BAN CƠ YẾU CHÍNH PHỦ

HỌC VIỆN KỸ THUẬT MẬT MÃ

PHÒNG CHỐNG VÀ ĐIỀU TRA TỘI PHẠM MÁY TÍNH

Đề tài

Dịch Learning Network forensics - chapter 1

***Sinh viên thực hiện*:**

- Nguyễn Đức Toàn
- Hà Ngọc Trâm
- Nguyễn Tiến Hoàng
- Vũ Anh Quân

Giáo viên hướng dẫn :
GV. Lại Minh Tuấn

Hà Nội, 12/2019

Mục Lục

Chương 1. Trở thành mạng 007

Chào mừng bạn đến với thế giới của các điệp viên, sự quyến rũ, công nghệ cao và nhanh chóng …

Đợi một chút!

Bạn có chắc là bạn đang đọc đúng cuốn sách? Cuốn sách này được cho là về pháp y mạng?

Vâng, bạn đang đọc đúng cuốn sách!

Hãy để tôi giúp bạn dễ hiểu hơn. Đây là về pháp y mạng. Điều đó nói rằng nó cũng là một quyến rũ thế giới đầy những gián điệp công nghệ cao và dữ liệu nhanh chóng (không có xe hơi, thật không may). Đây là một thế giới nơi nhân vật phản diện muốn sở hữu thế giới (hoặc ít nhất là thế giới kỹ thuật số của bạn) và nếu họ có thể sở hữu nó, họ muốn phá hủy nó.

Thế giới này cần một anh hùng. Một người có thể theo dõi các điệp viên, xác định các bí mật bị đánh cắp, đánh bại các nhân vật phản diện trong trò chơi của riêng họ, và cứu thế giới trong cuộc mặc cả.

Một anh hùng am hiểu công nghệ, lạnh lùng và tinh vi! Một 007 kỹ thuật số! Thôi nào, thừa nhận đi, ai không ưa thích bản thân như James Bond? Đây là cơ hội của bạn, một cơ hội để trở thành mạng 007.

Trong chương này, chúng tôi sẽ xây dựng sự hiểu biết về những gì chúng ta cần biết để liên doanh trong lĩnh vực pháp y mạng. Chúng tôi sẽ đề cập đến các chủ đề sau đây:

- 007 đặc điểm trong thế giới mạng
- Xác định các mối đe dọa cho doanh nghiệp
- Khảo sát vi phạm dữ liệu
- Xác định pháp y mạng
- Phân biệt giữa pháp y máy tính và pháp y mạng

- Tăng cường nền tảng kỹ thuật của chúng tôi
- Hiểu về an ninh mạng
- Mục tiêu an ninh mạng
- Dấu chân kỹ thuật số

Đặc tính 007 trong thế giới mạng

Trong thế giới 007, mọi thứ bắt đầu với một kích hoạt. Kích hoạt là một sự kiện hoặc sự cố mà cảnh báo cho tổ chức về các hoạt động không lành mạnh của những người được biết hoặc chưa biết.

Điều này có thể là phản ứng hoặc chủ động.

Là một phần của chiến lược phòng thủ chuyên sâu, mạng lưới tổ chức được bảo vệ bởi một số điều khiển phòng ngừa và thám tử (giám sát). Một kích hoạt có thể được xem xét phản ứng trong trường hợp một tổ chức nhận ra rằng các đối thủ của họ dường như đang nhận được bên trong thông tin, được giới hạn trong lưu thông và cực kỳ bí mật trong tự nhiên.

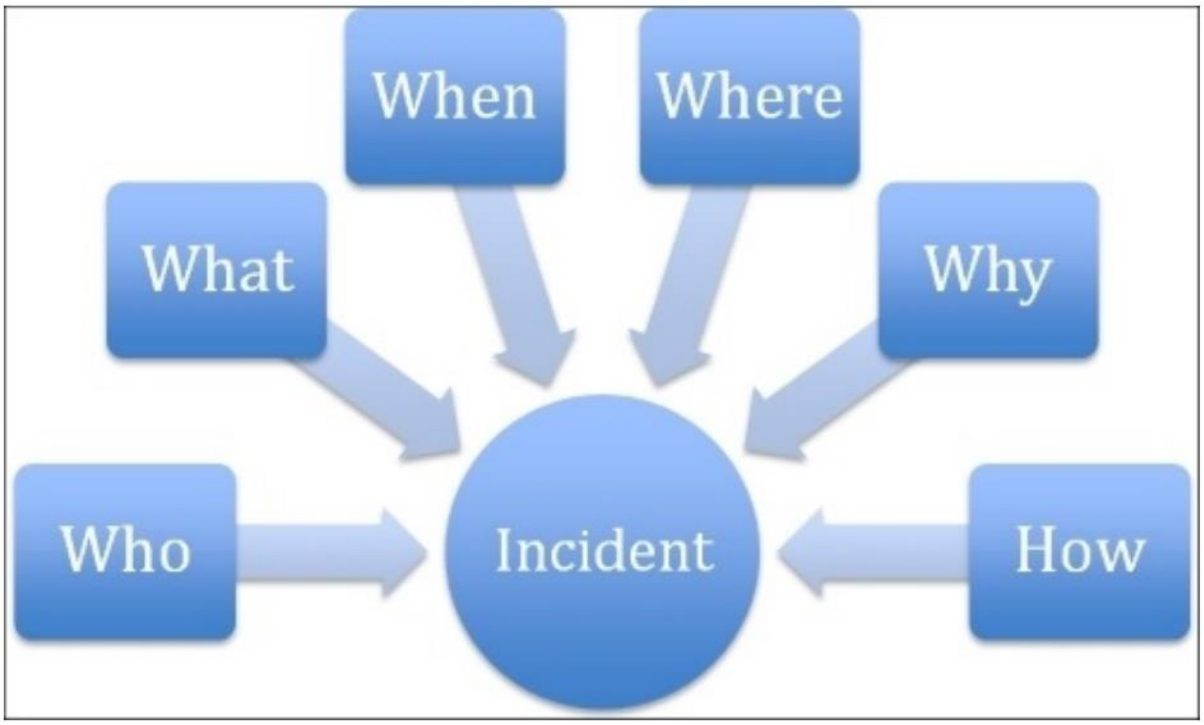
Tương tự, một kích hoạt chủ động có thể là kết quả của một tổ chức được ủy quyền kiểm tra thâm nhập và tập thể dục đánh giá lỗ hổng.

Sau sự kiện kích hoạt, một bài tập thu thập thông tin sơ bộ được bắt đầu, mà đỉnh điểm là một cuộc họp ngắn với 007 (điều tra viên), phác thảo tất cả các chi tiết hiện được biết về vi phạm/sự cố. Một số giả thuyết được đưa ra dựa trên thông tin thu thập cho đến nay. Kịch bản nguyên nhân và hiệu ứng có thể được khám phá. Có khả năng nghi phạm nội bộ và bên ngoài có thể được lọt vào danh sách để điều tra thêm.

Điều tra viên khởi xướng một bài tập thu thập thông tin / chứng cứ chính thức bằng cách sử dụng tất cả các loại công nghệ cao cấp có sẵn. Việc thu thập bằng chứng có thể được thực hiện từ lưu lượng mạng, bộ nhớ thiết bị đầu cuối và ổ cứng của máy tính bị xâm nhập hoặc thiết bị. Các công cụ chuyên dụng được yêu cầu để đạt được điều này. Điều này được thực hiện với quan điểm của

chứng minh hoặc bác bỏ các giả thuyết đã được thả nổi trước đó. Giống như **closed-circuit television (CCTV)** hoặc camera gián điệp được sử dụng để thu thập thông tin trong cuộc sống thực, trên một mạng, lưu lượng mạng được thu thập bằng các công cụ như **Wireshark**, bộ nhớ dễ bay hơi dữ liệu được thu thập bởi các công cụ như **Forensic Toolkit (FTK) Imager**, và hình ảnh phương tiện là được thu thập bởi các công cụ như **EnCase**.

Các thông tin được thu thập được phân tích cẩn thận và tỉ mỉ nhằm mục đích trích xuất bằng chứng liên quan đến vụ việc để giúp trả lời các câu hỏi, như thể hiện trong phần sau đây sơ đồ:

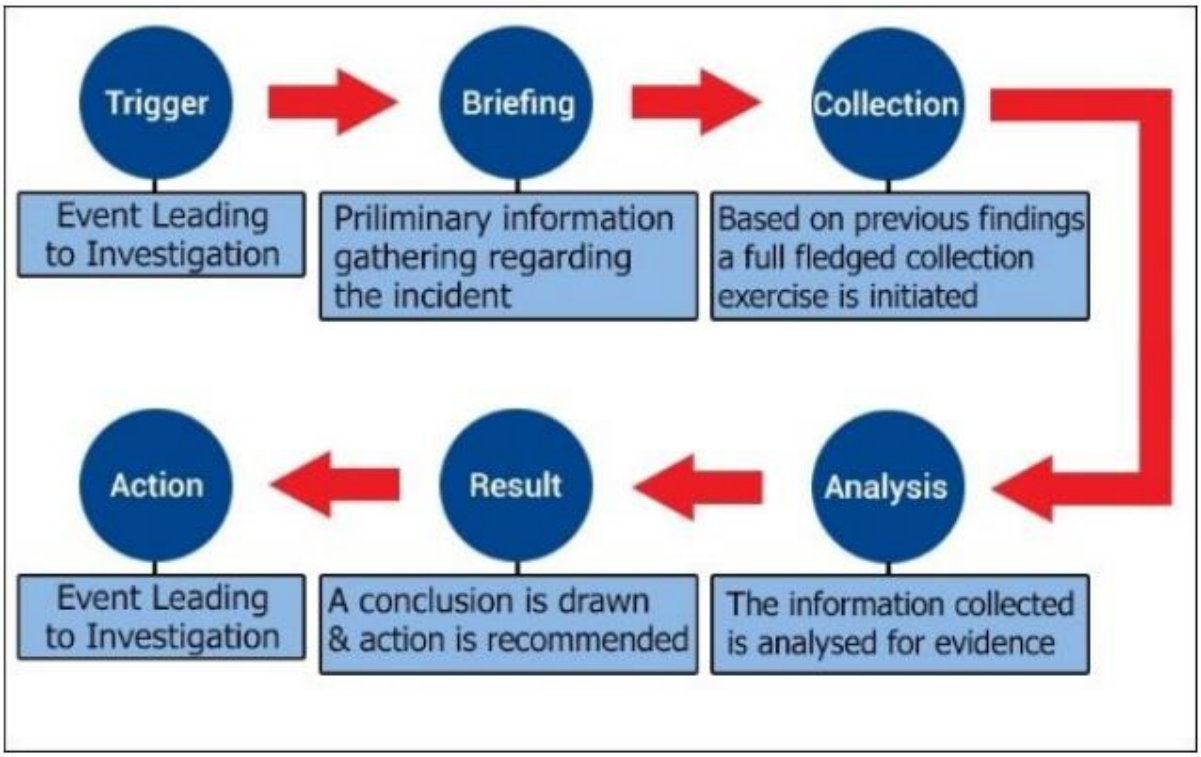


Một nỗ lực được thực hiện để trả lời các câu hỏi quan trọng sau:

- Ai đứng sau vụ việc?
- Điều gì thực sự đã xảy ra?
- Chuyện đó xảy ra khi nao?
- Đâu là tác động cảm thấy? Hoặc tài nguyên nào đã bị xâm phạm?
- Tại sao nó được thực hiện?

- Làm thế nào nó được thực hiện?

Dựa trên kết quả phân tích, một kết luận được rút ra và một số khuyến nghị nhất định là thực hiện. Những khuyến nghị này dẫn đến một hành động. Các hành động có thể bao gồm khắc phục, tăng cường phòng vệ, chấm dứt nhân viên / người trong cuộc, truy tố các nghi phạm, và như vậy dựa trên các mục tiêu của cuộc điều tra. Sơ đồ dòng sau đây tổng hợp gọn gàng hoàn thành quá trình:



Đặc điểm để Bond nhận biết trường hợp đã hoàn thành thành công

Điều tra pháp y mạng có thể rất tốn thời gian và phức tạp. Những điều tra thường rất nhạy cảm trong tự nhiên và có thể cực kỳ quan trọng như tốt. Để trở thành một Bond pháp y mạng hiệu quả, chúng ta cần phát triển các đặc điểm sau:

- **Chuẩn bị:** Giai đoạn chuẩn bị là điều cần thiết để cuối cùng đi đến kết luận thỏa đáng của một vụ án. Một phản ứng suy nghĩ bình tĩnh với một bộ sưu tập bằng chứng thích hợp quá trình đến từ đào tạo mở rộng và kiến thức về những gì cần làm trong sự kiện về sự xuất hiện của các kịch bản rất có thể đang xảy ra trong thế giới thực. Thực hành dẫn đến kinh nghiệm, dẫn đến khả năng đổi mới và đi ra ngoài hiểu biết sâu sắc về điều tra để giải quyết vụ án. Một tình huống mà điều tra viên không thể xác định một hệ thống bị xâm nhập có thể dẫn đến nhiều năm dữ liệu trộm cắp, dẫn đến sự chảy máu của tổ chức và sự sụp đổ cuối cùng và không kịp thời của nó. Một kịch bản trong đó một điều tra viên có thể xác định vấn đề nhưng không thể quyết định hành động để làm là xấu như nhau. Đây là nơi chuẩn bị đến. Quan trọng là biết phải làm gì trong hầu hết các tình huống.

  Một kế hoạch ứng phó sự cố rõ ràng cần được đưa ra. Nhân viên được đào tạo với các công cụ và quy trình cần thiết nên có sẵn để giải quyết mọi tình huống bất ngờ. Cũng như tổ chức thực hiện diễn tập chữa cháy thường xuyên, diễn tập ứng phó sự cố thể chế hóa như là một phần của chính sách tổ chức.

- **Thu thập thông tin / thu thập bằng chứng:** Một hệ thống toàn diện để giám sát các sự kiện & hoạt động mạng, lưu trữ nhật ký và sao lưu chúng là điều cần thiết. Đầu vào khác nhau được tạo bởi các công cụ ghi nhật ký sự kiện khác nhau, tường lửa, phòng chống xâm nhập & hệ thống phát hiện, và như vậy. Chúng cần được lưu trữ và / hoặc sao lưu an toàn vị trí để ngăn chặn sự giả mạo ngẫu nhiên hoặc cố ý.

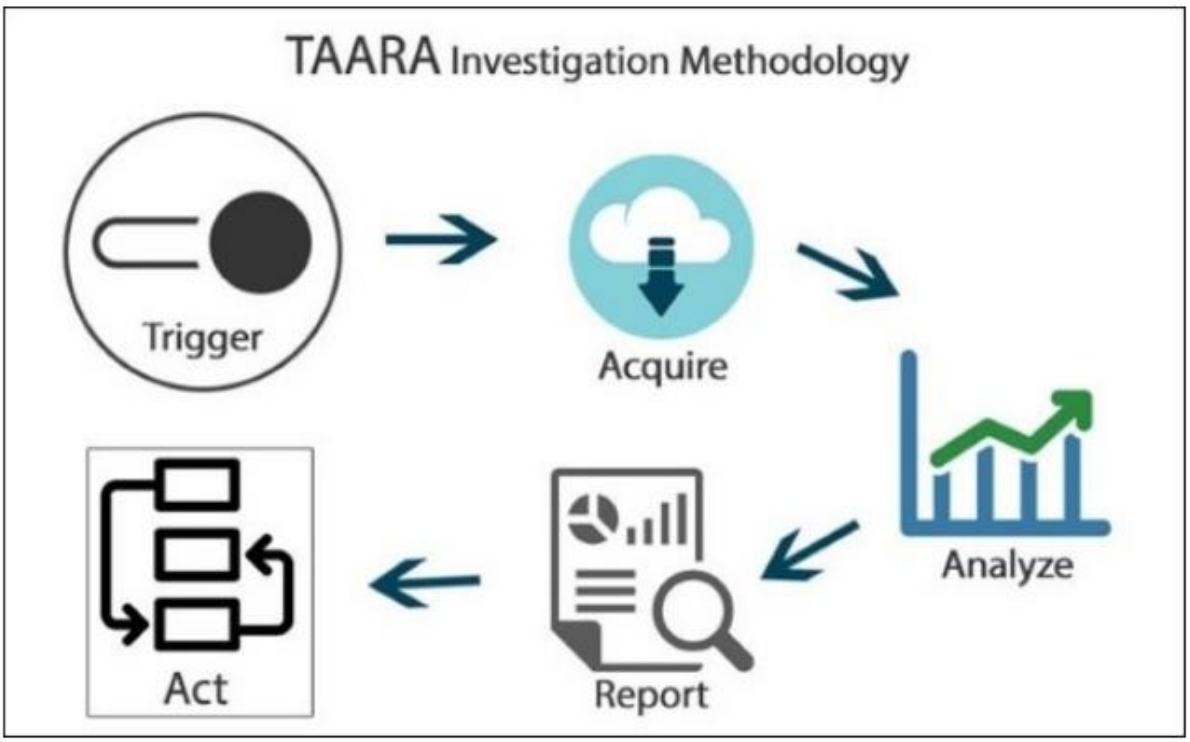
- **Hiểu biết về bản chất con người:** Một sự hiểu biết về bản chất con người là rất quan trọng. Điều này giúp điều tra viên xác định toán hạng modus, thuộc tính một động lực cho tấn công, và dự đoán và đánh bại kẻ địch Bước tiếp theo.
- **Hành động tức thì:** Giống như Bond bùng nổ thành hành động với một chút nguy hiểm, vì vậy phải là một điều tra viên. Dựa trên các chuẩn bị được thực hiện và ứng phó sự cố có kế hoạch, hành động ngay lập tức phải được thực hiện khi nghi ngờ thỏa hiệp mạng. Các câu hỏi như *hệ thống nên được đưa ra khỏi mạng? hoặc chúng ta nên cô lập nó từ mạng và xem những gì đang xảy ra?* nên đã được quyết định tại giai đoạn lập kế hoạch. Ở giai đoạn này, thời gian là điều cốt yếu và cần phải hành động ngay lập tức.
- **Sử dụng công nghệ:** Một điều tra viên nên có Bond tình yêu công nghệ cao. Tuy nhiên, một kiến thức kỹ lưỡng về các công cụ là phải. Một số công nghệ cao các công cụ giám sát đóng một vai trò quan trọng trong các cuộc điều tra dựa trên mạng. Các công cụ chuyên dụng giám sát lưu lượng mạng, xác định và truy xuất dữ liệu ẩn và bị che giấu, phân tích và trực quan hóa các bản ghi và hoạt động của mạng, và không tham gia vào các chương trình trong bộ nhớ và phần mềm độc hại và các công cụ được sử dụng bởi những kẻ xấu.
- **Suy luận suy diễn:** Một quá trình suy nghĩ logic, khả năng suy luận thông qua tất cả các bước liên quan và mong muốn xem xét trường hợp để kết luận đúng đắn của nó là các kỹ năng cần phải là một phần của kho vũ khí 007. Đặt câu hỏi cho tất cả các giả định, đặt câu hỏi về nguyên nhân và kết quả không thể nghi ngờ, kiểm tra khả năng xảy ra một sự kiện, v.v. là những đặc điểm nổi bật của một sự phát triển điều tra viên.

Phương pháp TAARA cho pháp y mạng

Có sự chồng chéo đáng kể giữa phản ứng sự cố và pháp y mạng trong thế giới doanh nghiệp, với các chuyên gia bảo mật thông tin được giao nhiệm vụ với cả hai vai trò. Để giúp đơn giản hóa sự hiểu biết về quy trình, chúng tôi đã đưa ra cách dễ dàng ghi nhớ khung TAARA:

- **Kích hoạt:** Đây là vụ việc dẫn đến cuộc điều tra.
- **Mua lại:** Đây là quá trình được thiết lập trong chuyển động bởi bộ kích hoạt, điều này được xác định trước là một phần của kế hoạch ứng phó sự cố, và nó liên quan đến việc xác định, thu nhận và thu thập thông tin và bằng chứng liên quan đến vụ việc. Điều này bao gồm nhận thông tin liên quan đến các yếu tố kích hoạt, lý do nghi ngờ sự cố và xác định và thu thập các nguồn bằng chứng cho phân tích tiếp theo.
- **Phân tích:** Tất cả các bằng chứng được thu thập cho đến nay được đối chiếu, tương quan và đã phân tích. Chuỗi các sự kiện được xác định. Những câu hỏi quan trọng như liệu sự cố có thực sự xảy ra hay không; nếu nó đã làm, chính xác những gì đã xảy ra; nó như thế nào đã xảy ra; ai đã tham gia; mức độ thỏa hiệp là gì; và v.v. trả lời dựa trên thông tin được thu thập trong giai đoạn này, nó có thể cần thiết để quay lại giai đoạn thu nhận để thu thập thêm bằng chứng. Phân tích sau đó được bắt đầu trên các bằng chứng mới thu được.
- **Báo cáo:** Dựa trên phân tích trước đó, một báo cáo được tạo ra trước các bên liên quan để xác định quá trình hành động tiếp theo.
- **Hành động:** Hành động được đề xuất trong báo cáo thường được thực hiện trong thời gian này.

Đây là hình ảnh đại diện trong hình ảnh sau đây:



Xác định các mối đe dọa cho doanh nghiệp

Dựa trên nguồn gốc của mối đe dọa, các cuộc tấn công có thể được phân loại thành các điều sau đây các loại:

- Nội bộ
- Bên ngoài
- Hỗn hợp

Các mối đe dọa nội bộ

Các mối đe dọa hoặc tấn công bắt nguồn từ trong mạng hoặc tổ chức được phân loại là các mối đe dọa nội bộ. Đây có thể là cố ý hoặc vô ý.

Thông thường, các mối đe dọa như vậy liên quan đến một người trong cuộc với ý định trung thực, kiến thức nội bộ và / hoặc truy cập. Người trong cuộc này đang tìm cách đánh cắp, sử dụng sai, sửa đổi, tham nhũng hoặc phá hủy nguồn lực doanh nghiệp. Hoàn toàn tự nhiên, người trong cuộc không có ý định bị bắt và do đó, làm cho mọi nỗ lực để che dấu vết của họ. Tuy nhiên, như chúng ta sẽ thấy sau trong này.

Chương này, mọi tương tác với hiện trường vụ án đều để lại dấu vết theo nguyên tắc **Locard’s exchange principle**.

Các quy tắc yếu và không rõ ràng, chính sách mạng, hệ thống bảo mật, v.v.

người trong cuộc. Người dùng truy cập không giới hạn và không bị giám sát tài nguyên mạng và dữ liệu một công thức chắc chắn cho thảm họa. Kiểm soát thực hiện không đúng, quyền ngẫu nhiên, truy cập vật lý không an toàn vào phòng máy chủ và vệ sinh mật khẩu kém góp phần vào mối đe dọa nghiêm trọng đến tài nguyên mạng.

Các mối đe dọa bên ngoài

Các mối đe dọa bên ngoài là những mối đe dọa bắt nguồn từ bên ngoài chu vi của mạng. Điều này có thể từ các cá nhân, nhóm hoặc thậm chí chính phủ. Một loạt các cuộc tấn công mạng trên toàn thế giới đã được truy tìm đến các diễn viên nhà nước như Trung Quốc, Bắc Triều Tiên và thậm chí HOA KỲ. Những tiết lộ của Snowden đã mở ra cho mọi người những ánh mắt về mối đe dọa thực sự của nhà nước - giám sát tài trợ.

Các mối đe dọa bên ngoài đến trong tất cả các hình dạng và kích cỡ. Cũng giống như các mối đe dọa nội bộ, đây có thể là Cố ý hay vô ý. Có đủ loại người ngoài kia muốn vào mạng của bạn. Một số muốn làm điều đó để có được thông tin bạn lưu trữ, một số làm điều đó để đóng cửa xuống mạng của bạn, một số làm điều đó vì họ không thích tuyên bố của công ty bạn CEO đã đưa ra vào thứ Tư tuần trước, và một số người muốn làm điều đó chỉ vì họ có thể. Đi thôi động lực sang một bên cho thời điểm này. Tôi nói hiện tại là một phần của pháp y mạng của chúng tôi điều tra yêu cầu trả lời phần Tại sao của phương trình vào một ngày sau đó.

Bất kỳ người ngoài nào muốn truy cập vào mạng của bạn phải thực hiện một số bước cụ thể trước khi họ có thể có được quyền truy cập của bất kỳ loại. Nó tốt nhất là không được tin vào khái niệm rằng, giống như trong những bộ phim, một hacker ngồi trước máy tính của anh ta, bắt đầu nhập và có cấp Quản trị viên truy cập trong vòng một vài phút. Đó là hư cấu không thể thay đổi.

Bước đầu tiên mà bất kỳ kẻ tấn công nào phải thực hiện là điều chỉnh lại mục tiêu. Cũng như bất kỳ tốt hay kẻ trộm hoàn thành sẽ phá án khu phố để xác định các mục tiêu tiềm năng, xác định vị trí của chúng điểm yếu, lên kế hoạch thời gian thích hợp để đột nhập và tìm ra cách để xâm nhập; bất kỳ tội phạm với ý định vào mạng phải trải qua một quá trình tương tự. Quá trình này là gọi là dấu chân. Điều này bao gồm một số bước tiếp theo là quét UDP mở & Cổng TCP, có thể được khai thác. Một nỗ lực sau đó được thực hiện để thử và lấy mật khẩu thông qua nhiều phương tiện như kỹ thuật xã hội, danh sách mật khẩu, vũ phu hoặc cầu vồng những cái bàn. Chế độ khám phá mật khẩu này là phương pháp khó nhất để vào mạng. Một ví dụ khác là khai thác điểm yếu như HĐH chưa được vá và chạy các chương trình khai thác phần mềm dễ bị tổn thương dẫn đến truy cập mở, tiếp theo là leo thang đặc quyền đến cấp quản trị viên.

Sau khi vào, điệp viên đã hoàn thành sẽ không làm gì để cho đi sự thật rằng họ có cấp quản trị viên truy cập. Nó chỉ là kịch bản kiddies hoặc tin tặc đói công khai đi phía trước để đánh bại các trang web để kiếm được hai phút nổi tiếng hoặc nổi tiếng của họ.

Mục tiêu tiếp theo là tạo ra một cửa hậu để truy cập không bị gián đoạn và lấy mọi đề phòng để che dấu vết của họ.

Nó có thể là vài tháng và, trong một số trường hợp, nhiều năm trước khi một sự xâm nhập của loại đó có thể phát hiện hoặc phát hiện. Đó là chén thánh của kẻ tấn công. Gián điệp không bị phát hiện! Mãi mãi!

Tuy nhiên, đó chính xác là nơi bạn đến, ông 007. Bạn phải tìm ra những gì mà đi trên mạng. Đôi khi, điều này cần phải được thực hiện cực kỳ bí mật. Khi dữ liệu Vi phạm được phát hiện, bạn cần vào chế độ tiêu diệt được cấp phép của mình để xác định như vậy xâm nhập và thu thập tất cả các bằng chứng của các quá trình liên quan!

Bạn cần xác định thủ phạm, thẩm vấn anh ta hoặc nhân chứng (pháp y thẩm vấn các gói dữ liệu, phương tiện và bộ nhớ) để xác định cái gì, khi nào, ở đâu, tại sao, và làm thế nào.

Khảo sát vi phạm dữ liệu

Có rất nhiều cuộc điều tra vi phạm dữ liệu / bảo mật thông tin / tội phạm mạng

được xuất bản hàng năm bởi những người của ngành tư vấn.

một vài tài liệu tham khảo trên mạng, được liệt kê dưới dạng sau:

- The Verizon Data Breach Investigations Report: http://www.verizonenterprise.com/DBIR/
- PwC UK—INFORMATION SECURITY BREACHES SURVEY 2014: http://www.pwc.co.uk/assets/pdf/cyber-security-2014-exec-summary.pdf
- The Ponemon Institute's Cost of Data Breach Survey: http://www.ponemon.org/blog/ponemon-institute-releases-2014-cost-of-data-breachglobal-analysis
- KPMG Cybercrime survey report: https://www.kpmg.com/IN/en/IssuesAndInsights/ArticlesPublications/Documents/KPMG_Cyber_Crime_survey_report_2014.pdf
- The InfoWatch Global Data Leakage Report, 2014: http://infowatch.com/sites/default/files/report/InfoWatch_Global_data_leak_report_2014_

Tất cả đều chỉ ra một sự thật không thể chấp nhận được là các vi phạm dữ liệu ngày càng trở nên đắt đỏ và sẽ tiếp tục như vậy.

Một số điểm được đưa ra bởi hầu hết trong số họ là:

- Chi phí vi phạm dữ liệu đang gia tăng.
- Đăng một khách hàng vi phạm tin tưởng mất niềm tin và có xu hướng thay đổi nhà cung cấp dịch vụ.Điều này đặc biệt phổ biến trong ngành dịch vụ tài chính.
- Đối với nhiều quốc gia, các cuộc tấn công độc hại hoặc tội phạm là nguyên nhân hàng đầu của các vi phạm dữ liệu.
- Trong hơn 50% các trường hợp, người trong cuộc có liên quan theo cách này hay cách khác.

Điều này có ý nghĩa gì với chúng ta? Nó chỉ có nghĩa là chúng ta đang ở đúng nơi vào đúng thời điểm. Sẽ luôn có một nhu cầu rất lớn đối với Sherlocks của

mạng. Chuyên gia có thể phát hiện, thu thập, đối chiếu, phân tích và điều tra sẽ thấy mình phải thuê danh sách các tập đoàn quy mô lớn nhất.

Hãy để bắt đầu với các nguyên tắc cơ bản của pháp luật dưới mọi hình thức

Nguyên tắc trao đổi Locard

Không có nghiên cứu về điều tra kỹ thuật số có thể được coi là bắt đầu tốt mà không hiểu của nền tảng của khoa học. Nguyên tắc trao đổi Locard từ là nền tảng trên phương pháp điều tra khoa học được xây dựng.

Tiến sĩ Edmond Locard (1877-1966) là một nhà khoa học người Pháp làm việc với người Pháp Mật vụ trong Thế chiến thứ nhất. Ông là người tiên phong trong khoa học pháp y và tội phạm học. Ông đã phát triển một phương pháp để xác định bản chất và nguyên nhân cái chết của Lính và tù nhân Pháp bằng cách kiểm tra các vết thương, vết bẩn và các dấu vết khác trên cơ thể.

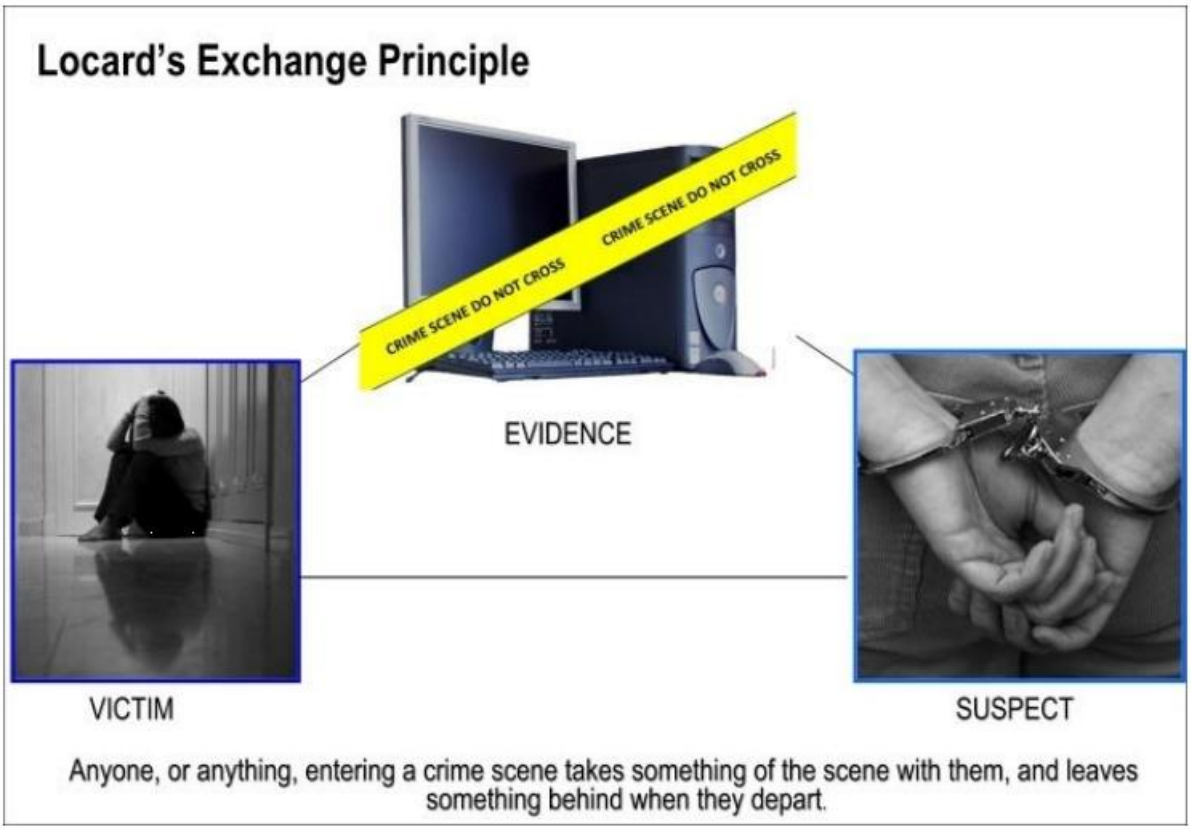
Ông được biết đến với cái tên Sherlock Holmes của Pháp.

Ông thường được ghi nhận khi nói rằng mọi liên lạc đều để lại dấu vết!

Ông suy đoán rằng bất kỳ ai hoặc bất cứ điều gì xâm nhập hoặc rời khỏi hiện trường vụ án (tương tác với hiện trường vụ án) hoặc để lại một cái gì đó phía sau hoặc để lại một cái gì đó từ nó (vô tình hoặc cố ý) và điều này có thể được sử dụng làm bằng chứng pháp y. Hãy xem xét một giết người. Bất cứ ai đi vào một điểm giết người có thể để lại bằng chứng về sự hiện diện của họ dưới dạng dấu chân, dấu vân tay, vân vân. Tương tự, khi ai đó rời khỏi hiện trường vụ án, họ có thể mang theo máu, bụi địa phương có thể bám vào giày, vân vân.

Làm thế nào điều này dịch vào thế giới mạng?

Về cơ bản, mọi nỗ lực giao tiếp với một thiết bị trên mạng đều để lại dấu vết một vài nơi; điều này có thể là tại tường lửa, hệ thống phát hiện xâm nhập, bộ định tuyến, nhật ký sự kiện….Tương tự, bất kỳ nỗ lực nào của một hành vi sai trái nội bộ để truy cập các tài nguyên trái phép cũng sẽ để lại dấu vết. Điều này được mô tả trong hình ảnh sau đây:



Locard's exchange principle in a digital world

Hãy lấy ví dụ về một cuộc tấn công lừa đảo. Như chúng ta đều biết, nó bắt đầu bằng một thư vô thưởng vô phạt với một chủ đề hấp dẫn ồ ạt. Thư lừa đảo có thể mang một tải trọng dưới dạng tệp đính kèm (ví dụ: Trojan) hoặc có liên kết dẫn đến kết quả tương tự. Trong trường hợp này, theo nguyên tắc trao đổi Locard, hai thực thể tương tác sẽ là máy tính bị ảnh hưởng và máy tính gửi lừa đảo. Một số bằng chứng trong trường hợp này sẽ là chính e-mail, Trojan Horse / phần mềm độc hại / keylogger, mật khẩu bị đánh cắp, mật khẩu thay đổi, cố gắng che dấu vết, vân vân. Cửa sau, một khi được phát hiện, có thể tiết lộ rất nhiều chi tiết và địa chỉ IP của các thiết bị điều khiển nó hoặc nhận được dữ liệu bị đánh cắp cũng sẽ được tính là bằng chứng. Trung tâm chỉ huy và kiểm soát cho hoạt động lừa đảo (nếu được xác định) cũng sẽ là một bằng chứng vàng.

Là một mạng 007, công việc của chúng tôi là tìm hiểu chuyện gì đang xảy ra và rút ra kết luận phù hợp.

Xác định pháp y mạng

Chính xác thì pháp y mạng là gì?

Theo Viện Tiêu chuẩn và Công nghệ Quốc gia (NIST), Pháp y kỹ thuật số, cũng được gọi là pháp y máy tính và mạng, có nhiều định nghĩa. Nói chung là xem xét việc áp dụng khoa học vào việc xác định, thu thập, kiểm tra và phân tích dữ liệu trong khi bảo tồn tính toàn vẹn của thông tin và duy trì nghiêm ngặt chuỗi lưu ký cho dữ liệu.

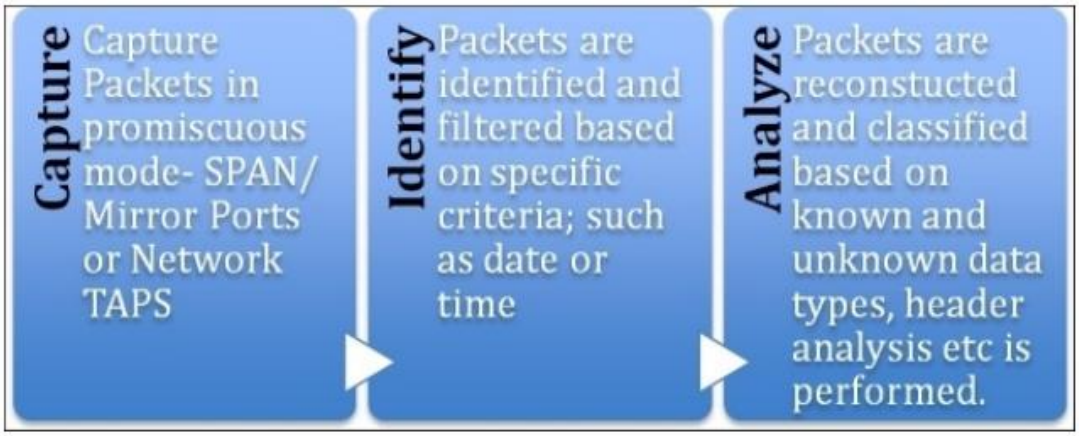
Tham khảo http://csrc.nist.gov/publications/nistpub/800-86/SP800-86.pdf để biết thêm thông tin.

Theo WhatIs.com, pháp y mạng là thu thập, ghi lại và phân tích mạng các sự kiện để khám phá nguồn gốc của các cuộc tấn công an ninh hoặc các sự cố khác.

Nói rộng ra, pháp y mạng, ở hầu hết mọi người Nhận thức về mối quan hệ, liên quan đến CIA quá trình. Trong trường hợp này, CIA là viết tắt của từ sau:

- Chụp (chụp gói)
- Xác định (xác định các gói dựa trên tiêu chí lọc nhất định, chẳng hạn như ngày và giờ)
- Phân tích (cả các gói đã biết và chưa biết để hiểu những gì đang diễn ra)

Hình ảnh sau đây minh họa điều này:



Nói rộng ra, pháp y mạng là tập hợp con của pháp y kỹ thuật số liên quan đến điều tra các sự kiện và hoạt động liên quan đến mạng kỹ thuật số. Điều này liên quan đến giám sát và nắm bắt lưu lượng mạng và dữ liệu liên quan từ các thiết bị trên mạng bằng mục tiêu thu thập chứng cứ theo cách được chấp nhận tại tòa án.

Phân biệt giữa pháp y máy tính và pháp y mạng

Network forensics là một nhánh của pháp y kỹ thuật số. Nó khác biệt đáng kể từ điều tra pháp y thông thường. Cần phải làm nổi bật sự khác biệt rằng mọi thứ rõ ràng hơn rất nhiều trong tâm trí điều tra viên mạng.

Không giống như các lĩnh vực pháp y kỹ thuật số khác, điều tra pháp y mạng đối phó với sự biến động và thông tin động. Pháp y đĩa hoặc máy tính chủ yếu xử lý dữ liệu ở phần còn lại. Quá trình bình thường được đơn giản hóa là xác định phương tiện cần điều tra, tạo và xác thực hình ảnh pháp y, xác định các hiện vật khác nhau cần điều tra, thực hiện một phân tích chuyên sâu, và theo dõi nó với một báo cáo nêu bật những phát hiện. Thông thường, những thứ này có thể bao gồm các tệp và tạo phẩm bị xóa, đặt tên sai và ẩn; mục đăng ký; tập tin được bảo vệ bằng mật khẩu; liên lạc qua thư điện tử; dữ liệu khắc; vân vân Tuy nhiên, tất cả chúng đại diện cho trạng thái của hệ thống tại thời điểm thu thập và hình ảnh.

Mạng pháp y bởi bản chất của nó là năng động. Trên thực tế, nó sẽ không thể tiến hành điều tra pháp y mạng nếu các thỏa thuận trước không được thực hiện để nắm bắt và lưu trữ lưu lượng mạng. Không thể phân tích những gì đã xảy ra với mạng chảy mà không có một bản sao của nó. Điều này tương tự như có một cảnh quay camera quan sát cho một cụ thể biến cố. Khi vắng mặt, người ta chỉ có thể phỏng đoán những gì đã xảy ra dựa trên cái khác bằng chứng hoàn cảnh. Khi cảnh quay thực tế có sẵn, miễn là điều tra viên biết những gì cần tìm kiếm, sự cố hoàn toàn có thể được xây dựng lại và nó trở nên rất nhiều dễ dàng hơn để xác định thủ phạm.

Ngoài ra, pháp y mạng liên quan đến việc phân tích các bản ghi. Đây có thể là một chút nghệ thuật như cũng như khoa học.

Thông thường các thiết bị mạng, ứng dụng, hệ điều hành đang sử dụng và khác lập trình và thiết bị thông minh trên mạng tạo nhật ký. Nhật ký được tính thời gian. Chúng có thể khá khó hiểu về bản chất và các thiết bị khác nhau sẽ giải quyết giống nhau sự kiện theo những cách khác nhau. Một số hệ điều hành sẽ gọi một hành động đăng nhập là đăng nhập; trong khi đó, một thiết bị khác có thể gọi nó là đăng nhập và một phần ba có thể gọi nó là xác thực người dùng

biến cố. Nội dung tin nhắn và cú pháp của nhật ký là dành riêng cho nhà cung cấp. Nó cũng có thể thay đổi từ ứng dụng vào ứng dụng.

Đĩa pháp y không có những loại phức tạp. Trong khi các bản ghi tồn tại và làm khác nhau trên các ứng dụng và hệ điều hành, mức độ phụ thuộc vào nhật ký trong trường hợp đĩa pháp y không cao bằng pháp y mạng.

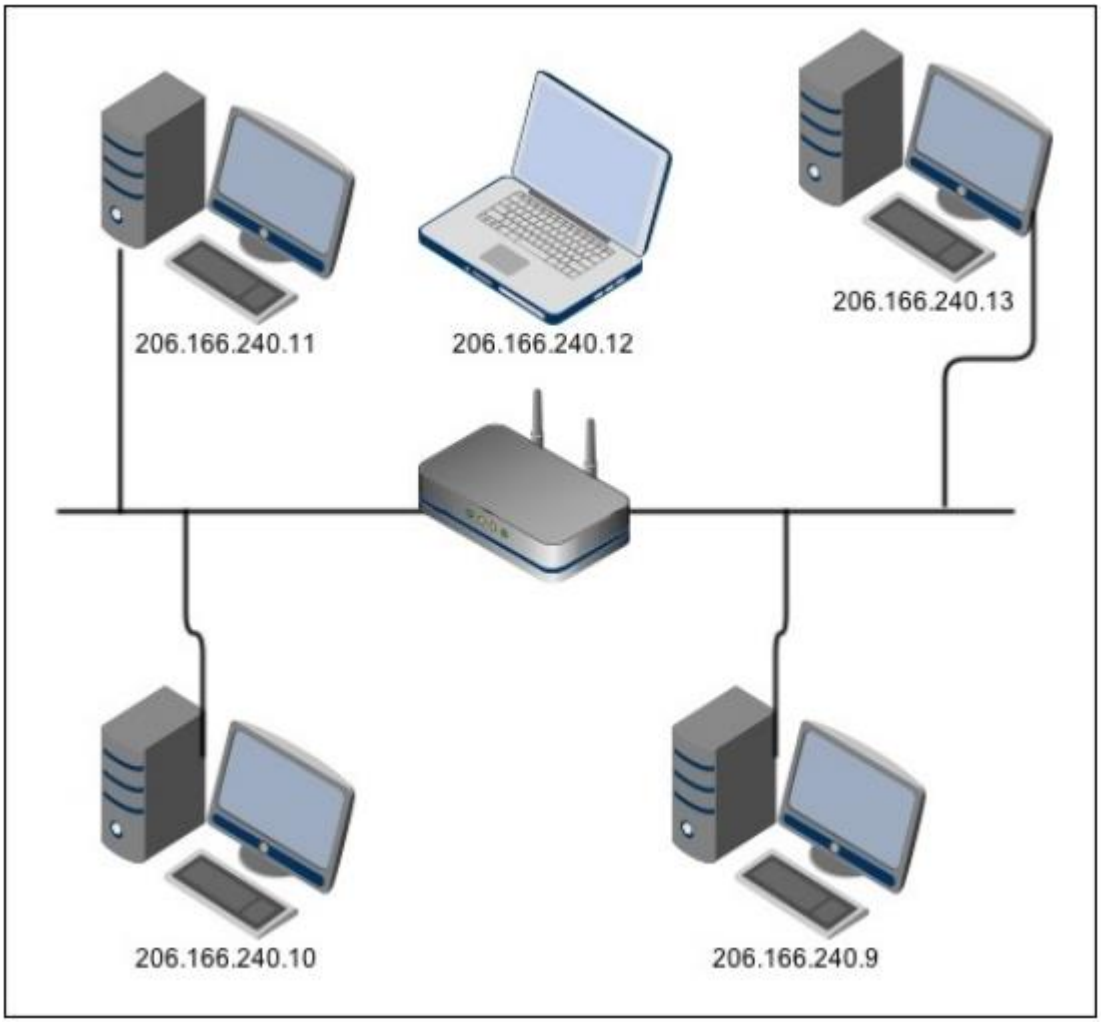
Điều đó nói rằng, tất cả các pháp y đĩa, mạng và bộ nhớ đi đôi với nhau. Hầu hết các cuộc điều tra có thể liên quan đến ít nhất một vài, nếu không phải tất cả, các nguyên tắc của pháp y kỹ thuật số trong mọi trường hợp cường độ hợp lý.

Trong thực tế, một trường hợp mà pháp y đĩa không được sử dụng trong một cuộc điều tra có thể được xem xét tương đương với một trường hợp thông thường mà bằng chứng camera quan sát đã bị bỏ qua.

Tăng cường nền tảng kỹ thuật của chúng tôi

Trước khi chúng tôi phát triển các kỹ năng về pháp y mạng, chúng ta cần phải có những nguyên tắc cơ bản nhất định.

Một mạng, theo cách nói chung, là một nhóm các máy tính / thiết bị được kết nối với nhau khác Kết nối có thể có dây hoặc không dây. Mỗi thiết bị trên mạng đều có một địa chỉ mạng duy nhất. Điều này có thể là tạm thời (phiên cụ thể) hoặc vĩnh viễn. Địa chỉ là số lượng dễ dàng cho máy tính làm việc với; tuy nhiên, chúng không dành cho con người cần nhớ. Chúng được gọi là địa chỉ IP. Ví dụ: 206.166.240.9. Hãy xem xét sơ đồ sau:



Một mạng đơn giản

Để làm cho những địa chỉ số này dễ dàng cho con người nhớ, chúng được lưu trữ dưới dạng văn bản địa chỉ dưới dạng bản ghi Máy chủ tên miền (DNS). Máy chủ DNS chịu trách nhiệm dịch địa chỉ Internet văn bản thành địa chỉ Internet số.

Trong khi các địa chỉ IP số xác định một máy chủ lưu trữ cụ thể hoạt động trên mạng, một số cổng số được sử dụng để xác định các quy trình cụ thể đang chạy trên máy chủ máy móc. Số lượng cổng không bị giới hạn chức năng. Một số cổng phổ biến là như sau:

Port number	Application
20	FTP
21	FTP
23	Telnet
25	SMTP (mail)
79	Finger
80	HTTP
110	POP3 (mail)
443	HTTPS

Khi các thiết bị được kết nối với nhau; chúng có thể giao tiếp. Cách giao tiếp giữa các thiết bị là thông qua trao đổi dữ liệu. Dữ liệu được truyền bằng các gói. Tin nhắn được chia thành các gói và truyền qua mạng. Mỗi gói này có kích thước tối đa được chỉ định, được chia thành vùng dữ liệu và tiêu đề. Mỗi gói được gửi từ một máy tính nguồn đến một máy tính hoặc thiết bị đích, địa chỉ và thông tin của chúng là cần thiết để sắp xếp đúng trình tự các gói và được viết lại trong phần tiêu đề.

Giao tiếp giữa hai máy tính được kết nối trên mạng bị chi phối bởi các quy tắc được gọi là giao thức.

Các giao thức xác định như sau:

- Addressing of messages
- Routing of messages
- Error detection
- Error recovery
- Packet sequence
- Flow controls

Thiết kế giao thức dựa trên mô hình kiến trúc phân tầng, chẳng hạn như Hệ thống Open Systems Interconnection (OSI).

Đây còn được gọi là mô hình bảy tầng.

Mô hình bảy tầng

Đúng như tên gọi, mô hình này bao gồm bảy tầng. Mỗi tầng trong số này được giải thích như sau:

- Tầng 1: Đây được gọi là tầng vật lý. Đây là cơ sở hạ tầng vật lý thực tế dữ liệu đi qua. Bao gồm các dây cáp, trung tâm, vv. Đây là thiết bị điện tử đảm bảo truyền tải vật lý và tiếp nhận dữ liệu dạng thô, bit, byte không cấu trúc.
- Tầng 2: Đây được gọi là tầng liên kết. tầng này chịu trách nhiệm đóng gói dữ liệu và biểu diễn chúng ở tầng vật lý. Điều này sẽ bắt đầu và chấm dứt một liên kết logic giữa hai nút trên mạng. tầng 2 chịu trách nhiệm chuyển dữ liệu không có lỗi trên tầng vật lý.
- Tầng 3: Đây được gọi là tầng mạng. tầng này phụ trách một gói truyền từ một nguồn đến đích của nó. tầng này quyết định tuyến đường, ánh xạ của các địa chỉ logic và vật lý, và kiểm soát lưu lượng dữ liệu.
- tầng 4: Đây được gọi là tầng vận chuyển. tầng vận chuyển phụ trách phân phối các gói từ một nguồn đến đích. Điều này đảm bảo rằng thông điệp được phân phối theo trình tự mà không bị trùng lặp hoặc mất và không có lỗi.
- Tầng 5: Đây được gọi là tầng phiên. tầng phiên quản lý mạng truy cập. Nó thiết lập các phiên giữa các tiến trình đang chạy trên các nút khác nhau thông qua cổng logic khác nhau. tầng 5 cũng xử lý việc thiết lập phiên, bảo trì và chấm dứt.
- Tầng 6: Đây được gọi là tầng trình diễn. Vai trò của tầng trình diễn là định dạng dữ liệu truyền đến các ứng dụng, chuyển đổi dữ liệu, nén / giải nén, mã hóa, v.v. Điều này cho phép người dùng cuối truy cập đến các dịch vụ Windows khác nhau như chia sẻ tài nguyên, in từ xa, v.v.
- Tầng 7: Đây được gọi là tầng ứng dụng. Đây là tầng người dùng cuối. tầng này chứa các ứng dụng, như Java, Microsoft Word, v.v., được sử dụng bởi người dùng cuối cùng.

Khi dữ liệu di chuyển giữa các tầng, mỗi tầng sẽ thêm hoặc xóa tiêu đề của nó cho đơn vị dữ liệu. Tại đích, mỗi tiêu đề được thêm vào sẽ bị xóa từng cái một cho đến khi nhận được dữ liệu ứng dụng dành cho nó.

Mô hình TCP / IP

Mô hình TCP / IP chỉ bao gồm bốn tầng. Là ứng dụng, giao vận, internet,

và mạng.

Các tầng này được hiển thị trong bảng sau:

Tên lớp	Mô tả
Ứng dụng	Chịu trách nhiệm cho các ứng dụng và quy trình đang chạy trên mạng
Giao vận	Cung cấp phân phối dữ liệu đầu cuối
Internet	Định tuyến datagram và dữ liệu
Mạng	Cho phép truy cập vào mạng vật lý

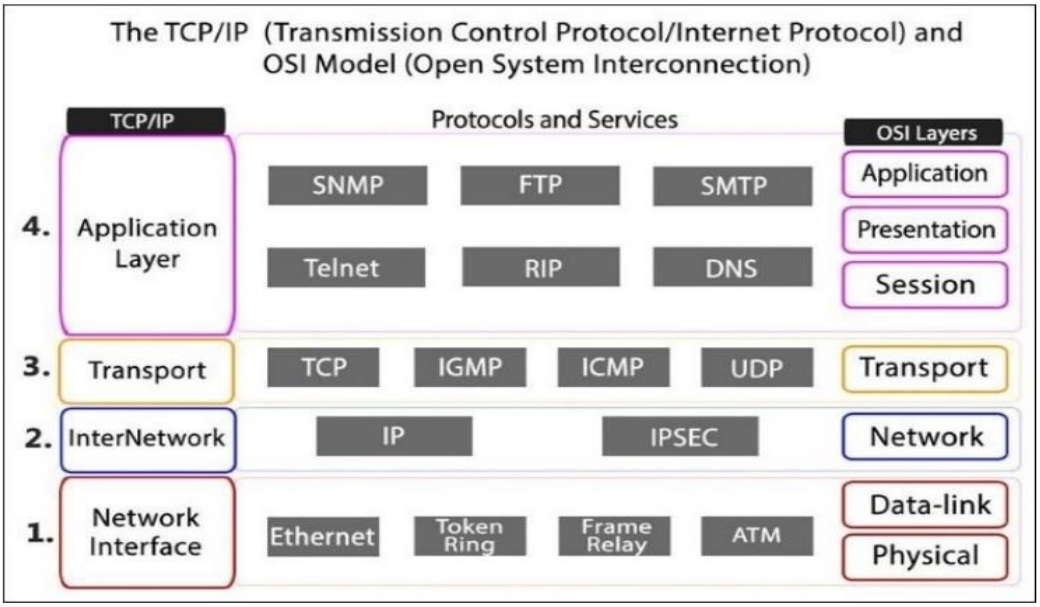
Chúng ta hãy xem xét từng cái một, bắt đầu từ lớp giao diện mạng và làm việc theo cách của chúng tôi trở lên.

- Lớp mạng: Lớp mạng (hoặc lớp giao diện mạng, như được biết đến) là nền tảng của mô hình TCP / IP. Làm cho các tín hiệu được truyền trên mạng. Nó truyền và nhận bit qua phần cứng mạng, chẳng hạn như cáp đồng trục hoặc cáp xoắn đôi. Bao gồm các giao thức sau:

    - Ethernet
    - Token-ring
    - Frame relay
    - FDDI
    - X.25
    - RS-232
    - v.35
- Lớp Internet: Lớp Internet là trung tâm của mô hình TCP / IP. Chúng truyền dữ liệu vào IP datagram và thực hiện định tuyến cho các datagram này dựa trên thông tin nguồn và đích trong tiêu đề. Các giao thức được sử dụng ở lớp này bao gồm:
    - Internet Protocol (IP)
    - Internet Control Message Protocol (ICMP)
    - Address Resolution Protocol (ARP)
    - Reverse Address Resolution Protocol (RARP)
- Lớp giao vận: Lớp này quản lý phiên giao tiếp giữa máy chủ. Trong quá trình vận chuyển dữ liệu, xác định mức độ dịch vụ và trạng thái kết nối. Tầng giao vận sử dụng các giao thức sau:
    - Transmission Control Protocol (TCP)
    - User Datagram Protocol (UDP)
    - Real-time Transport Protocol (RTP)

- Lớp ứng dụng: Lớp ứng dụng kết hợp các chức năng của tầng ứng dụng, trình bày và giao vận. Lớp này định nghĩa cách máy chủ lưu trữ giao diện chương trình với các dịch vụ lớp giao vận cũng như ứng dụng giao thức liên quan của chúng. Một số giao thức trong lớp này như sau:
    - Simple Mail Transfer Protocol (SMTP)
    - HTTP
    - FTP
    - Telnet
    - Simple Network Management Protocol (SNMP)
    - DNS
    - Trivial File Transfer Protocol (TFTP)
    - X-Windows

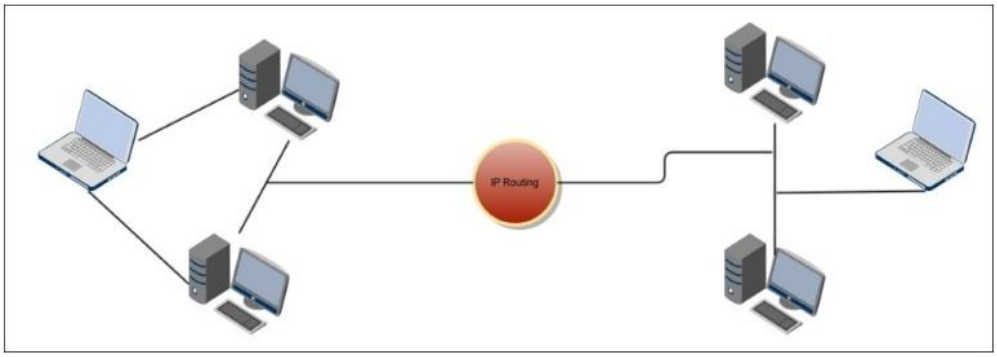
Hình ảnh sau đây mô tả cả hai mô hình ở dạng hình ảnh. Nó cũng cho thấy mối liên hệ giữa chúng:



Hiểu khái niệm kết nối giữa mạng / Internet

Năm 1966, Defense Advanced Research Project Agency Network, đã thực hiện một mạng lưới nghiên cứu về mạng. Bao gồm kết nối một số mạng máy tính dựa trên các giao thức khác nhau.

Điều này đã đặt ra một vấn đề duy nhất là phải xác định một giao thức kết nối chung của các giao thức local. Giao thức Internet (IP) đóng vai trò này bằng cách xác định địa chỉ duy nhất cho một thiết bị mạng và máy chủ. Sơ đồ sau mô tả sự kết nối này của các thiết bị sử dụng định tuyến IP:



Internet Protocol (IP)

Bất cứ khi nào chúng ta thấy một người lạ mà chúng ta muốn nói chuyện, sẽ luôn có ích nếu chúng ta sử dụng ngôn ngữ. Trong thế giới máy tính, ngôn ngữ giao tiếp được gọi là giao thức. IP là một trong những ngôn ngữ mà nhiều máy tính sử dụng để giao tiếp với nhau như một phần của mô hình kiến trúc lớp.

Phía trên của IP, có TCP, UDP và một số thứ khác.

Có hai phiên bản của IP đang được sử dụng, như sau:

- Internet Protocol version 4 (IPv4)
- Internet Protocol version 6 (IPv6)

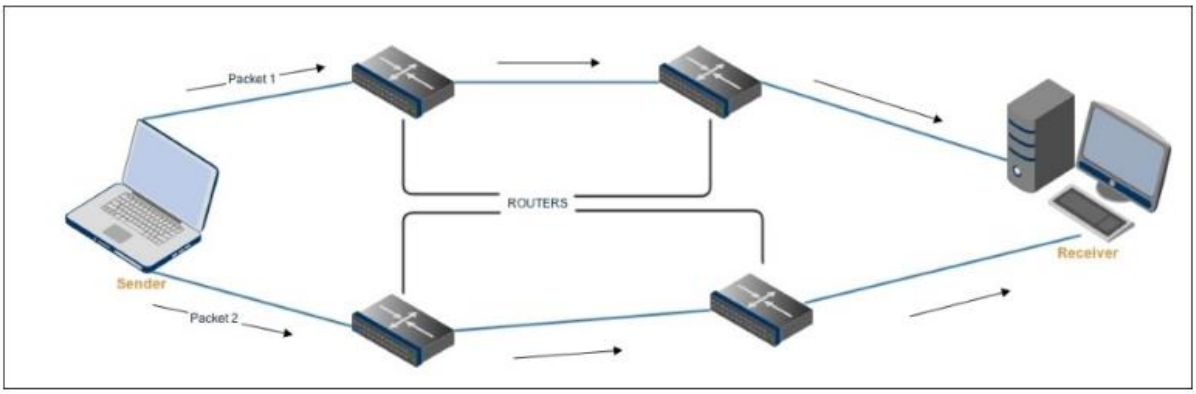
Giao thức Internet có hai chức năng chính sau:

- Chia luồng dữ liệu thành các gói kích thước tiêu chuẩn tại nguồn và sau đó đặt chúng cùng nhau một lần nữa theo đúng thứ tự tại điểm đến.
- Hướng dẫn hoặc định tuyến gói thông qua một số mạng trung gian, bắt đầu từ địa chỉ IP của thiết bị nguồn đến địa chỉ IP của thiết bị đích.

Làm thế nào nó hoạt động?

Nó phân tách hoặc chia nhỏ dữ liệu ban đầu (sẽ được gửi) thành các datagram. Mỗi datagram sẽ có một tiêu đề, bao gồm địa chỉ IP và số cổng của đích. Datagram sau đó được gửi đến các cổng được chọn, nghĩa là các bộ định tuyến IP. Các bộ định tuyến này được kết nối với mạng cục bộ và mạng lưới nhà cung cấp dịch vụ IP cùng một lúc. Các bộ định tuyến bắt đầu quá trình chuyển tiếp, trong đó các datagram được chuyển từ cổng này sang cổng khác cho đến khi chúng đến đích cuối cùng.

Sơ đồ sau minh họa khái niệm này theo cách dễ hiểu:



Bất cứ khi nào hai máy chủ liên lạc với nhau bằng giao thức Internet, không có cần cho một kết nối liên tục. Một máy chủ gửi dữ liệu cho người khác thông qua gói dữ liệu. Mỗi tiêu đề gói chứa các địa chỉ đích nguồn cũng như chuỗi số và được coi là một đơn vị dữ liệu độc lập. TCP có trách nhiệm đọc các tiêu đề gói và đặt các gói theo đúng trình tự để tin nhắn có thể đọc được.

Ngày nay, phiên bản IP được sử dụng rộng rãi nhất là IPv4. Tuy nhiên, IPv6 cũng đang bắt đầu được hỗ trợ. IPv6 được giới thiệu khi nhận ra rằng các địa chỉ IPv4 đang sắp cạn kiệt. Kết quả là sự gia tăng theo cấp số nhân của số lượng

thiết bị được kết nối với Internet trong dự đoán cạn kiệt địa chỉ IPv4. IPv6 cung cấp địa chỉ dài hơn nhiều và cũng có khả năng nhiều người dùng Internet hơn. IPv6 bao gồm các khả năng của IPv4 và bất kỳ máy chủ nào có thể hỗ trợ các gói IPv6 cũng có thể hỗ trợ các gói IPv4.

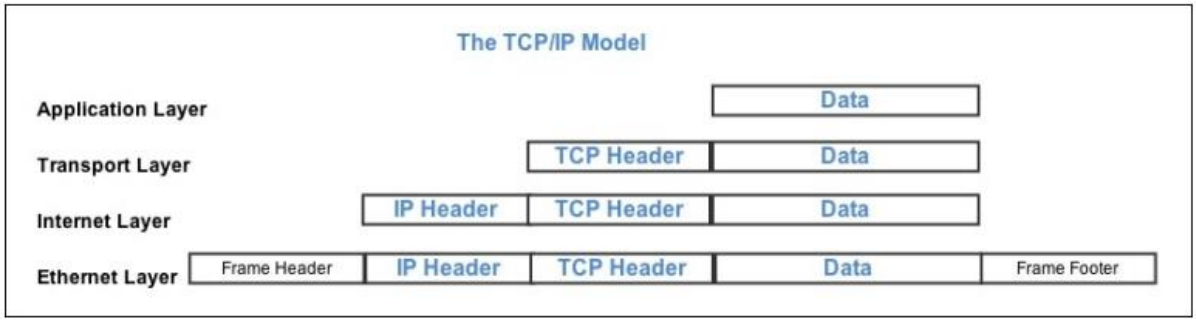
Cấu trúc của gói IP

Chúng ta hãy xem cấu trúc sau của gói IP:

- Các giới hạn và chức năng của IP được xác định bởi các trường ở đầu gói. Đây được gọi là tiêu đề khung.
- Các trường địa chỉ nguồn và đích có 32 bit được phân bổ để mã hóa dữ liệu của chúng.
- Thông tin bổ sung khác nhau, chẳng hạn như tổng chiều dài gói tính bằng byte, được mã hóa trong 16 byte trong phần còn lại của tiêu đề.

Thông thường, tầng ứng dụng sẽ gửi dữ liệu được truyền tới tầng giao vận. Tầng giao vận thêm một tiêu đề và gửi nó đến tầng Internet. Tầng internet thêm tiêu đề riêng của nó vào đây và gửi nó đến tầng vật lý truyền tải dưới dạng một datagram IP. Tầng mạng thêm tiêu đề khung riêng của nó và chân trang và sau đó truyền qua mạng vật lý.

Ở đầu kia, khi nhận được datagram, quá trình này bị đảo ngược và các tiêu đề bị tước bỏ khi dữ liệu di chuyển từ tầng này sang tầng khác. Sơ đồ sau đại diện cho cách các tiêu đề được thêm và xóa khi chúng ta di chuyển từ tầng này sang tầng khác:



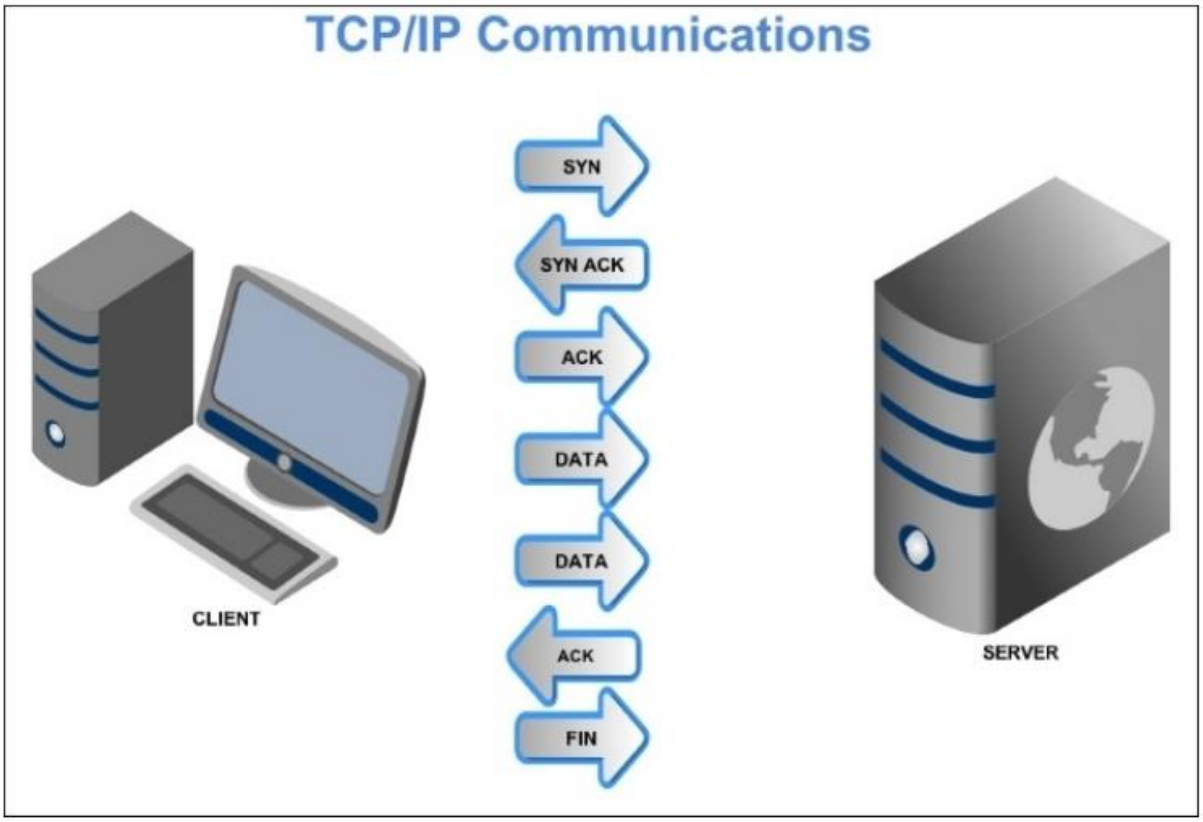
Tiêu đề datagram khi chúng ta di chuyển từ tầng này sang tầng khác

Transmission Control Protocol (TCP)

Gói IP là một dịch vụ cơ bản không đảm bảo an toàn. TCP khắc phục điều này bằng cách thêm các yếu tố sau:

- Phát hiện lỗi
- Truyền dữ liệu an toàn
- Đảm bảo rằng dữ liệu được nhận theo đúng thứ tự

Trước khi gửi dữ liệu, TCP yêu cầu các máy tính thiết lập kết nối với nhau:



Truyền tải TCP / IP

Trong khi IP bị giới hạn trong việc gửi các luồng dữ liệu 64 kb, các luồng dữ liệu lớn có thể được gửi dưới dạng một luồng dữ liệu lớn sử dụng TCP. TCP thực hiện điều này bằng cách chia luồng dữ liệu thành riêng gói dữ liệu. Mỗi gói được đánh số và số thứ tự của nó được lưu trong tiêu đề. Khi đến nơi, các gói khác nhau này được ghép lại bằng cách sử dụng trình tự và trình tự số xác nhận. TCP chỉ định số cổng. Điều này cải thiện qua IP. Mỗi máy TCP / IP có thể giao tiếp bằng 65.536 cổng khác nhau hoặc ổ cắm.

Tất cả dữ liệu trong gói TCP được kèm theo một tiêu đề. Tiêu đề chứa thông tin liên quan đến cổng nguồn, cổng đích, số thứ tự, xác nhận chuỗi số, và một số dữ liệu tiêu đề lẫn lộn với nhau.

Giao thức gói dữ liệu người dùng (UDP)

Tương tự như TCP, UDP cũng được xây dựng trên đỉnh (lớp trên cùng) IP. Nó có cùng giới hạn kích thước gói IP là 64 kb . Tuy nhiên, nó cho phép xác định số cổng, Điều này cung cấp 65.536 cổng khác nhau, giống như TCP. Do đó, mỗi máy có hai bộ 65.536 cổng: một cho TCP và một cho UDP.
Sự khác biệt giữa hai loại này: UDP là giao thức không có kết nối, không có bất kỳ phương tiện phát hiện lỗi nào. Nó chỉ cung cấp hỗ trợ cho việc truyền dữ liệu từ đầu này sang đầu kia mà không có bất kỳ xác minh nào. Vì nó không thực hiện thêm bất kỳ xác minh nào, UDP rất nhanh. Đây là tính năng chính của nó và nó cực kỳ hữu ích trong việc gửi dữ liệu nhỏ và lặp đi lặp lại ở tốc độ rất cao. Một số ví dụ về điều này là truyền phát âm thanh và video, trò chơi, thông tin thời gian được truyền phát liên tục, v.v.

Giao thức ứng dụng Internet

Lớp trên cùng của TCP / IP là lớp ứng dụng. Tài liệu định nghĩa của Lực lượng đặc nhiệm kỹ thuật Internet (IETF) cho lớp ứng dụng trong bộ giao thức Internet là RFC 1123. Vai trò của lớp ứng dụng là hỗ trợ các ứng dụng mạng bằng các giao thức ứng dụng.
Một số giao thức ứng dụng bao gồm:

- Telnet: Đây là giao thức dựa trên văn bản cho phép người dùng thực hiện điều khiển từ xa đăng nhập vào máy tính khác.
- Giao thức truyền tệp (FTP): Đây là để truyền tệp.
- SMTP: để vận chuyển thư điện tử.
- DNS: để hỗ trợ mạng.
- SNMP: dành cho quản lý máy chủ từ xa.
- Giao thức truyền siêu văn bản (HTTP).
- Giao thức truyền tin tức mạng (NNTP): Điều này cho phép người dùng tạo các nhóm mới xung quanh các đối tượng cụ thể.

Các ứng dụng mới hơn cũng có thể sinh ra các giao thức ứng dụng bổ sung như BitTorrent, Bitcoin, eDonkey, v.v.

Hiểu biết về an ninh mạng

Chúng ta sống trong một thế giới của mạng có dây (cũng có thể là mạng không dây), ngày càng kết nối với nhau. Các mạng được kết nối này là đặc quyền của hầu hết các dữ liệu trên thế giới và có nguy cơ cao.

Ngày nay, chúng ta càng kết nối với nhau, chúng ta càng có nhiều nguy cơ. Với các cuộc tấn công ngày càng tinh vi trở nên tự động, dễ dàng có sẵn và có thể sử dụng được bởi hầu hết các tội phạm cấp thấp, mối đe dọa đối với tài nguyên của chúng ta luôn ở mức cao nhất mọi thời đại. Các kỹ thuật ẩn danh tiến hóa và tinh vi giúp làm cho mọi thứ trở nên phức tạp hơn. Tội phạm thường chạy theo đồng tiền. Các cuộc tấn công được tập trung và nhắm mục tiêu nhiều hơn với sự ưu tiên của nỗ lực được hướng tới các mục tiêu có thể dẫn đến một khoản tiền. Hãy cùng xem các loại mối đe dọa tồn tại.

Các loại mối đe dọa

Khi chúng ta kết nối mạng của chúng ta với thế giới bên ngoài (tôi biết, tôi biết, chúng ta phải!), chúng ta giới thiệu khả năng người ngoài cố gắng khai thác mạng của chúng ta, đánh cắp dữ liệu của chúng ta, lây nhiễm hệ thống của chúng ta bằng virus và Trojan hoặc làm quá tải máy chủ của chúng ta, do đó tác động và cản trở hiệu suất của chúng ta.
Tuy nhiên, nếu mạng của chúng ta bị ngắt kết nối với thế giới bên ngoài, các mối đe dọa vẫn sẽ tồn tại. Trên thực tế, hầu hết các khảo sát và nghiên cứu (như đã đề cập trước đó) chỉ ra một thực tế không thể chối cãi rằng hầu hết các mối đe dọa (trên 50%) là do các hoạt động có chủ ý hoặc vô ý được thực hiện bởi những người trong cuộc (những người thuộc về nội bộ). Mặc dù hiếm khi có thể cô lập hoặc ngăn cách một mạng lưới kinh doanh với thế giới bên ngoài, ngay cả khi chúng ta làm như vậy, không có gì đảm bảo rằng nó sẽ đảm bảo an ninh mạng. Dựa trên sự hiểu biết này, chúng ta phải xem xét các mối đe dọa bên trong và bên ngoài.

Các mối đe dọa nội bộ

Nhìn lại lịch sử, chúng ta sẽ thấy nhiều ví dụ đáng chú ý về toàn bộ vương quốc bị thua cuộc do hành động của những nội gián bên trong. Thông tin có giá trị như các tuyến đường ẩn để tiếp cận phía sau một đội quân (sân sau), loại, điểm mạnh và điểm yếu của hệ thống phòng thủ (quét và lỗ hổng), và mã truy cập và mật khẩu (mở vừng) khi bị rò rỉ cho kẻ thù có thể gây ra tổn thất không thể khắc phục. Vương quốc và tập đoàn có thể sụp đổ. Tôn Tử, chiến lược gia và tướng quân Trung Quốc cổ đại, trong chuyên luận võ thuật của ông, Nghệ thuật chiến tranh, khuyến cáo mạnh mẽ về việc sử dụng người trong cuộc để giành chiến thắng trong các trận chiến. Ý kiến của ông ấy về cách tốt nhất để chiến thắng một trận chiến là không đánh mà thắng.

Các mối đe dọa bắt nguồn từ bên trong mạng có xu hướng nghiêm trọng hơn nhiều so với các mối đe dọa bắt nguồn từ bên ngoài.

Giống như một kẻ thù vô danh trong các bức tường của tòa thành có thể gây chết người; tương tự, người nội bộ trong mạng lưới của bạn có thể rất nguy hiểm trừ khi được xác định và chứa rất nhanh.

Người trong cuộc thường có nhiều kiến thức về mạng, tài nguyên sẵn có và cấu trúc của nó. Họ đã được cấp một mức độ truy cập nhất định để có thể thực hiện công việc của họ. Các công cụ bảo mật mạng như tường lửa, hệ thống ngăn chặn xâm nhập (IPS), hệ thống phát hiện xâm nhập (IDS), v.v được triển khai ở ngoại vi của mạng và thường hướng ra ngoài và những người trong cuộc như vậy nằm dưới radar trong bối cảnh này.

Một người trong cuộc có thể đánh cắp thông tin theo nhiều cách công nghệ thấp. Đơn giản chỉ cần lắp ổ USB và sao chép dữ liệu ra khỏi mạng là một cách đánh cắp dữ liệu rất phổ biến. Việc ghi đĩa DVD với tổ chức sở hữu trí tuệ của tổ chức và đi ra khỏi cơ sở với điều này bị mắc kẹt trong ổ đĩa DVD máy tính xách tay xảy ra khá thường xuyên. Một số kẻ thông minh sao chép dữ liệu vào thẻ nhớ USB và sau đó xóa nó để khi được kiểm tra, họ có thể chứng minh rằng thiết bị USB trống và khi về đến nhà, họ có thể khôi phục dữ liệu bằng các công cụ khôi phục miễn phí. Một người trong cuộc có thể khá nguy hiểm; tuy nhiên, khi có nhiều người trong cuộc làm việc song song, tình hình có thể khá nghiêm trọng. Những mối đe dọa này cần được giải quyết và giảm thiểu nhanh chóng để ngăn chặn thiệt hại đáng kể.

Các mối đe dọa bên ngoài

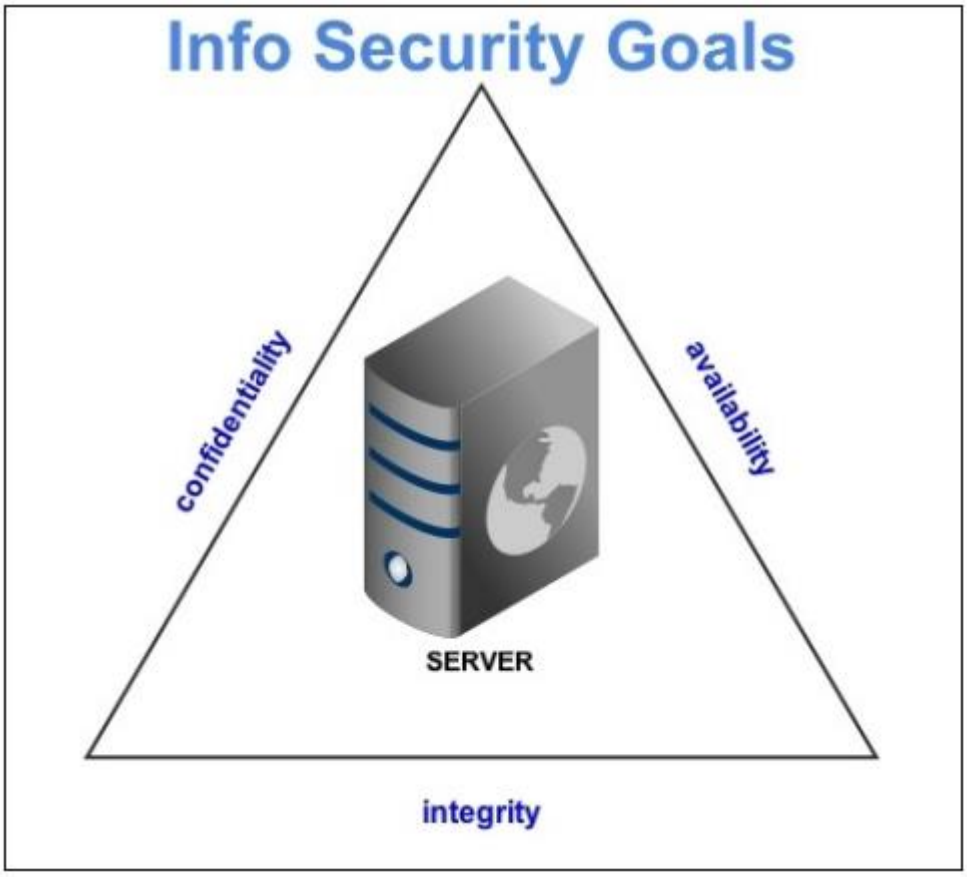
Thông thường, những kẻ tấn công bên ngoài không có kiến thức chuyên sâu về mạng của bạn. Khi họ bắt đầu, họ không có thông tin đăng nhập hoặc truy cập để vào mạng. Sau khi xác định được mục tiêu tiềm năng, bước đầu tiên là tiến hành trinh sát trên mạng. Để làm điều này, họ thực hiện quét ping. Điều này giúp xác định các địa chỉ IP phản hồi ping và có thể truy cập từ bên ngoài. Khi các địa chỉ IP này được xác định, quá trình quét cổng được thực hiện. Mục tiêu là xác định các dịch vụ mở trên các địa chỉ IP này. Hệ điều hành (HĐH) được lấy dấu vân tay để hiểu về kiểu dáng, kiểu máy và bản dựng được triển khai. Điều này giúp kẻ tấn công xác định các lỗ hổng chưa được vá có thể. Người ngoài sẽ xác định và khai thác lỗ hổng đã biết để thỏa hiệp bất kỳ một trong các dịch vụ được phát hiện trước đó trên máy chủ. Khi kẻ tấn công đã giành được quyền truy cập vào máy chủ, kẻ tấn công sẽ làm việc để leo thang các đặc quyền, che dấu vết và tạo ra các cửa hậu để truy cập không bị giám sát trong tương lai. Sau đó, họ sẽ sử dụng hệ thống này như một nền tảng để tấn công và thỏa hiệp các hệ thống khác trong mạng này và thế giới nói chung.

Mục tiêu an ninh mạng

Trong thế giới ngày nay, tốc độ cao, luôn luôn di chuyển, không có người đàn ông nào là một hòn đảo. Tương tự là trường hợp với các mạng công ty. Liên lạc và liên lạc liên tục với thế giới bên ngoài, các ứng dụng dựa trên đám mây, lưu trữ dữ liệu trên nền tảng đám mây và ngoại vi và BYOD dẫn đến một môi trường mạng ngày càng được kết nối. Một nền kinh tế toàn cầu phát triển mạnh về thông tin, công nghệ tiên tiến cho phép giao dịch liền mạch và nhu cầu liên tục của con người để truy cập thông tin trực tuyến là những yếu tố dẫn đến rủi ro bảo mật cao hơn.
Ngày nay, người ta có thể giả định một cách an toàn rằng hầu hết các mạng công ty được kết nối với các mạng khác.
Các mạng này chạy các giao thức dựa trên tiêu chuẩn.
Các mạng này cũng sẽ có một số ứng dụng, có thể có các giao thức độc quyền.
Vì các ứng dụng như vậy được đặt ra, trọng tâm của các nhà phát triển là nhiều hơn về chức năng và ít bảo mật hơn. Hơn nữa, không có hệ thống vá lỗ hổng thường xuyên trong các ứng dụng này.
Vô số thiết bị được kết nối và các ứng dụng đa dạng trong mạng công ty khá phức tạp và khối lượng của chúng không ngừng tăng lên

Từ góc độ an ninh mạng, các mục tiêu chính như sau:

- Bảo mật
- Toàn vẹn
- Sẵn sàng



Mục tiêu an ninh mạng

Tính bảo mật

Dữ liệu cư trú trên các mạng là huyết mạch của bất kỳ tổ chức nào. Khía cạnh bảo mật của an ninh mạng liên quan đến việc giữ dữ liệu riêng tư.
Điều này đòi hỏi phải hạn chế quyền truy cập vật lý vào các thiết bị và thành phần được nối mạng cũng như truy cập logic vào dữ liệu nút và lưu lượng mạng.
Để làm điều này, các quản trị viên mạng đã thiết lập tường lửa và hệ thống phát hiện và ngăn chặn xâm nhập. Danh sách kiểm soát truy cập (ACL) ngăn chặn truy cập trái phép vào tài nguyên mạng. Lưu lượng truy cập mạng được mã hóa ngăn chặn mọi rò rỉ dữ liệu do kẻ chặn lưu lượng truy cập gây ra. Thông tin cụ thể, chẳng hạn như tên người dùng và mật khẩu, được yêu cầu để truy cập tài nguyên mạng.
Những tiết lộ của Snowden, là một ví dụ về việc vi phạm mục tiêu bảo mật của an ninh mạng. Các tiêu đề gần đây liên quan đến rò rỉ dữ liệu tại Sony Pictures là một ví dụ rõ ràng khác.

Tính toàn vẹn

Mạng có dữ liệu chuyển động. Nếu kẻ tấn công có quyền truy cập vào mạng, chúng sẽ có khả năng âm thầm sửa đổi / giả mạo lưu lượng sẽ gây ra, ít nhất, một sự hiểu lầm giữa những người giao tiếp và ở đầu kia của quang phổ, nó có thể gây ra không thể khắc phục gây hại cho người dân và các tổ chức.

Các ví dụ về vi phạm an ninh mạng ảnh hưởng đến mục tiêu toàn vẹn bao gồm:

Chặn các thông tin liên lạc liên quan đến thanh toán điện tử, sửa đổi chúng để phản ánh các chi tiết ngân hàng khác nhau và chuyển hướng thanh toán từ người gửi không nghi ngờ. Đây là một vấn đề phổ biến đang được quan sát trong những ngày này, đặc biệt là giữa các nhà xuất khẩu quy mô nhỏ và người mua của họ.

Một thực thể thuế của chính phủ đã có trang web của họ bị xâm phạm. Kẻ tấn công rất cẩn thận chỉ sửa đổi phần liên quan đến thuế suất. Những điều này đã giảm đáng kể. Kết quả là, chính phủ đã mất doanh thu đáng kể vì hầu hết các khoản chuyển tiền được thực hiện theo tỷ lệ được đăng trên trang web.

Một số tổ chức triển khai một giải pháp toàn vẹn dữ liệu để thực hiện xác thực nguồn gốc và xác minh rằng lưu lượng truy cập có nguồn gốc từ nguồn sẽ gửi nó.

Tính sẵn sàng

Dữ liệu ở phần còn lại và quá cảnh thực sự đang thực hiện một nhiệm vụ cho tổ chức. Miễn là dữ liệu hoặc thông tin này có thể truy cập được đối với người dùng được ủy quyền và xác thực, tác vụ có thể được thực hiện. Thời điểm một sự cố làm gián đoạn truy cập, ngăn người dùng thực hiện các tác vụ của họ, mục tiêu sẵn có của bảo mật mạng bị vi phạm.

Đã có một số ví dụ điển hình về sự thỏa hiệp sẵn có trong quá khứ, như được trình bày dưới đây:

Vào ngày 26 tháng 4 năm 2007, Estonia, một quốc gia nhỏ ở vùng Baltic đã trải qua một làn sóng tấn công từ chối dịch vụ (DoS). Những cuộc tấn công mạng này đã được phát động như một cuộc biểu tình phản đối chính phủ Estonia xóa bỏ tượng đài Chiến binh Đồng ở Tallinn. Điều này đã được dựng lên vào năm 1947 như là một tượng đài chiến tranh trong Thế chiến II của Liên Xô. Hiệu quả đã được cảm nhận trên một số tổ chức, bao gồm ngân hàng, chính phủ và các trường đại học, lấy tài nguyên mạng ngoại tuyến. Cuộc tấn công này kéo dài trong ba tuần và làm rung chuyển cả đất nước. Trên thực tế, một trong những hậu quả của cuộc tấn công này là sự hình thành chính sách của chính phủ Hoa Kỳ về chiến tranh mạng.

Một ví dụ rất phổ biến đã được thể hiện trong bộ phim Die Hard 4, Live Live hoặc Die Hard, trong đó siêu cảnh sát, John McClane đảm nhận một tên khủng bố trên Internet, người đã làm việc tấn công và đóng cửa một cách có hệ thống chính phủ, giao thông và kinh tế Hoa Kỳ . Bộ phim này được công nhận rộng rãi khi thêm từ Fire Sale vào từ vựng của người bình thường trong bối cảnh không gian mạng.

Ngày nay, một số cuộc tấn công phổ biến nhất ảnh hưởng đến mục tiêu sẵn có là tấn công lũ lụt, tấn công logic / phần mềm, ném bom thư, tấn công DoS, tấn công DoS tình cờ và tấn công từ chối dịch vụ phân tán (DDoS)

Mạng được khai thác như thế nào?

Giống như tất cả con người đều có điểm yếu, mạng cũng có điểm yếu. Chúng được gọi là lỗ hổng. Lỗ hổng, trong một hệ thống thông tin, là một điểm yếu mà kẻ tấn công tận dụng để có quyền truy cập trái phép vào hệ thống hoặc dữ liệu của nó.

Cách thức hoạt động thông thường để tận dụng lỗ hổng mạng là viết chương trình thực hiện việc này. Những loại chương trình này được gọi là khai thác. Hầu hết các khai thác là độc hại trong tự nhiên. Như tên cho thấy, một khai thác có nghĩa là khai thác điểm yếu của hệ thống.
Lỗ hổng có thể có nhiều loại. Một số ví dụ được hiển thị như sau:

- Các lỗ hổng vật lý hoặc thiên tai (như sóng thần ở Đông Nam Á)
- Lỗ hổng thiết kế mạng Lỗ hổng cấu hình mạng Lỗ hổng giao thức
- Lỗ hổng ứng dụng
- Các lỗ hổng được nhắm mục tiêu như phần mềm độc hại
- Quy trình vận hành tiêu chuẩn / kiểm soát lỗ hổng
- Lỗ hổng bảo mật vật lý
- Lỗ hổng của con người

Như chúng ta đều biết, một chuỗi chỉ mạnh bằng liên kết yếu nhất của nó. Trong trường hợp bảo mật mạng, liên kết yếu nhất thường là con người. Thống kê cho thấy một người trong cuộc thường tung ra nhiều cuộc tấn công nhất vào tài sản thông tin. Vì vậy, hầu hết các tổ chức thiết lập các kiểm soát để ngăn chặn lạm dụng nội bộ.

Dấu chân kỹ thuật số

Trong một khoảnh khắc, hãy để hồi tưởng lại về phần nguyên tắc trao đổi Locard. Để nhắc lại, về cơ bản nó cho thấy mọi liên hệ đều để lại dấu vết. Điều này có nghĩa là, trong bối cảnh kỹ thuật số, là tất cả các tương tác với hệ thống / mạng kỹ thuật số sẽ để lại một số loại vật phẩm / dữ liệu phía sau làm bằng chứng của sự kiện này. Những hiện vật này được gọi là dấu chân kỹ thuật số. Chúng có hai loại sau:

- Private
- Active

Dấu chân kỹ thuật số thụ động được hệ thống tạo ra mà không có kiến thức của người dùng, chẳng hạn như trong trường hợp dán mật khẩu từ tệp vào bằng chứng ứng dụng hoặc bản sao có thể được tìm thấy trong bộ nhớ dễ bay hơi. Cookies là một ví dụ khác về điều này.
Người dùng tạo ra các dấu chân kỹ thuật số hoạt động một cách có chủ ý, chẳng hạn như trong trường hợp bài đăng trên Facebook, gửi e-mail hoặc lưu trữ và truyền hình ảnh.
Chúng thường tồn tại và có thể được phục hồi từ các mục sau:

- Bộ nhớ thiết bị
- Dung lượng đĩa bao gồm nhật ký
- Chụp lưu lượng truy cập mạng

Tóm lược

Hành trình của chúng ta vào vương quốc của pháp y mạng đã bắt đầu. Chúng ta bắt đầu bằng cách xác định các đặc điểm sẽ khiến chúng ta trở thành 007 trong thế giới pháp y mạng. Điều này được theo sau bằng cách tìm hiểu về phương pháp TAARA cho các cuộc điều tra. chúng ta cũng đã tìm hiểu về các mối đe dọa khác nhau đối với một doanh nghiệp trong khi củng cố các nguyên tắc cơ bản kỹ thuật của chúng ta. Đến cuối chương, chúng ta hiểu sâu hơn về an ninh mạng cũng như pháp y mạng.

Trong chương tiếp theo, chúng ta sẽ tìm hiểu làm thế nào để xác định các nguồn chứng cứ khác nhau cần thiết cho một cuộc điều tra pháp y mạng. chúng ta cũng sẽ học cách thu thập và xử lý các bằng chứng một cách an toàn. Vậy hãy bắt đầu!!!