hái niệm an ninh mạng Cybersecurity

### ****Đối tượng bị tấn công****

Có thể là cá nhân, doanh nghiệp, các tổ chức chính phủ hoặc phi chính phủ, cơ quan nhà nước, thậm chí đối tượng có thể là cả một quốc gia. Tuy nhiên, đối tượng phổ biến nhất của các cuộc tấn công mạng là các doanh nghiệp. Đơn giản vì mục tiêu chính của những kẻ tấn công là vì lợi nhuận.

### ****Mục đích tấn công mạng****

Bên cạnh những mục đích phổ biến như trục lợi phi pháp, tống tiền doanh nghiệp, hiện thị quảng cáo kiếm tiền, thì còn tồn tại một số mục đích khác phức tạp và nguy hiểm hơn: cạnh tranh không lành mạnh giữa các doanh nghiệp, tấn công an ninh hoặc kinh tế của một quốc gia, tấn công đánh sập một tổ chức tôn giáo, v.v.

Ngoài ra, một số hacker tấn công mạng chỉ để mua vui, thử sức, hoặc tò mò muốn khám phá các vấn đề về an ninh mạng.

### ****Hacker là ai?****

Ban đầu, những kẻ tấn công mạng được gọi là Cyber-crime (tội phạm mạng), tuy nhiên công chúng thường biết đến họ dưới cái tên **“hacker”** (kẻ xâm nhập), ở Việt Nam gọi là **tin tặc**. Các hacker đều là những người có kiến thức cực kỳ chuyên sâu về an ninh mạng, khoa học máy tính, khoa học mật mã, cơ sở dữ liệu,…Thậm chí, kiến thức của hacker còn được đánh giá là sâu và rộng hơn các kỹ sư CNTT thông thường.

### ****Tấn công trung gian (Man-in-the-middle attack)****

Tấn công trung gian (MitM), hay **tấn công nghe lén**, xảy ra khi kẻ tấn công xâm nhập vào một giao dịch/sự giao tiếp giữa 2 đối tượng. Khi đã chen vào giữa thành công, chúng có thể đánh cắp dữ liệu của giao dịch đó.

Loại hình này xảy ra khi:

* Nạn nhân truy cập vào một mạng Wifi công cộng không an toàn, kẻ tấn công có thể “chen vào giữa” thiết bị của nạn nhân và mạng Wifi đó. Vô tình, những thông tin nạn nhân gửi đi sẽ rơi vào tay kẻ tấn công.
* Khi phần mềm độc hại được cài đặt thành công vào thiết bị, một kẻ tấn công có thể dễ dàng xem và điều chỉnh dữ liệu của nạn nhân.

## ****Giải pháp chống tấn công mạng****

### ****Đối với cá nhân****

* Bảo vệ mật khẩu cá nhân bằng cách: đặt mật khẩu phức tạp, bật tính năng bảo mật 2 lớp – xác nhận qua điện thoại,… Chi tiết tại: [3 kiểu Tấn công Password cơ bản & cách phòng chống](https://cystack.net/vi/resource/3-hinh-thuc-tan-cong-password-co-ban/)
* Hạn chế truy cập vào các điểm wifi công cộng
* Không sử dụng phần mềm bẻ khóa (crack)
* Luôn cập nhật phần mềm, hệ điều hành lên phiên bản mới nhất.
* Cẩn trọng khi duyệt email, kiểm tra kỹ tên người gửi để phòng tránh lừa đảo.
* Tuyệt đối không tải các file hoặc nhấp vào đường link không rõ nguồn gốc.
* Hạn chế sử dụng các thiết bị ngoại vi (USB, ổ cứng) dùng chung.
* Sử dụng một phần mềm diệt Virus uy tín.

### ****Đối với tổ chức, doanh nghiệp****

* [Xây dựng một chính sách bảo mật](https://cystack.net/vi/resource/xay-dung-chinh-sach-bao-mat-cho-doanh-nghiep/) với các điều khoản rõ ràng, minh bạch
* Lựa chọn các phần mềm, đối tác một cách kỹ càng. Ưu tiên những bên có cam kết bảo mật và cam kết cập nhật bảo mật thường xuyên.
* Tuyệt đối không sử dụng các phần mềm crack
* Luôn cập nhật phần mềm, firmware lên phiên bản mới nhất.
* Sử dụng các dịch vụ đám mây uy tín cho mục đích lưu trữ.
* Đánh giá bảo mật & Xây dựng một chiến lược an ninh mạng tổng thể cho doanh nghiệp, bao gồm các thành phần: [bảo mật website,](https://cystack.net/vi/resource/bao-mat-website/) bảo mật hệ thống máy chủ, mạng nội bộ, hệ thống quan hệ khách hàng (CRM), [bảo mật IoT](https://cystack.net/vi/resource/bao-mat-thiet-bi-iot/), bảo mật hệ thống CNTT – vận hành…
* Tổ chức các buổi đào tạo, [training kiến thức sử dụng internet an toàn cho nhân viên](https://cystack.net/vi/resource/lam-sao-de-nang-cao-y-thuc-bao-mat-cua-nhan-vien/).

# Tìm hiểu về tấn công Man in the middle

[07/05/2018](https://ssl.vn/tim-hieu-ve-tan-cong-man-in-the-middle.html) [Hoàng Tùng](https://ssl.vn/author/tunghv)

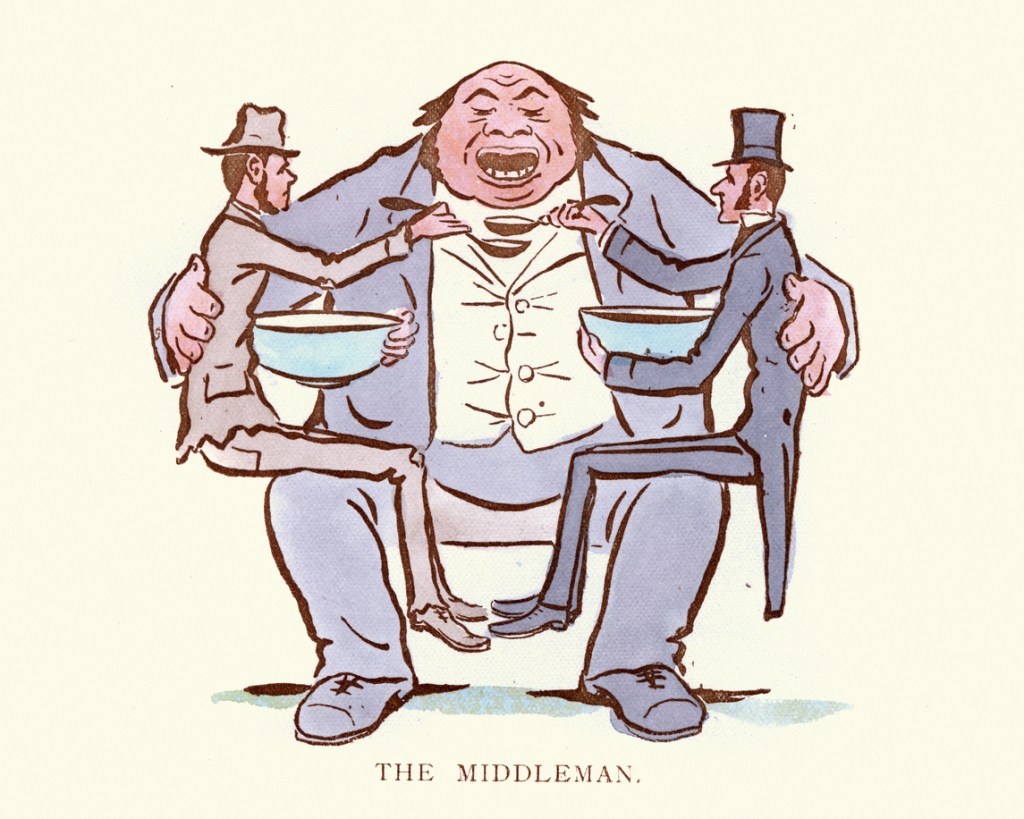


Bạn có thể đã nghe thuật ngữ ‘Man-in-the-middle (MiTM) Attack’ ? Có thể bạn đã mường tượng được phần nào về cách thức tấn công của nó. Nhưng bạn vẫn đang băn khoăn ‘Chính xác thì cuộc Man-in-the-middle là gì?’ Đúng? Hãy để chúng tôi giải thích cho bạn. Như đúng cái tên của nó, loại tấn công xảy ra khi có một thiết bị nằm ở giữa hai hệ thống giao tiếp và cố gắng để ngăn chặn việc chuyển giao thông tin liên tục. Nói một cách đơn giản, một cuộc tấn công MiTM là một phiên bản hiện đại của bugging.

Đầu tiên nhìn xung quanh bạn, nhìn vào chiếc smartphone của bạn, nhìn vào các ứng dụng trong đó, nhìn vào PC của bạn, nhìn vào những thiết bị thông minh kết nối với nhau, nhìn vào trang web bạn đang xem. Những thứ này có gì chung? Điều gì đang thúc đẩy tất cả những điều này phát triển? Câu trả lời sẽ là dữ liệu / thông tin. Cho dù đó là từ một máy tính khác, một máy chủ khác, một quốc gia khác – dữ liệu không biết giới hạn.

Thật không may, tất cả các chuyến đi này mang đến những câu hỏi không thể tránh khỏi về an ninh và riêng tư. Khi dữ liệu rời đi từ điểm cuối này đến điểm kết thúc khác, khoảng thời gian truyền dẫn là nơi kiểm soát nó bị mất phần nào. Khi kẻ tấn công tự đặt mình vào giữa điểm kết thúc và chặn và / hoặc tampers với dữ liệu này trong quá cảnh, nó được gọi là tấn công man-in-the-middle (MiTM). Theo thuật ngữ của công an thì nó tương tự nghe lén vậy.

Đúng vậy, khi bạn cố gắng nghe lỏm được cuộc trò chuyện giữa hai người mà họ không biết, nó giống như một cuộc tấn công **Man in the middle**.

Bạn đã thấy người đàn ông này? Không. Có lẽ là không.

Trong khi truyền dữ liệu đang diễn ra giữa một thiết bị (PC / Điện thoại) và máy chủ web, kẻ tấn công sử dụng các kỹ năng và công cụ của anh ta để đặt một thiết bị vào giữa hai điểm cuối và chặn dữ liệu. Trong khi hai bên tin rằng họ đang nói chuyện với nhau, nhưng thật sự họ đang liên lạc (và thông qua) thủ phạm.

Các cuộc tấn công này không chỉ diễn ra trong quá trình truyền thông giữa các thiết bị, mà còn có thể xảy ra ở bất cứ nơi nào hai hệ thống đang trao đổi dữ liệu.

## Man in the middle hoạt động như thế nào?

Khi nói đến các cuộc tấn công MiTM, không chỉ có một phương pháp duy nhất có thể gây ra thiệt hại – có bốn! Đó là Sniffing, Packet Injection, Session Hijacking và SSL Stripping. Hãy cùng tìm hiểu qua về các phương pháp này

* **Sniffing:** Sniffing hoặc Packet Sniffing là một kỹ thuật được sử dụng để nắm bắt các gói dữ liệu chảy vào và ra khỏi một hệ thống / mạng. Packet Sniffing trong mạng tương đương với việc nghe trộm trong điện thoại. Hãy nhớ rằng Sniffing là hợp pháp nếu được sử dụng đúng cách và nhiều doanh nghiệp làm điều đó vì mục đích bảo mật.
* **Packet Injection:** Trong kỹ thuật này, kẻ tấn công đưa các gói dữ liệu độc hại vào với dữ liệu thông thường. Bằng cách này, người dùng thậm chí không nhận thấy tệp / phần mềm độc hại vì chúng đến như một phần của luồng truyền thông hợp pháp. Những tập tin này rất phổ biến trong các cuộc tấn công trung gian cũng như các cuộc tấn công từ chối dịch vụ.
* **Gỡ rối phiên:** Bạn đã từng gặp lỗi “Phiên hoạt động đã hết hạn” chưa? Nếu bạn đã từng thực hiện thanh toán trực tuyến hoặc điền vào biểu mẫu, bạn sẽ biết thuật ngữ này. Thời gian giữa khi bạn đăng nhập vào tài khoản ngân hàng của bạn và đăng xuất khỏi tài khoản đó được gọi là một phiên. Các phiên này thường là mục tiêu của tin tặc vì chúng có khả năng chứa thông tin kín đáo. Trong hầu hết các trường hợp, một hacker thiết lập sự hiện diện của anh ta / cô ta trong phiên, và cuối cùng nắm quyền kiểm soát nó. Các cuộc tấn công này có thể được thực thi theo nhiều cách khác nhau.
* **Loại bỏ SSL:** SSL Stripping hoặc SSL Downgrade attack là một loài hiếm khi nói đến các cuộc tấn công MiTM, nhưng cũng là một trong những nguy hiểm nhất. Như chúng ta đều biết, chứng chỉ [SSL / TLS](https://ssl.vn/tim-hieu-ve-su-khac-nhau-giua-tls-va-ssl.html) giữ liên lạc của chúng tôi an toàn trực tuyến thông qua mã hóa. Trong các cuộc tấn công SSL, kẻ tấn công loại bỏ kết nối SSL / TLS và giao thức được chuyển từ HTTPS an toàn sang HTTP không an toàn.

## Làm thế nào để ngăn chặn các cuộc tấn công man-in-the-middle?

Hãy nhớ rằng những cuộc tấn công này không dễ dàng như việc tắt tai nghe của bạn, chúng có tính chất rất phức tạp. Bạn cần phải có một số kỹ năng về kĩ thuật và phải được hỗ trợ bởi các công cụ phù hợp.

Dưới đây là các thực tiễn được đề xuất của chúng tôi để bảo vệ chống lại các cuộc tấn công giữa người:

* Đảm bảo rằng các trang web bạn truy cập đã được cài [SSL](https://ssl.vn/tag/ssl)
* Trước khi nhấp vào email, hãy kiểm tra người gửi email
* Nếu bạn là quản trị viên trang web, bạn nên triển khai [HSTS](https://ssl.vn/tag/giao-thuc-hsts)
* KHÔNG mua hàng hoặc gửi dữ liệu nhạy cảm trên mạng Wi-Fi công cộng.
* Đảm bảo trang web của bạn không có bất kỳ nội dung hỗn hợp nào
* Nếu trang web của bạn đang sử dụng SSL, hãy đảm bảo bạn đã tắt giao thức SSL / TLS không an toàn. Bạn chỉ nên bật TLS 1.1 và TLS 1.2
* Không nhấp vào liên kết hoặc email độc hại
* Không tải xuống nội dung vi phạm bản quyền
* Bảo mật mạng gia đình / công việc của bạn
* Có các công cụ bảo mật thích hợp được cài đặt trên hệ thống của bạn