. Tương tự, Authenticity đảm bảo quá trình xác thực thông tin chắc chắn từ người dùng hợp lệ- những người có thể khẳng định thông ti và các tin nhắn chuyển tiếp đó bắt nguồn từ họ. Quá trình xác thực qua nhận dạng và mật khẩu kết hợp, ta có thể hoàn thành việc chứng minh xác thực

Figure 1-1 Elements of Information Security

Non-Repudiation (Tính không thể chối cãi)

Non-Repudiation là một trong những trụ cột của đảm bảo thông tin (information assurance) – bảo đảm việc truyền đi và nhận lại thông tin giữa người gửi với người nhận qua nhiều loại công nghệ như chữ ký kỹ thuật số hoặc mật mã. **Non-Repudiation** là cam kết xác thực, người gửi sẽ không thể chối bỏ những gì mình đã gửi. Tương tự như vậy, bên nhận sẽ không thể phủ định việc mình đã nhận. Hợp đồng kỹ thuật số, chữ ký, tin nhắn qua email sử dụng công nghệ **Non-repudiation**.

The Security, Functionality, and Usability Triangle

Trong một hệ thống, mức độ bảo mật là thước đo độ mạnh yếu của việc bảo mật, chức năng và tính khả dụng. Chúng ta biết rằng, ba điều này kết hợp tạo thành "tam giác" **Security, functionality & usability**.

Hãy xem xét một "trái bóng" nằm trong tam giác này. Khi trái bóng nằm trong trong tâm, điều đó có nghĩa là cả ba yếu tố đã nêu đều mạnh mẽ hơn. Ở khía cạnh khác, khi trái bóng lại gần phía "**Security**" hơn, có nghĩa là hệ thống đang tiêu tốn nhiều tài nguyên hơn cho việc bảo mật, chức năng và tính khả dụng của hệ thống cần nhiều sự quan tâm hơn. Một hệ thống bảo mật bắt buộc phải cung cấp cho người dùng sự bảo vệ mạnh mẽ song song với đem lại cho họ những dịch vụ, những đặc điểm và tính khả dụng cần thiết

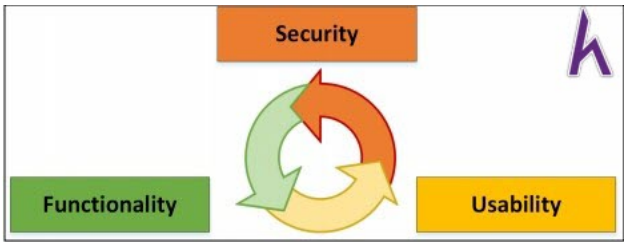

Figure 1-2 Security, Functionality & Usability Triangle

Việc thực thi hệ thống bảo mật cao cấp thường có sức ảnh hưởng một cách dễ dàng đến mức độ của chức năng và tính khả dụng. Chẳng cần ai dùng đến một hệ thống với phần nhìn xuống cấp. Trong khi phát triển một thiết bị, triển khai bảo mật trong hệ thống, chuyên gia bảo mật phải tâm niệm rằng cần chắc chắn về chức năng và tính khả dụng. Vậy nên, ba yếu tố này trong tam giác cần luôn được cân bằng.