INDUSTRIAL UNIVERSITY OF HOCHIMINH CITY

Chương 2:
CÁC MỐI ĐE DỌA ĐẾN AN TOÀN THÔNG TIN

THREATS TO INFORMATION SECURITY

Nội dung

- Khái niệm cơ bản
- Một số mối đe dọa
- Các tấn công và cách phòng chống

1. Khái niệm cơ bản

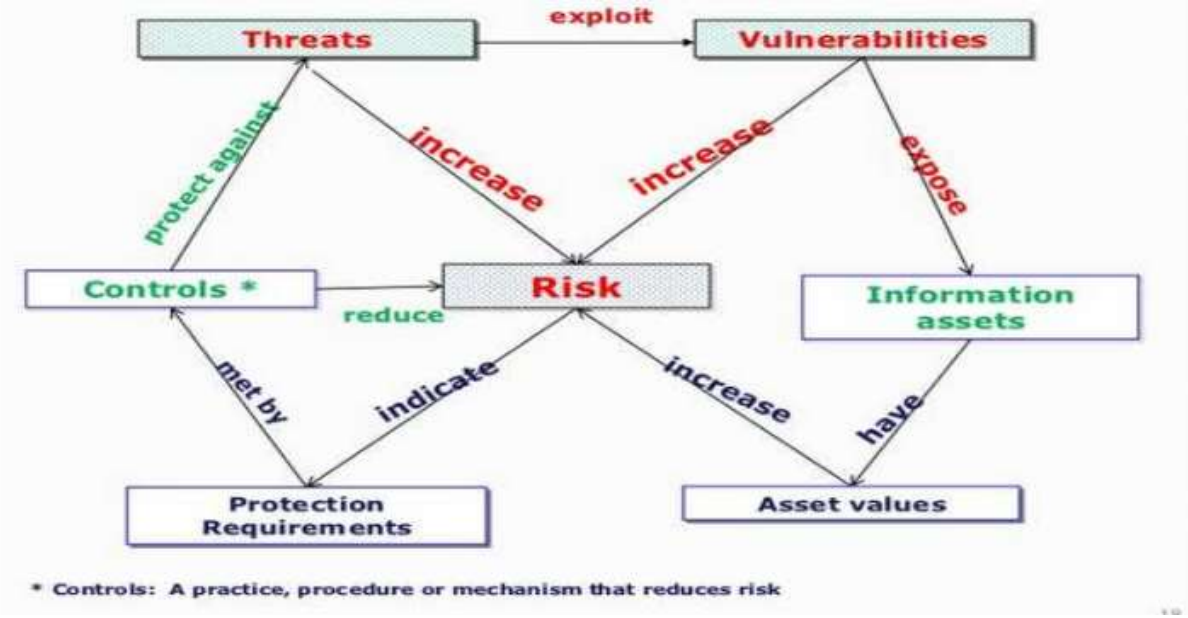
Lỗ hổng – Mối đe dọa – Rủi ro

- Vulnerability (lỗ hổng):
  - một điểm yếu trong tổ chức, hệ thống IT, hoặc mạng mà có thể được khám phá bởi mối đe dọa.
- Threat (mối nguy/mối đe dọa)
  - một cái gì đó mà có thể gây thiệt hại đến tổ chức, hệ thống IT hoặc hệ thống mạng.
- Risk (rủi ro)
  - một khả năng mà một mối đe dọa khai thác lỗ hổng trong tài sản và gây ra nguy hại hoặc mất mát đến tài sản

1. Khái niệm cơ bản

Lỗ hổng – Mối đe dọa – Rủi ro

- Mối quan hệ giữa lỗ hổng, mối đe dọa, rủi ro



1. Khái niệm cơ bản

- Tấn công (Attacks)
  - Hành động khai thác lỗ hổng (tức là một điểm yếu được xác định) trong hệ thống kiểm soát
  - Thực hiện tấn công nhằm gây thiệt hại hoặc ăn cắp thông tin của tổ chức hoặc cá nhân

1. Khái niệm cơ bản

- Để bảo vệ thông tin của tổ chức, bạn cần biết điều gì?
  - Thông tin nào cần được bảo vệ
  - Các hệ thống lưu trữ, truyền tải và xử lý
  - Biết những mối đe dọa (threats) mà bạn đối mặt
  - Nắm bắt được các mối đe dọa đến con người, ứng dụng, dữ liệu và hệ thống thông tin

2. Phân loại các mối đe dọa

- Hành động vô ý (Inadvertent Acts)
- Hành động cố ý (Delierate Acts)
- Thảm họa tự nhiên (Natural Disaster)
- Lỗi về kỹ thuật (Technical Failures)
  - Lỗi về phần cứng
  - Lỗi về phần mềm
- Lỗi về quản lý (Management)
  - Không xây dựng hoặc thực thi chính sách ATTT
  - Không cập nhật diễn biến và công nghệ

https://www.slideshare.net/swapneel07/threats-to-information-security

Hành động vô ý (Inadvertent Acts)

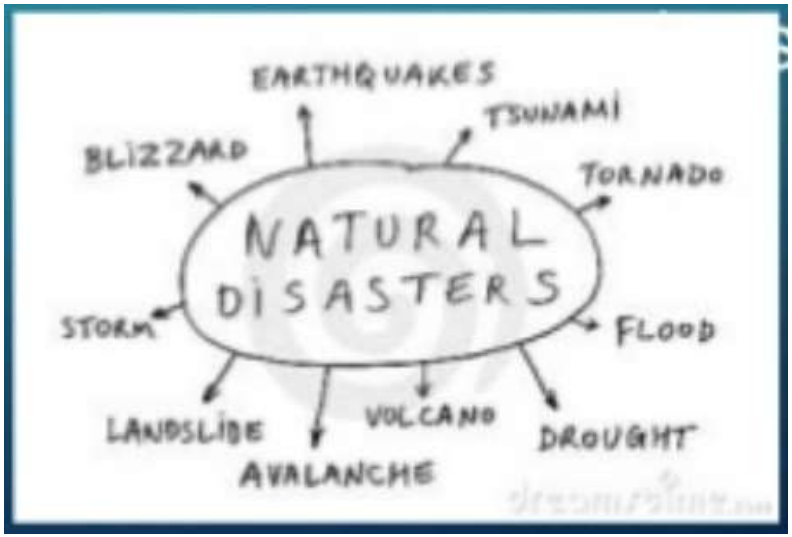
- Là những hành động mà xảy bởi lỗi nào đó, người thực hiện không cố ý
- Kẻ tấn công không có ác ý
- Các hành động lỗi của con người, sai lệch từ chất lượng dịch vụ, truyền thông lỗi là các hành động vô ý.
- Nhân viên hoặc người dùng hệ thống cũng là mối đe dọa nội bộ hệ thống

Hành động cố ý (Delierate Acts)

- Là các hành động được thực hiện bởi người của tổ chức làm tổn hại đến thông tin
- Các kẻ tấn công có một ý định xấu và muốn ăn cắp hoặc phá hủy dữ liệu
- Bao gồm các hành động như gián điệp, hacking, Cracking

Thảm họa tự nhiên (Natural Disaster)

- Sức mạnh của thiên nhiên là rất nguy hiểm bởi vì chúng là điều không ngờ và xuất hiện đôi khi không có cảnh báo
- Chúng phá vỡ cuộc sống của con người nhưng cũng gây nguy hại đến thông tin được lưu vào trong máy tính
- Các mối đe dọa này có thể tránh nhưng chúng ta phải có những biện pháp phòng ngừa cần thiết



Lỗi về kỹ thuật (Technical Failures)

- Chia làm 2 loại:
  - Lỗi về phần cứng
  - Lỗi về phần mềm
- Lỗi về phần cứng:
  - Nó xảy ra khi nhà sản xuất phân phối thiết bị có lỗi mà nhà sản xuất có thể biết hoặc không biết
- Lỗi phần mềm kỹ thuật:
  - Những lỗi này có thể khiến hệ thống hoạt động theo cách không mong muốn hoặc bất ngờ. Một số trong số này là không thể phục hồi trong khi một số xảy ra định kỳ

Lỗi trong quản lý (Management Failure)

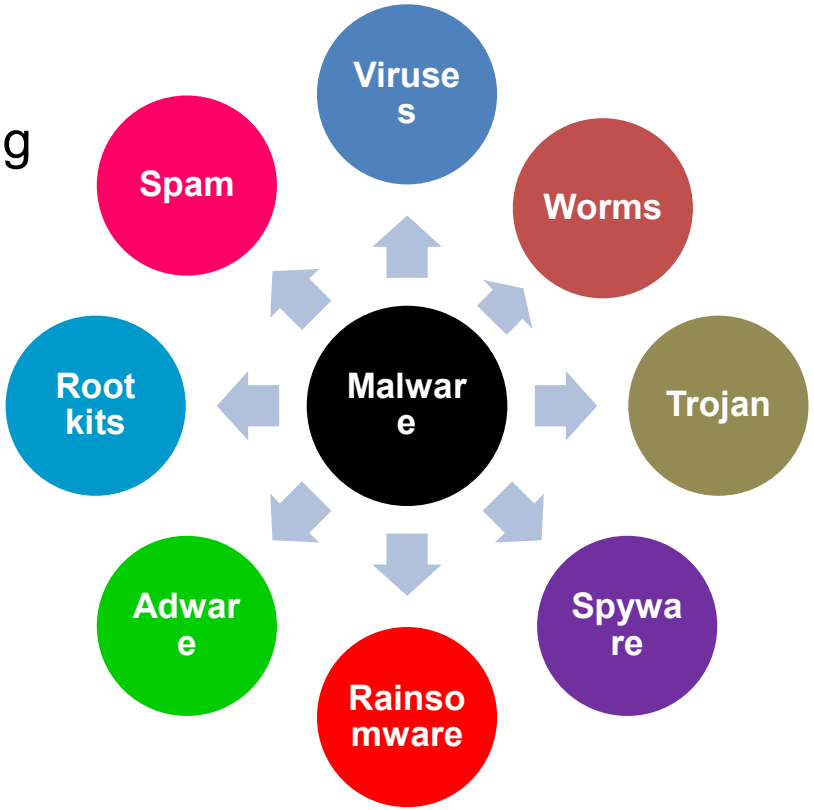
- Quản lý phải luôn luôn cập nhật về diễn biến và công nghệ hiện tại
- Kế hoạch phù hợp phải được thực hiện bởi nhà quản lý để bảo vệ tốt thông tin
- Các chuyên gia CNTT cũng phải giúp ban quản lý trong việc bảo vệ thông tin, bằng cách hỗ trợ ban quản lý nâng cao công nghệ mới nhất

3. Các cách tấn công và cách phòng chống

1. Mã độc
2. Tấn công Password
3. Backdoor
4. Denial-of-service (DoS)
5. Distributed denial-of-service (DDoS)
6. Spam
7. Mail bombing
8. Spoofing
9. Man-in-the-middle
10. Sniffers
11. Social engineering

3.1 Mã độc (Malware)

- Đó là bất cứ phần mềm độc hại được thiết kế để làm nguy hại đến một máy tính mà không có sự đồng thuận của người dùng
- Ví dụ



3.1 Mã độc (Malware)

Bảo vệ chống lại mã độc

- Đảm bảo rằng bạn đã cập nhật hệ điều hành và các phần mềm chống mã độc
- Không sử dụng phần mềm không có bản quyền hoặc tải các tập tin từ những nguồn không đáng tin cậy.
- Thực hiện quét (scans) ổ đĩa cứng thường xuyên
- Sử dụng phần mềm có bản quyền

3.2 Tấn công Password

- Password là gì?
- Có 3 dạng tấn công Password phổ biến:
  - **Brute Force Attack** (tấn công dò mật khẩu)
  - **Dictionary Attack** (tấn công từ điển)
  - **Key Logger Attack** (tấn công Key Logger)

3.2 Tấn công Password

- **Brute Force Attack** (tấn công dò mật khẩu)
  - Kẻ tấn công sử dụng một công cụ mạnh mẽ, có khả năng thử nhiều username và password cùng lúc (từ dễ đến khó) cho tới khi đăng nhập thành công.
  - VD: đặt mật khẩu đơn giản như 123456, password123, daylamatkhau,… rất dễ bị tấn công brute force.

3.2 Tấn công Password

- **Dictionary Attack** (tấn công từ điển)
  - Là một biến thể của Brute Force Attack
  - Tuy nhiên kẻ tấn công nhắm vào các từ có nghĩa thay vì thử tất cả mọi khả năng.
  - Nhiều người dùng có xu hướng đặt mật khẩu là những từ đơn giản và có ngữ nghĩa. VD: motconvit, iloveyou,… Đây là lý do khiến Dictionary Attack có tỉ lệ thành công cao hơn.

3.2 Tấn công Password

- **Key Logger Attack** (tấn công Key Logger)
  - Kẻ tấn công lưu lại lịch sử các phím mà nạn nhân gõ, bao gồm cả ID, password hay nhiều nội dung khác.
  - Kẻ tấn công cần phải sử dụng một phần mềm độc hại (malware) đính kèm vào máy tính (hoặc điện thoại) nạn nhân, phần mềm đó sẽ ghi lại tất cả những ký tự mà nạn nhân nhập vào máy tính và gửi về cho kẻ tấn công. Phần mềm này được gọi là Key Logger.
  - Nguy hiểm hơn 2 cách tấn công trên, do việc đặt mật khẩu phức tạp không giúp ích gì trong trường hợp này.

3.2 Tấn công Password

- 3 tấn công trên chỉ là các dạng tấn công mật khẩu trực tiếp.
- Ngoài ra, kẻ tấn công có thể tấn công gián tiếp thông qua việc:
  - Lừa đảo người dùng tự cung cấp mật khẩu (Tấn công giả mạo Phishing);
  - Tiêm nhiễm Malware
  - Tấn công vào cơ sở dữ liệu – kho lưu trữ mật khẩu người dùng của các dịch vụ…

3.2 Tấn công Password

Cách phòng chống

- **Đặt mật khẩu phức tạp**
  - Tuy đơn giản nhưng biện pháp này giúp người dùng phòng tránh được hầu hết các cuộc tấn công dò mật khẩu thông thường.
  - Một mật khẩu mạnh thường bao gồm: chữ IN HOA, chữ thường, số, ký tự đặc biệt (ví dụ @$*%&#)
- **Bật xác thực 2 bước**:
  - Hầu hết dịch vụ cho phép người dùng bật xác thực 2 bước khi đăng nhập trên thiết bị mới. Điều này khiến hacker có hack được mật khẩu cũng không thể đăng nhập được.
  - Hiện tại Facebook, Gmail, các ngân hàng, ví điện tử… đều có tính năng này.

3.2 Tấn công Password

Cách phòng chống

- **Quản lý mật khẩu tập trung**:
  - Việc lưu tất cả mật khẩu trên một thiết bị là con dao hai lưỡi. Người dùng cân nhắc khi thực hiện.
- **Thay đổi mật khẩu định kì:**
  - Gây khó khăn cho quá trình hack mật khẩu của tin tặc.
- **Thận trọng khi duyệt web**:
  - Tin tặc có thể hack mật khẩu của bạn bằng cách tạo ra một đường link giả mạo. Link giả thường gần giống trang web chính vì thế, luôn thận trọng với các đường link trước khi đưa thông tin cá nhân

3.2 Tấn công Password

Cách phòng chống

- **Cẩn trọng khi mở email, tải file**:
  - Tuyệt đối không mở file lạ, và luôn kiểm tra địa chỉ email người gửi xem có chính xác không.
  - VD: tên người gửi là Ngọc Luân JSC nhưng địa chỉ email là ngoclunajsc thì có dấu hiệu lừa đảo.

3.2 Tấn công Password

Bị hack mật khẩu phải làm sao?

- **Ngay lập tức khóa dịch vụ đang sử dụng**:
  - Liên hệ trực tiếp với các nhà cung cấp dịch vụ (ngân hàng, facebook, gmail…) để yêu cầu tạm ngưng dịch vụ cho tài khoản của bạn.
- **Ngắt kết nối với các dịch vụ khác (nếu có)**:
  - Nếu bạn bị mất tài khoản Gmail, cần ngắt kết nối với tài khoản facebook, tài khoản ngân hàng bằng cách thông báo cho nhân viên hỗ trợ.
- **Xác nhận danh tính để lấy lại mật khẩu:**
  - Bạn chỉ cần chọn "Forget Password" hoặc "Quên mật khẩu" rồi tiến hành nhập thông tin cần thiết để lấy lại mật khẩu. Mỗi dịch vụ khác nhau yêu cầu xác minh thông tin khác nhau, thông thường chính là thông tin bạn sử dụng để đăng ký tài khoản

3.3 Tấn công bằng Backdoor

- **Backdoor (cửa hậu)**
  - Backdoor trong phần mềm hay hệ thống máy tính thường là một cổng không được thông báo rộng rãi.
  - Cho phép người quản trị xâm nhập hệ thống để tìm nguyên nhân gây lỗi hoặc bảo dưỡng (do nhà phát triển tạo ra).
  - Hacker và gián điệp dùng backdoor để truy cập bất hợp pháp vào hệ thống (cài đặt thông qua một số mã độc).

3.3 Tấn công bằng Backdoor

- **Cách phát hiện tấn công Backdoor**
  - Rất khó phát hiện, tùy thuộc vào hệ hiều hành
  - Dụng phần mềm antimalware quét và kiểm tra backdoor
  - Một số trường hợp khác đòi hỏi phải sử dụng các công cụ chuyên dụng, hoặc các công cụ giám sát giao thức để kiểm tra gói mạng mới có thể phát hiện được backdoor.

3.3 Tấn công bằng Backdoor

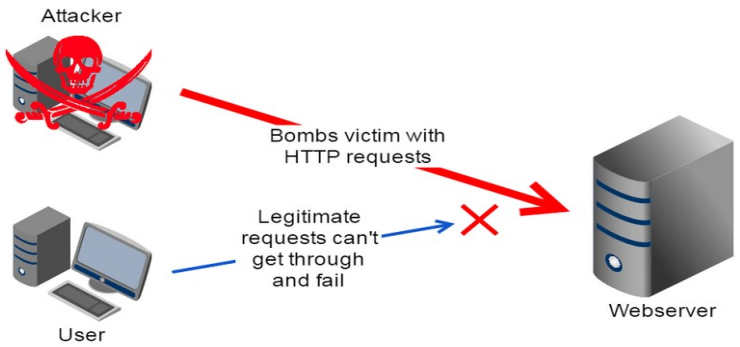
- **Cách phòng chống**
  - Tuân thủ đúng các phương pháp bảo mật
  - Chỉ cài đặt các phần mềm tin cậy và đảm bảo đã bật tường lửa (firewall) trên thiết bị (firewall có thể ngăn chặn các cuộc tấn công backdoor, hạn chế lưu lượng truyền qua các cổng mở)
  - Theo dõi lưu lượng mạng để phát hiện và kiểm tra xem có sự hiện diện của backdoor hay không

3.4 Tấn công từ chối dịch vụ

- **Denial-of-service (DoS)**
  - Là hình thức tấn công khá phổ biến hiện nay, nó khiến cho máy tính mục tiêu không thể xử lý kịp các tác vụ và dẫn đến quá tải.
  - Các cuộc tấn công DOS này thường nhắm vào các máy chủ ảo (VPS) hay Web Server của các doanh nghiệp lớn như ngân hàng, chính phủ hay là các trang thương mại điện tử…

3.4 Tấn công từ chối dịch vụ

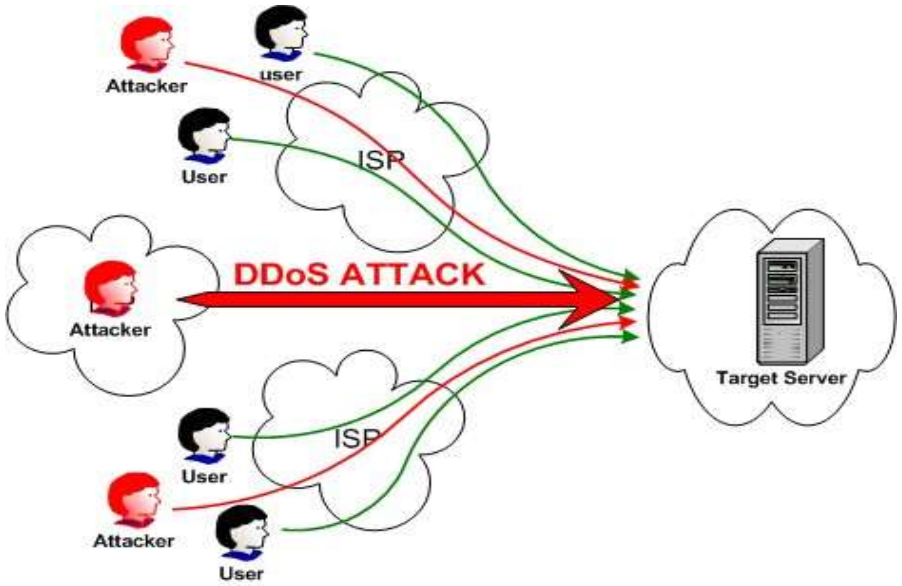
- **Denial-of-service (DoS)**



- Tấn công DOS thường chỉ được tấn công từ một địa điểm duy nhất, tức là nó sẽ xuất phát tại một điểm và chỉ có một dải IP thôi. Bạn có thể phát hiện và ngăn chặn được.

3.4 Tấn công từ chối dịch vụ

- **Distributed Denial Of Service (DDoS)**



3.4 Tấn công từ chối dịch vụ

- **Distributed Denial Of Service (DDoS)**
  - Là một dạng tấn công nhằm gây cạn kiện tài nguyên hệ thống máy chủ và làm ngập lưu lượng băng thông Internet, khiến truy cập từ người dùng tới máy chủ bị ngắt quãng, truy cập chập chờn, thậm chí không thể truy cập được Internet, làm tê liệt hệ thống hoặc thậm chí là cả một hệ thống mạng nội bộ.
  - Tấn công **DDOS** mạnh hơn **DOS** rất nhiều, điểm mạnh của hình thức này đó là nó được phân tán từ nhiều dải IP khác nhau, chính vì thế người bị tấn công sẽ rất khó phát hiện để ngăn chặn được.
  - Hacker không chỉ sử dụng máy tính của họ để thực hiện một cuộc tấn công vào một trang web hay một hệ thống mạng nào đó, mà họ còn lợi dùng hàng triệu máy tính khác để thực hiện việc này.

3.5 Mail Bombs

- Là một dạng của DoS
- Một số lượng lớn email được gửi đến một tài khoản với mục đích chính là hạ gục tài khoản email mục tiêu (gián đoạn trong quá trình nhận/chuyển và xử lý các thư hợp pháp)

3.5 Tấn công Mail Bombs

- Tấn công Mailbomb thường tấn công các máy chủ email.
- Trong kiểu tấn công này thay vì các gói, các email quá lớn hoặc email rác được lọc (ngăn chặn) thì lại liên tục được gửi đến một máy chủ email mục tiêu.
- Điều này thường làm sập máy chủ email do tải đột ngột và khiến chúng vô dụng cho đến khi được sửa chữa.

3.6 Tấn công Man-in-the-middle

Tấn công xen giữa (Man-in-the-middle)

- Là một kiểu tấn công mạng, trong đó kẻ tấn công chặn đường liên lạc giữa 2 bên
- Mục tiêu là bất kỳ loại giao tiếp trực tuyến nào, như trao đổi email, phương tiện truyền thông mạng xã hội hoặc thậm chí các trang web tài chính, các kết nối liên quan đến khóa công khai hoặc khóa riêng và các trang web yêu cầu đăng nhập.
- Tin tặc có thể xem dữ liệu riêng tư của bạn (các cuộc hội thoại, thông tin đăng nhập hoặc thông tin tài chính). Họ cũng có thể gửi và nhận dữ liệu mà bạn không biết.

3.6 Tấn công Man-in-the-middle

Các loại tấn công Man-in-the-middle

- Email Hijacking (Đánh cắp email)
  - Chiếm quyền điều khiển email của các tổ chức ngân hàng hoặc tài chính. Họ có quyền truy cập vào tài khoản cá nhân của nhân viên và khách hàng và theo dõi các giao dịch. Khi có cơ hội, họ sử dụng địa chỉ email của ngân hàng để gửi hướng dẫn riêng cho khách hàng. Bằng cách làm theo các hướng dẫn này, khách hàng vô tình gửi tiền của họ cho những kẻ tấn công thay vì ngân hàng của họ.

3.6 Tấn công Man-in-the-middle

Các loại tấn công Man-in-the-middle

- Wi-Fi Eavesdropping (Nghe lén Wifi)
  - Kẻ tấn công thiết lập một địa chỉ Wi-Fi có tên có vẻ hợp pháp. Sau đó, họ chờ người dùng (bạn) kết nối với mạng Wi-Fi. Khi bạn kết nối với Wi-Fi, tin tặc có thể truy cập thiết bị của bạn, theo dõi hoạt động của bạn và chặn dữ liệu cá nhân của bạn. Sau đó dùng các thông tin đó thực hiện một tấn công khác.

3.6 Tấn công Man-in-the-middle

Các loại tấn công Man-in-the-middle

- **Session Hijacking (chiếm phiên làm việc)**
  - Một phiên là khoảng thời gian bạn đã đăng nhập và làm việc trong hệ thống (các hệ thống ngân hàng, tài chính)
  - Mục tiêu lấy thông tin đăng nhập, thông tin cá nhân, theo dõi phiên làm việc thông qua các cookie của bạn thậm chí thay mặt bạn thực hiện một số giao dịch.

3.6 Tấn công Man-in-the-middle

Các loại tấn công Man-in-the-middle

- **IP Spoofing/DNS Spoofing/HTTPS Spoofing**

3.6 Tấn công Man-in-the-middle

Bảo vệ khỏi tấn công MITM

- Sử dụng kết nối HTTPS
- Sử dụng HSTS (HTTP Strict Transport Security)
- Luôn luôn cập nhật hệ thống và chương trình của bạn
- Cẩn thận với mạng Wi-Fi
- Sử dụng mạng riêng ảo (VPN)

3.7 Tấn công Sniffing

- Sniffing là một chương trình lắng nghe trên hệ thống mạng để truyền dữ liệu. Sniffing cho phép các cá nhân nắm bắt dữ liệu khi nó truyền qua mạng.
- Kỹ thuật này được sử dụng bởi các chuyên gia mạng để chuẩn đoán các sự cố mạng và bởi những users có ý định xấu để thu thập dữ liệu không được mã hóa, như password và username. Nếu thông tin này được ghi lại trong quá trình người dùng có thể truy cập vào hệ thống hoặc mạng.
- Khởi đầu Sniffer là tên một sản phẩm của Network Associates có tên là Sniffier Analyzer.

3.7 Tấn công Sniffing

- Đối tượng Sniffing là:
  - Password (từ Email, Web, SMB, FTP, SQL hoặc Telnet)
  - Các thông tin về thẻ tín dụng
  - Văn bản của Email
  - Các tập tin đang di động trên mạng (tập tin Email, FTP hoặc SMB)

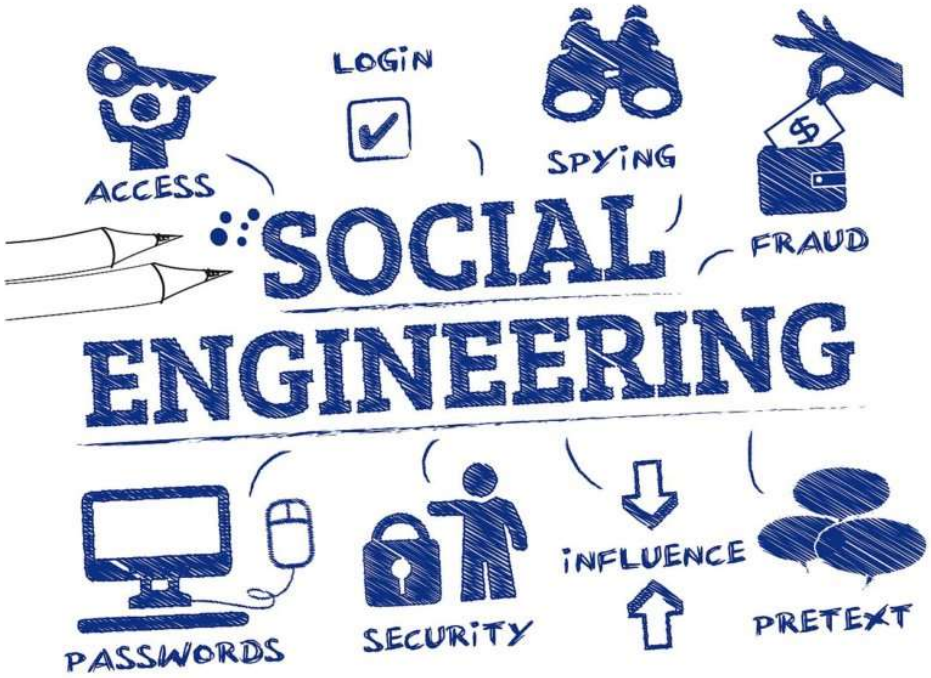
3.7 Tấn công Sniffing

- Sniffing thường được sử dụng vào 2 mục đích khác biệt nhau.
  - Tích cực:
    - Chuyển đổi dữ liệu trên đường truyền để quản trị viên có thể đọc và hiểu ý nghĩa của những dữ liệu đó.
    - Bằng cách nhìn vào lưu lượng của hệ thống cho phép quản trị viên có thể phân tích lỗi đang mắc phải trên hệ thống lưu lượng của mạng.
    - Một số Sniffing tân tiến có thêm tính năng tự động phát hiện và cảnh báo các cuộc tấn công đang được thực hiện vào hệ thống mạng mà nó đang hoạt động. (Intrusion Detecte Service)
    - Ghi lại thông tin về các gói dữ liệu, các phiên truyền...Giúp các quản trị viên có thể xem lại thông tin về các gói dữ liệu, các phiên truyền sau sự cố...Phục vụ cho công việc phân tích, khắc phục các sự cố trên hệ thống mạng.
  - Tiêu cực:
    - Nghe lén thông tin trên mạng để lấy các thông tin quan trọng.

Tấn công Social Engineering

Tấn công Social Engineering

- là kỹ thuật tác động đến con người, nhằm mục đích lấy được thông tin hoặc đạt được một mục đích mong muốn.
- Dựa vào điểm yếu tâm lý, nhận thức sai lầm của con người về việc bảo mật thông tin, sử dụng sự ảnh hưởng và thuyết phục để đánh lừa người dùng nhằm khai thác các thông tin có lợi cho cuộc tấn công, hoặc thuyết phục nạn nhân thực hiện một hành động nào đó.



Tấn công Social Engineering

Các hình thức tấn công Social Engineering phổ biến

- **Phishing**
- **Watering Hole**
- **Pretexting**
- **Baiting và Quid Pro Quo**

Tấn công Social Engineering

Phishing

- Ghép từ “Fishing” và Phony” (“câu cá” và “lừa dảo”)
- Là một hình thức lừa đảo bằng cách giả mạo các tổ chức có uy tín như ngân hàng, trang web giao dịch trực tuyến, các công ty thẻ tín dụng để lừa người dùng chia sẻ thông tin tài chính bí mật như: tên đăng nhập, mật khẩu giao dịch và những thông tin nhạy cảm khác.

Tấn công Social Engineering

Các kiểu tấn công Phishing

- Spear phishing
  - Tấn công cá nhân hoặc tổ chức cụ thể, với nội dung được thiết kế riêng cho nạn nhân. Hacker phải thu thập và đối chiếu các thông tin của nạn nhân (tên, chức danh, email, tên đồng nghiệp, mối quan hệ,…) để tạo ra một email lừa đảo đáng tin cậy, yêu cầu bạn cung cấp thông tin của mình. Bạn tưởng email đó là email từ một người hoặc bất kỳ tổ chức nào mà bạn biết.
  - Ví dụ, something.com có thể có tên miền phụ tên là paypal.something.com. Kẻ tấn công tạo một ID email là support@paypal.something.com. Email có vẻ khá giống với ID email liên quan đến PayPal.
  - Là mối đe dọa nghiêm trọng đối với doanh nghiệp, chính phủ và gây thiệt hại lớn

Tấn công Social Engineering

Các kiểu tấn công Phishing

- **Spear phishing**
  - Các biện pháp bảo vệ khỏi Spear Phishing
    - Nếu bạn nhận được bất kỳ email nào, dưới bất kỳ hình thức nào, yêu cầu bạn cung cấp thông tin chi tiết, thứ mà bạn không cảm thấy thoải mái khi chia sẻ, hãy coi đó là một hình thức spear phishing và trực tiếp loại bỏ nó. Bỏ qua các email, tin nhắn đó và kết thúc các cuộc gọi như vậy.
    - Chỉ chia sẻ những gì cần thiết trên các trang mạng xã hội
    - Nên có một phần mềm bảo mật tốt để lọc các email của mình. Bạn có thể thêm chứng chỉ email và mã hóa cho các ứng dụng email mà bạn sử dụng để bạn được bảo vệ tốt hơn. Nhiều cuộc tấn công spear phishing có thể bị phát hiện bằng các chương trình hoặc chứng chỉ bảo mật được tích hợp hay cài đặt cho ứng dụng email.

Tấn công Social Engineering

Các kiểu tấn công Phishing

- **Clone phishing**
  - Hacker sao chép các email hợp pháp, nhưng thay thế đường dẫn hoặc trong email. Khi người dùng nhấp vào liên kết hoặc mở tệp đính kèm, tài khoản của họ sẽ bị hacker kiểm soát. Sau đó, hacker sẽ giả mạo danh tính của nạn nhân để thực hiện phishing trong chính tổ chức của nạn nhân

Tấn công Social Engineering

Các kiểu tấn công Phishing

- **Phone phishing**
  - "vice phishing" hoặc "vishing"
  - Các phisher sẽ tự xưng là đại điện của ngân hàng, sở cảnh sát, hoặc thậm chí sở thuế vụ tại địa phương bạn sống. Họ sẽ đe dọa và yêu cầu bạn cung cấp thông tin tài khoản hoặc nộp phạt qua chuyển khoản hoặc bằng thẻ trả trước để tránh bị theo dõi

Tấn công Social Engineering

Các kiểu tấn công Phishing

- **Lừa đảo qua mạng xã hội:**
  - Hacker thực hiện bằng cách gửi đường dẫn qua tin nhắn, trạng thái Facebook hoặc các mạng xã hội khác. Các tin nhắn này có thể là thông báo trúng thưởng các hiện vật có giá trị như xe SH, xe ôtô, điện thoại iPhone,… và hướng dẫn người dùng truy cập vào một đường dẫn để hoàn tất việc nhận thưởng.
  - Ngoài việc lừa nạn nhân nộp lệ phí nhận thưởng, tin tặc có thể chiếm quyền điều khiển tài khoản, khai thác thông tin danh sách bạn bè sử dụng cho các mục đích xấu như lừa mượn tiền, mua thẻ cào điện thoại,…

Tấn công Social Engineering

Cách phòng tránh tấn công Phishing

- Không mở email từ người lạ
- KHông nhấp vào các liên kết đáng ngờ trong email
- Nếu nghi ngờ một trang web trông có vẻ không hợp pháp, bạn hãy nhập địa chỉ trang web hợp pháp trên trình duyệt web theo cách thủ công
- Kiểm tra xem các website có dùng các giao thức hỗ trợ bảo mật không
- Nếu nghi ngờ một email không hợp pháp, hãy lấy các thông tin trong email đó để kiểm tra xem có cuộc tấn công lừa đảo nào thực hiện bằng phương pháp tương tự không
- Sử dụng phần mềm bảo mật chống phần mềm độc hại đáng tin cậy

Tấn công Social Engineering

Watering Hole

- Hacker tấn công có chủ đích vào các TC/DN thông qua việc lừa các thành viên truy cập vào các trang web chứa mã độc.
- Tin tặc thường nhắm đến các trang web có nhiều người truy cập, web "đen" hoặc tạo ra các trang web riêng để lừa người dùng, trong đó cố ý chèn vào website các mã khai thác liên quan đến các lỗ hổng trình duyệt.
- Nếu truy cập vào website, các mã độc này sẽ được thực thi và lây nhiễm vào máy tính của người dùng.

Tấn công Social Engineering

Kịch bản của tấn công Watering Hole

- Bước 1: Thu thập thông tin về TC/DN mục tiêu, gồm danh sách các website mà các nhân viên hay lãnh đạo của tổ chức thường xuyên truy cập. Sau đó, tin tặc bắt đầu tìm kiếm các trang web mà chúng để có thể xâm nhập, kết hợp với kỹ thuật tấn công local attack để nâng cao khả năng tấn công.
- Bước 2: Sau khi đã chiếm được quyền điều khiển của một website mà các nhân viên của tổ chức thường xuyên truy cập, tin tặc sẽ thực hiện chèn các mã khai thác các lỗ hổng thông qua trình duyệt, ứng dụng flash hay java
- Bước 3: Sau khi người dùng truy cập vào các trang web độc hại, ngay lập tức mã độc sẽ được thực thi. Khi đó, tin tặc sẽ chiếm quyền điều khiển và cài đặt các chương trình độc hại cho phép điều khiển từ xa lên máy tính nạn nhân. Từ đó, khai thác các thông tin từ người dùng hoặc sử dụng chính máy đó để tấn công các máy tính khác.

Tấn công Social Engineering

Pretexting

- Hacker tập trung vào việc tạo ra một lý do hợp lý, hoặc một kịch bản đã được tính toán từ trước để ăn cắp thông tin cá nhân của nạn nhân.
- Hacker có thể sẽ cố thao túng các mục tiêu để khai thác các điểm yếu về cấu trúc của một tổ chức hoặc công ty. Ví dụ, một tin tặc mạo danh một kiểm toán viên của dịch vụ CNTT bên ngoài công ty với những lý lẽ hợp lý, đủ sức thuyết phục nhân viên an ninh về mặt vật lý, cho phép tin tặc vào cơ sở làm việc của công ty đó.
- Không giống như các email lừa đảo vốn lợi dụng sự sợ hãi và khẩn cấp của nạn nhân, các cuộc tấn công Pretexting dựa vào việc xây dựng cảm giác tin cậy cho đối tượng cần khai thác.

Tấn công Social Engineering

Baiting và Quid Pro Quo

- Lợi dụng sự tò mò của con người hoặc hứa hẹn về một mặt hàng hay một sản phẩm hấp dẫn nào đó để đánh lừa nạn nhân. Ví dụ điển hình là một kịch bản tấn công mà tin tặc sử dụng một tệp độc hại được giả mạo thành bản cập nhật phần mềm hoặc phần mềm phổ biến nào đó.
- Hacker cũng có thể tấn công Baiting về mặt vật lý, ví dụ như phát miễn phí thẻ USB bị nhiễm độc trong khu vực lân cận của tổ chức mục tiêu và đợi nhân viên nội bộ lây nhiễm phần mềm độc hại vào máy tính của công ty. Sau khi được thực thi trên các máy tính, các phần mềm độc hại được cài đặt trên các USB này sẽ giúp tin tặc chiếm được toàn quyền điều khiển, qua đó phục vụ cho mục đích tấn công tiếp theo.

Tấn công Social Engineering

Baiting và Quid Pro Quo

- Quid Pro Quo hay Something For Something là biến thể của Baiting.
- Thay vì dụ đưa ra lời hứa về một sản phẩm, hacker hứa hẹn một dịch vụ hoặc một lợi ích dựa trên việc thực hiện một hành động cụ thể nào đó qua một một dịch vụ hoặc lợi ích được tin tặc xây dựng để trao đổi thông tin hoặc quyền truy cập.
- Hacker mạo danh nhân viên CNTT của một tổ chức lớn. Hacker đó cố gắng liên lạc qua điện thoại với nhân viên của tổ chức định tấn công, sau đó cung cấp và hướng dẫn cho họ một số thông tin liên quan đến việc nâng cấp hoặc cài đặt phần mềm. Để tạo điều kiện cho việc thực hiện các hành vi độc hại, các hacker sẽ yêu cầu nạn nhân tạm thời vô hiệu hóa phần mềm antivirus cài trong máy, nhờ đó ứng dụng độc hại được thực thi mà không gặp phải bất cứ trở ngại nào.

Tấn công Social Engineering

Biện pháp phòng chống Social Engineering- Đối với cá nhân

- Cẩn thận và không nên trả lời bất kỳ thư rác nào yêu cầu xác nhận, cập nhật bất kỳ thông tin nào về tài khoản của cá nhân, TC/DN.
- Không kích chuột vào bất kỳ liên kết đi kèm với thư rác nếu không chắc chắn về nó.
- Cảnh giác với các thông tin khuyến mại, trúng thưởng nhận được trên MXH; Không nhấp chuột vào các đường dẫn của các trang web lạ; Không cung cấp thông tin cá nhân, đặc biệt là tài khoản ngân hàng; Sử dụng mật khẩu phức tạp đối với các tài khoản MXH và thường xuyên thay đổi các mật khẩu này.
- Cảnh giác khi thực hiện truy cập vào các trang web, đặc biệt là các trang web không phổ biến vì chúng rất có thể tồn tại lỗ hổng mà tin tặc đang nhắm vào để khai thác.

Tấn công Social Engineering

Biện pháp phòng chống Social Engineering - Đối với TC/DN

- Phân chia tài khoản, quyền hạn và trách nhiệm rõ ràng đối với các tài khoản MXH, website, hệ thống.
- Tránh sử dụng một mật khẩu cho nhiều tài khoản khác nhau nhằm tránh nguy cơ lộ lọt thông tin.
- Hạn chế đăng những thông tin cá nhân, thông tin công ty, doanh nghiệp lên mạng xã hội để tránh kẻ xấu mạo danh.
- Nâng cao kiến thức về tấn công và cách phòng tránh Social Engineering, kỹ năng ATTT cho cán bộ, nhân viên; Thực hiện các buổi tập huấn với các tình huống giả mạo, qua đó nâng cao nhận thức, ý thức cảnh giác và kinh nghiệm đối phó với những tình huống tương tự.
- Thường xuyên cập nhật bản vá cho phần mềm, hệ điều hành.