



BÀI GIẢNG AN TOÀN & BẢO MẬT THÔNG TIN

CHƯƠNG 1 - TỔNG QUAN

TS. NGUYỄN ĐÌNH DƯƠNG
BỘ MÔN KHMT - KHOA CÔNG NGHỆ THÔNG TIN

Email: duongnd@utc.edu.vn

Ngày 03/07/2022



Nội dung

Giới thiệu

Một số khái niệm cơ bản

Các bước cơ bản trong ATBMTT



Nội dung

Giới thiệu

Một số khái niệm cơ bản

Các bước cơ bản trong ATBMTT



1. Giới thiệu

- Con người luôn sống trong môi trường trao đổi thông tin hàng ngày, hàng giờ. Mọi hoạt động xã hội, chính trị, kinh tế trong thời đại mới hiện nay thực chất đều là những hoạt động thu thập, xử lý, lưu trữ và trao đổi thông tin.
- Trong phần lớn trường hợp trao đổi thông tin giữa hai đối tác, người ta không hề muốn để thông tin bị lộ cho người thứ ba biết.
- Trong bối cảnh đó An toàn và Bảo mật thông tin luôn là mối quan tâm hàng đầu trong mọi giao dịch xã hội, đặc biệt là giao dịch điện tử trên môi trường Internet.
- Để bảo vệ bí mật cho thông tin của mình được gửi đi, người ta phải dùng **mật mã** tức là dùng những phương pháp biến đổi làm cho bản gốc của thông tin (*plaintext*) biến thành một dạng bí mật (*ciphertext*) mà chỉ có những người nắm được quy luật mới có thể biến đổi ngược lại thành dạng nguyên gốc ban đầu.



1. Giới thiệu

Mật mã là gì ?

- *Mật mã (cryptology)*: là một lĩnh vực khoa học chuyên nghiên cứu về các phương pháp và kỹ thuật đảm bảo an toàn và bảo mật trong truyền tin liên lạc với giả thiết sự tồn tại của các thế lực thù địch, những kẻ muốn ăn cắp thông tin để lợi dụng và phá hoại.
- Mật mã (cryptology) là sự kết hợp của 2 lĩnh vực:
 - Mã hoá (cryptography): nghiên cứu các kỹ thuật toán học nhằm cung cấp các công cụ hay dịch vụ đảm bảo an toàn thông tin. Các sản phẩm của lĩnh vực này là các *hệ mã mật*, *các hàm băm*, *các hệ chữ ký điện tử*, *các cơ chế phân phối*, *quản lý khoá* và *các giao thức mật mã*.
 - Thám mã (cryptanalysis): nghiên cứu các kỹ thuật toán học phục vụ phân tích phá mật mã và/hoặc tạo ra các đoạn mã giả nhằm đánh lừa bên nhận tin. Sản phẩm của lĩnh vực này là các *phương pháp thám mã*, *giả mạo chữ ký*, *tấn công hàm băm* và *các giao thức mật mã*.

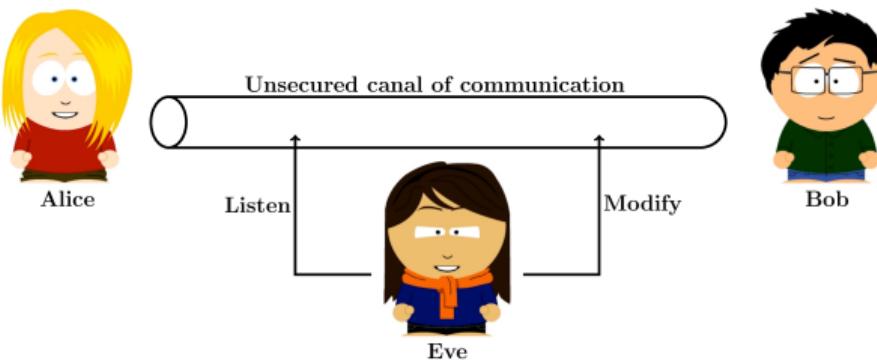


Ứng dụng của mật mã

- Với các chính phủ: bảo vệ truyền tin mật trong quân sự và ngoại giao, bảo vệ thông tin các lĩnh vực tầm cỡ lợi ích quốc gia.
- Trong các hoạt động kinh tế: bảo vệ các thông tin nhạy cảm trong giao dịch như hồ sơ pháp lý hay y tế, các giao dịch tài chính hay các đánh giá tín dụng ...
- Với các cá nhân: bảo vệ các thông tin nhạy cảm, riêng tư trong liên lạc với thế giới qua các giao dịch sử dụng máy tính và/hoặc kết nối mạng.



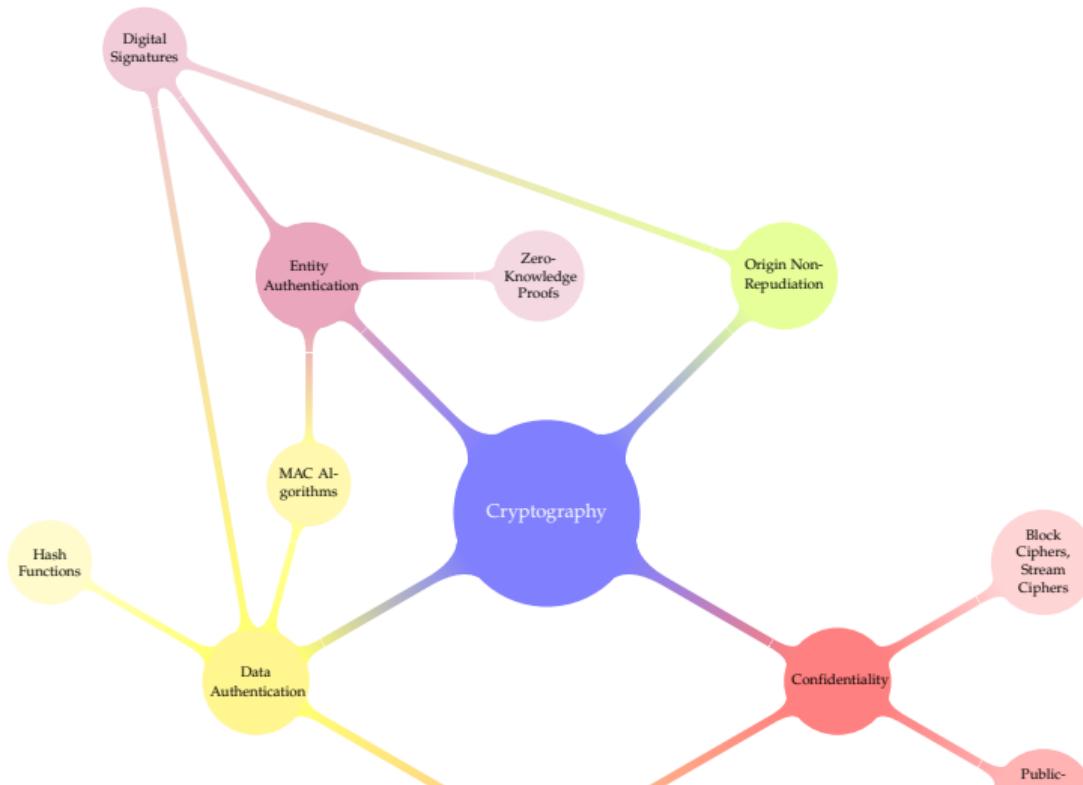
1. Giới thiệu



- Làm thế nào Alice có thể gửi tin nhắn cho Bob qua internet để chỉ Bob có thể đọc nó? (ngay cả khi họ chưa từng gặp nhau trong quá khứ!)
- Làm thế nào Alice có thể ký điện tử một tài liệu để mọi người chắc chắn rằng cô ấy là người đã ký và không ai có thể giả mạo chữ ký của cô ấy?
- Làm thế nào bạn có thể chia sẻ một bí mật giữa năm người để bạn không nhận được bất kỳ thông tin nào về bí mật đó nếu bạn chỉ có bốn lượt chia sẻ?
- Bạn có thể chứng minh rằng bạn biết một bí mật mà không tiết lộ bất kỳ thông tin nào về bản chất hoặc nội dung của bí mật này không?



1. Giới thiệu





1. Giới thiệu

Sơ lược lịch sử mật mã

- **Thời kỳ tiền khoa học:** Tính từ thượng cổ cho đến 1949. Trong thời kỳ này, mật mã học được coi là một ngành mang nhiều tính thủ công, nghệ thuật hơn là tính khoa học. Các hệ mật mã được phát minh và sử dụng trong thời kỳ này được gọi là các hệ mật mã cổ điển
 - Mã hoá Caesar (Caesar's cipher), cách đây 2000 năm: các chữ cái được thay thế bằng các chữ cái cách chúng 3 vị trí về bên phải trong bản alphabet: **DASEAR** → **FDHVDU**
 - Vernam cipher (1926): đem thực hiện phép XOR văn bản gốc (plaintext) với một chuỗi nhị phân ngẫu nhiên có độ dài bằng độ dài của văn bản gốc (chuỗi này là chính là khoá của phép mã hoá). Trong cipher loại này, khoá chỉ được dùng đúng một lần duy nhất.



1. Giới thiệu

- **Ký nguyên mật mã được coi là ngành khoa học:** được đánh dấu bởi bài báo nổi tiếng của Claude Shannon "*Communication theory of secrecy systems*", 1949. Bài báo Shannon đã nền móng cho việc áp dụng công cụ toán, cụ thể là xác suất, trong xây dựng mô hình và đánh giá tính mật của các hệ mã mật.
- Sự bùng nổ thực sự trong lý thuyết về mật mã (Cryptology) chỉ bắt đầu từ bài báo của hai nhà bác học Diffie và Hellman, "*New directions in cryptography*", 1976. Trong đó, các ông đã chứng tỏ rằng trong truyền tin bí mật, không nhất thiết là cả hai bên đều phải nắm khoá bí mật (tức bên gửi phải làm cách nào đó chuyển được khoá mật cho bên nhận). Hơn nữa họ đã lần đầu tiên giới thiệu khái niệm về *chữ ký điện tử* (digital signature).



Nội dung

Giới thiệu

Một số khái niệm cơ bản

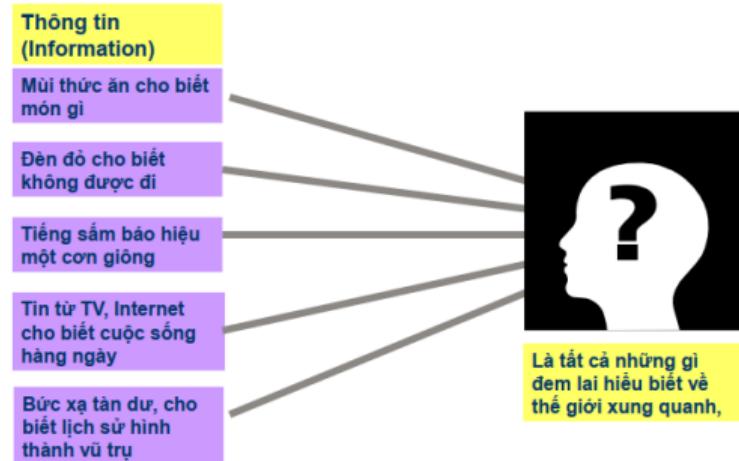
Các bước cơ bản trong ATBMTT



2. Một số khái niệm cơ bản

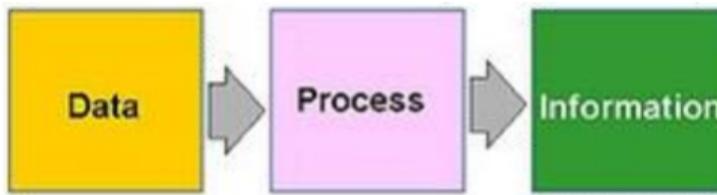
Dữ liệu và thông tin

- Thông tin (*information*) là khái niệm trừu tượng, giúp con người hiểu và nhận thức thế giới, giúp họ thực hiện hợp lý công việc cần làm.
- Thông tin có thể truyền từ người này sang người khác.
- Thông tin là kết quả xử lý, điều khiển và tổ chức dữ liệu theo cách mà nó sẽ bổ sung thêm tri thức cho người nhận.





2. Một số khái niệm cơ bản



- Dữ liệu (*data*) là biểu diễn của thông tin, được thể hiện bằng các tín hiệu vật lý.
- Dữ liệu trong thực tế có thể là:
 - Các số liệu thường được mô tả bằng số như trong các bảng biểu
 - Các ký hiệu qui ước, ví dụ chữ viết
 - Các tín hiệu vật lý ví dụ như ánh sáng, âm thanh, nhiệt độ, áp suất, ...

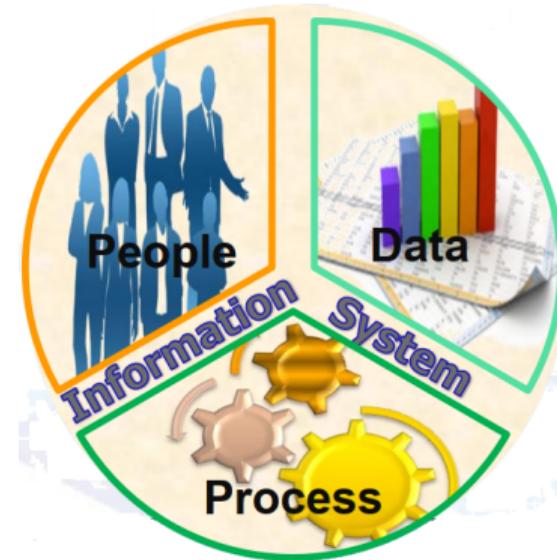
⊕ **Nhận xét:** Theo quan niệm chung của người làm CNTT thì thông tin là những hiểu biết của con người về một lĩnh vực nào đấy, còn dữ liệu là thông tin được biểu diễn và xử lý trong MT.



2. Một số khái niệm cơ bản

An toàn & Bảo mật HTTT

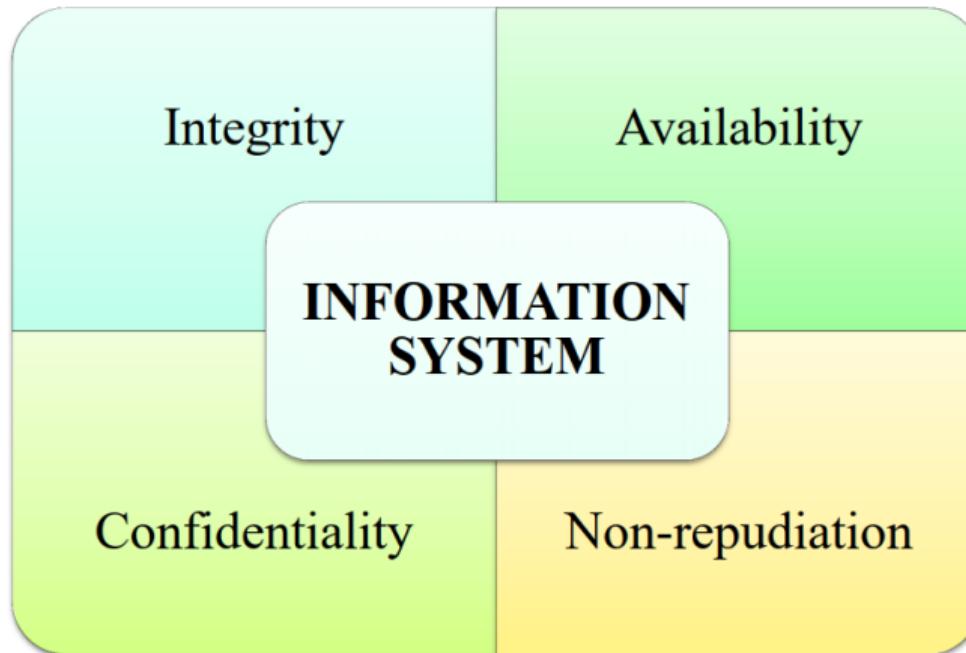
- **Hệ thống thông tin (Information Systems)** là một hệ thống gồm con người, dữ liệu và những hoạt động xử lý dữ liệu và thông tin trong một tổ chức.
- **AT&BM HTTT (Information Systems Security)** là bảo vệ hệ thống thông tin chống lại việc truy cập, sử dụng, chỉnh sửa, phá hủy, làm lộ và làm gián đoạn thông tin và hoạt động của hệ thống một cách trái phép.





2. Một số khái niệm cơ bản

Yêu cầu của AT& BM HTTT

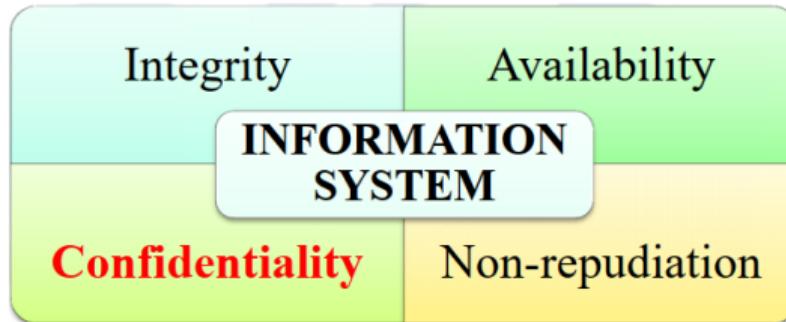




2. Một số khái niệm cơ bản

Yêu cầu của AT& BM HTTT

- **Tính bảo mật (Confidentiality):** bảo vệ dữ liệu không bị lộ ra ngoài một cách trái phép.



Ví dụ 2.1

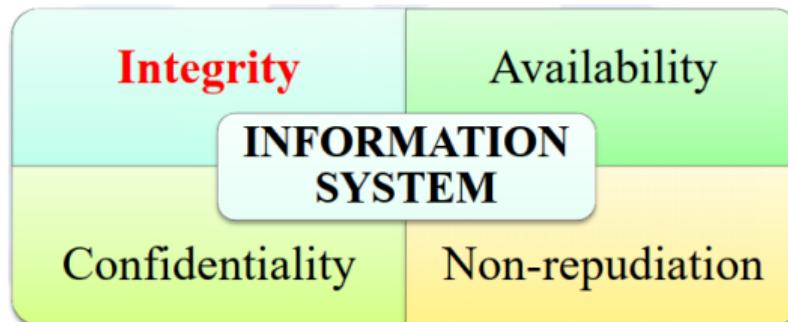
Trong hệ thống ngân hàng, một khách hàng (KH) được phép xem thông tin số dư tài khoản của mình nhưng không được phép xem thông tin của KH khác.



2. Một số khái niệm cơ bản

Yêu cầu của AT& BM HTTT

- **Tính toàn vẹn (Integrity):** Chỉ những người dùng được ủy quyền mới được phép chỉnh sửa dữ liệu.



Ví dụ 2.2

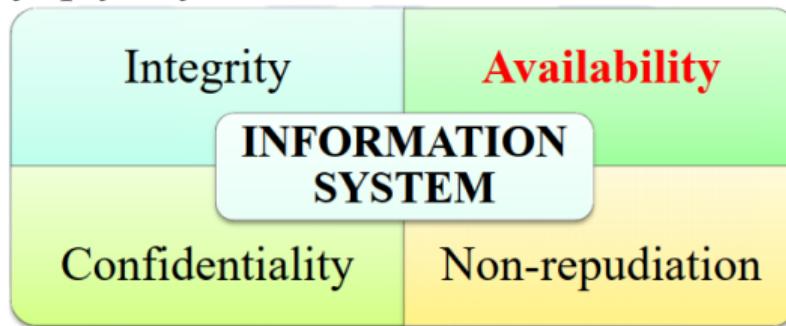
Trong hệ thống ngân hàng, không cho phép KH tự thay đổi thông tin số dư của tài khoản của mình.



2. Một số khái niệm cơ bản

Yêu cầu của AT& BM HTTT

- **Tính sẵn sàng (Availability):** Đảm bảo dữ liệu luôn sẵn sàng khi những người dùng hoặc ứng dụng được ủy quyền yêu cầu.



Ví dụ 2.3

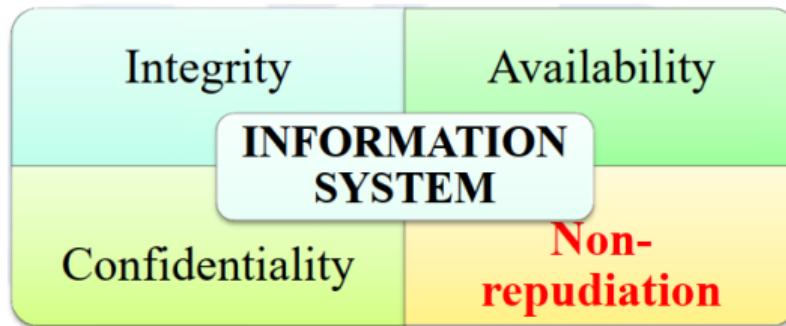
Trong hệ thống ngân hàng, cần đảm bảo rằng KH có thể truy vấn thông tin số dư tài khoản bất kỳ lúc nào theo như quy định.



2. Một số khái niệm cơ bản

Yêu cầu của AT& BM HTTT

- **Tính chống từ chối (Non-repudiation):** Khả năng ngăn chặn việc từ chối một hành vi đã làm.



Ví dụ 2.4

Trong hệ thống ngân hàng, có khả năng cung cấp bằng chứng để chứng minh một hành vi KH đã làm, như rút tiền, chuyển tiền.



2. Một số khái niệm cơ bản

Mục tiêu của AT& BM HTTT

- **Ngăn chặn:** Ngăn chặn kẻ tấn công vi phạm các chính sách bảo mật.





2. Một số khái niệm cơ bản

Mục tiêu của AT& BM HTTT

- **Ngăn chặn:** Ngăn chặn kẻ tấn công vi phạm các chính sách bảo mật.
- **Phát hiện:** Phát hiện các vi phạm chính sách bảo mật.





2. Một số khái niệm cơ bản

Mục tiêu của AT& BM HTTT

- **Ngăn chặn:** Ngăn chặn kẻ tấn công vi phạm các chính sách bảo mật.



- **Phát hiện:** Phát hiện các vi phạm chính sách bảo mật.



- **Phục hồi:**

- Chặn các hành vi vi phạm đang diễn ra, đánh giá và sửa lỗi;
- Tiếp tục hoạt động bình thường ngay cả khi tấn công





Nội dung

Giới thiệu

Một số khái niệm cơ bản

Các bước cơ bản trong ATBMTT



3. Các bước cơ bản trong ATBMTT

Xác định các mối đe dọa

Lựa chọn chính sách bảo mật

Lựa chọn cơ chế bảo mật



3. Các bước cơ bản trong ATBMTT

Xác định các mối đe dọa

Lựa chọn chính sách bảo mật

Lựa chọn cơ chế bảo mật

- Xác định các mối đe dọa (*threat*): Cái gì có thể làm hại đến hệ thống?
- Lựa chọn chính sách bảo mật (*security policy*): Điều gì cần mong đợi ở hệ thống bảo mật?
- Lựa chọn cơ chế bảo mật (*security mechanism*): Cách nào để hệ thống bảo mật có thể đạt được những mục tiêu bảo mật đề ra?



3. Các bước cơ bản trong ATBMTT

Xác định các mối đe dọa

Xác định các mối
đe dọa

Lựa chọn chính
sách bảo mật

Lựa chọn cơ
chế bảo mật



3. Các bước cơ bản trong ATBMTT

Xác định các mối đe dọa

Xác định các mối
đe dọa

Lựa chọn chính
sách bảo mật

Lựa chọn cơ
chế bảo mật

- Các mối đe dọa bảo mật (security threat) là những sự kiện có ảnh hưởng đến an toàn của hệ thống thông tin.
- Các mối đe dọa được chia làm 4 loại:
 - Xem thông tin một cách bất hợp pháp
 - Chính sửa thông tin một cách bất hợp pháp
 - Từ chối dịch vụ
 - Từ chối hành vi



3. Các bước cơ bản trong ATBMTT

Một số mối đe doạ thường gặp

- Lỗi và thiếu sót của người dùng (Errors and Omissions)
- Gian lận và đánh cắp thông tin (Fraud and Theft)
- Kẻ tấn công nguy hiểm (Malicious Hackers)
- Mã nguy hiểm (Malicious Code)
- Tấn công từ chối dịch vụ (Denial-of-Service Attacks)
- Social Engineering



3. Các bước cơ bản trong ATBMTT

Lỗi và thiếu sót của người dùng

- Mối đe dọa của hệ thống thông tin xuất phát từ những lỗi bảo mật, lỗi thao tác của những người dùng trong hệ thống.
- Là mối đe dọa hàng đầu đối với một hệ thống thông tin
- Giải pháp:
 - Huấn luyện người dùng thực hiện đúng các thao tác, hạn chế sai sót
 - Nguyên tắc: quyền tối thiểu (least privilege)
 - Thường xuyên back-up hệ thống



3. Các bước cơ bản trong ATBMTT

Gian lận và đánh cắp thông tin

- Mỗi đe dọa này do những kẻ tấn công từ bên trong hệ thống (inner attackers), gồm những người dùng giả mạo hoặc những người dùng có ý đồ xấu.
- Những người tấn công từ bên trong luôn rất nguy hiểm.
- Giải pháp:
 - Định ra những chính sách bảo mật tốt: có chứng cứ xác định được kẻ tấn công từ bên trong



3. Các bước cơ bản trong ATBMTT

Kẻ tấn công nguy hiểm

- Kẻ tấn công nguy hiểm xâm nhập vào hệ thống để tìm kiếm thông tin, phá hủy dữ liệu, phá hủy hệ thống.
- 5 bước để tấn công vào một hệ thống:
 - Thăm dò (Reconnaissance)
 - Quét lỗ hổng để tấn công (Scanning)
 - Cố gắng lấy quyền truy cập (Gaining access)
 - Duy trì kết nối (Maintaining access)
 - Xóa dấu vết (Cover his track)



3. Các bước cơ bản trong ATBMTT

Mã nguy hiểm

- Mã nguy hiểm là một đoạn mã không mong muốn được nhúng trong một chương trình nhằm thực hiện các truy cập trái phép vào hệ thống máy tính để thu thập các thông tin nhạy cảm, làm gián đoạn hoạt động hoặc gây hại cho hệ thống máy tính.
- Bao gồm: virus, worm, trojan horses, spyware, adware, backdoor, ...



3. Các bước cơ bản trong ATBMTT

Tấn công từ chối dịch vụ

- Là kiểu tấn công ngăn không cho những người dùng khác truy cập vào hệ thống
- Làm cho hệ thống bị quá tải và không thể hoạt động
- DoS: tấn công “one-to-one”
- DDoS(distributed denial of service)
 - Sử dụng các Zombie host
 - Tấn công “many-to-one”



3. Các bước cơ bản trong ATBMTT

Social Engineering

- Social engineering sử dụng sự ảnh hưởng và sự 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.
- Kẻ tấn công có thể lợi dụng các đặc điểm sau của con người để tấn công:
 - Mong muốn trở nên hữu dụng
 - Tin người
 - Nỗi sợ gấp rắc rối
 - Đơn giản đến mức cẩu thả
- Có 2 loại Social Engineering;
 - Social engineering dựa trên con người liên quan đến sự tương tác giữa con người với con người để thu được thông tin mong muốn.
 - Social engineering dựa trên máy tính: liên quan đến việc sử dụng các phần mềm để cò găng thu thập thông tin cần thiết



3. Các bước cơ bản trong ATBMTT

Social engineering dựa trên con người

- Nhân viên gián điệp/giả mạo
- Giả làm người cần được giúp đỡ
- Giả làm người quan trọng
- Giả làm người được ủy quyền
- Giả làm nhân viên hỗ trợ kỹ thuật



3. Các bước cơ bản trong ATBMTT

Social engineering dựa trên máy tính

- Phising: lừa đảo qua thư điện tử
- Vishing: lừa đảo qua điện thoại
- Pop-up Windows
- File đính kèm trong email
- Các website giả mạo
- Các phần mềm giả mạo



3. Các bước cơ bản trong ATBMTT

Xác định các mối đe dọa

Lựa chọn chính sách bảo mật

Lựa chọn cơ chế bảo mật



3. Các bước cơ bản trong ATBMTT

Xác định các mối đe dọa

Lựa chọn chính sách bảo mật

Lựa chọn cơ chế bảo mật

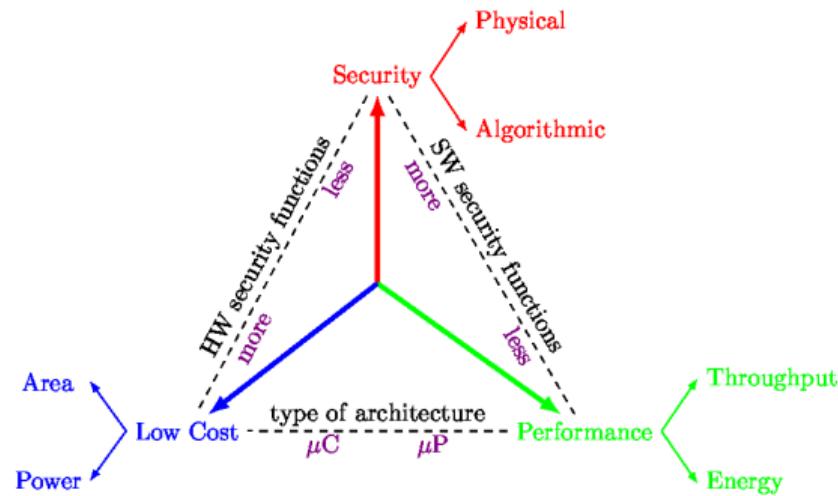
- Việc bảo mật hệ thống cần có một chính sách bảo mật rõ ràng.
- Cần có những chính sách bảo mật riêng cho những yêu cầu bảo mật khác nhau
- Xây dựng và lựa chọn các chính sách bảo mật cho hệ thống phải dựa theo các chính sách bảo mật do các tổ chức uy tín về bảo mật định ra (compliance): **NIST, SP800, ISO17799, HIPAA**



3. Các bước cơ bản trong ATBMTT

Lựa chọn chính sách bảo mật

- Chính sách bảo mật phải cân bằng giữa 3 yếu tố





3. Các bước cơ bản trong ATBMTT

Xác định các mối đe dọa

Lựa chọn chính sách bảo mật

Lựa chọn cơ chế bảo mật



3. Các bước cơ bản trong ATBMTT

Xác định các mối đe dọa

Lựa chọn chính sách bảo mật

Lựa chọn cơ chế bảo mật

- Xác định cơ chế bảo mật phù hợp để hiện thực các chính sách bảo mật và đạt được các mục tiêu bảo mật đề ra
- Có 4 cơ chế bảo mật:
 - Điều khiển truy cập (Access control)
 - Điều khiển suy luận (Inference control)
 - Điều khiển dòng thông tin (Flow control)
 - Mã hóa (Encryption)



3. Các bước cơ bản trong ATBMTT

Điều khiển truy cập

- *Điều khiển truy cập (Access control)*: là cơ chế điều khiển, quản lý các truy cập vào hệ thống cơ sở dữ liệu.
- Các bước trong điều khiển truy cập
 - Người dùng cung cấp danh định (identity)
 - Người dùng chứng minh danh định đó là đúng
 - Xác định quyền mà người dùng có



3. Các bước cơ bản trong ATBMTT

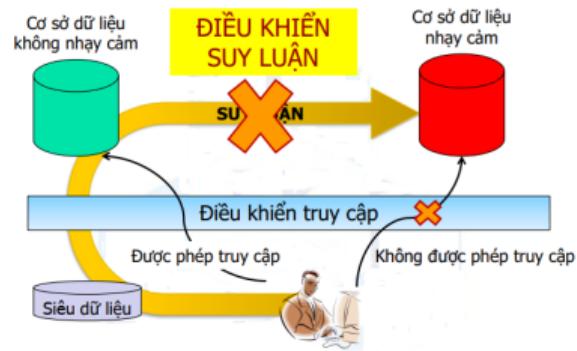
Điều khiển suy luận

- **Điều khiển suy luận (Inference control):** là việc quản lý, điều khiển các truy cập vào những cơ sở dữ liệu thống kê (statistical database) bởi vì từ những dữ liệu thống kê có thể suy luận ra được những thông tin nhạy cảm.
 - Tập dữ liệu X: user A có thể đọc
 - Tập dữ liệu Y: user A không được phép đọc
 - ... nhưng: $Y = f(X)$
→ Nếu user A biết được hàm f thì có thể tìm được tập Y (mà user A không được phép xem).



3. Các bước cơ bản trong ATBMTT

Điều khiển suy luận





3. Các bước cơ bản trong ATBMTT

Điều khiển dòng thông tin

- *Dòng thông tin (Information flow)* giữa đối tượng (object) X và đối tượng Y xảy ra khi có một chương trình đọc dữ liệu từ X và ghi vào Y.
- *Điều khiển dòng thông tin (Flow control)* nhằm ngăn chặn dòng thông tin đi từ đối tượng dữ liệu được bảo vệ sang đối tượng dữ liệu ít được bảo vệ hơn.



3. Các bước cơ bản trong ATBMTT

Điều khiển dòng thông tin

- **Kênh biến đổi (Covert Channels)** là những kênh truyền mà qua đó dòng thông tin có thể được truyền ngầm ra bên ngoài một cách bất hợp pháp.
- Có 2 loại convert channel:
 - Kênh lưu trữ (Storage channel): thông tin được truyền qua những đốï tượng lưu trữ trung gian
 - Kênh thời gian (Timing channel): một phần thông tin có thể bị lộ ra ngoài thông qua thời gian tính toán các dữ liệu liên quan đến thông tin đó.



3. Các bước cơ bản trong ATBMTT

Mã hóa

- *Mã hóa (Encryption)* là những giải thuật tính toán nhằm chuyển đổi những văn bản gốc (plaintext), dạng văn bản có thể đọc được, sang dạng văn bản mã hóa (ciphertext), dạng văn bản không thể đọc được.
- Chỉ người dùng có được khóa đúng mới có thể giải mã được văn bản mã hóa về dạng văn bản rõ ban đầu.
- Mã hóa dữ liệu được sử dụng để bảo vệ những dữ liệu nhạy cảm.



3. Các bước cơ bản trong ATBMTT

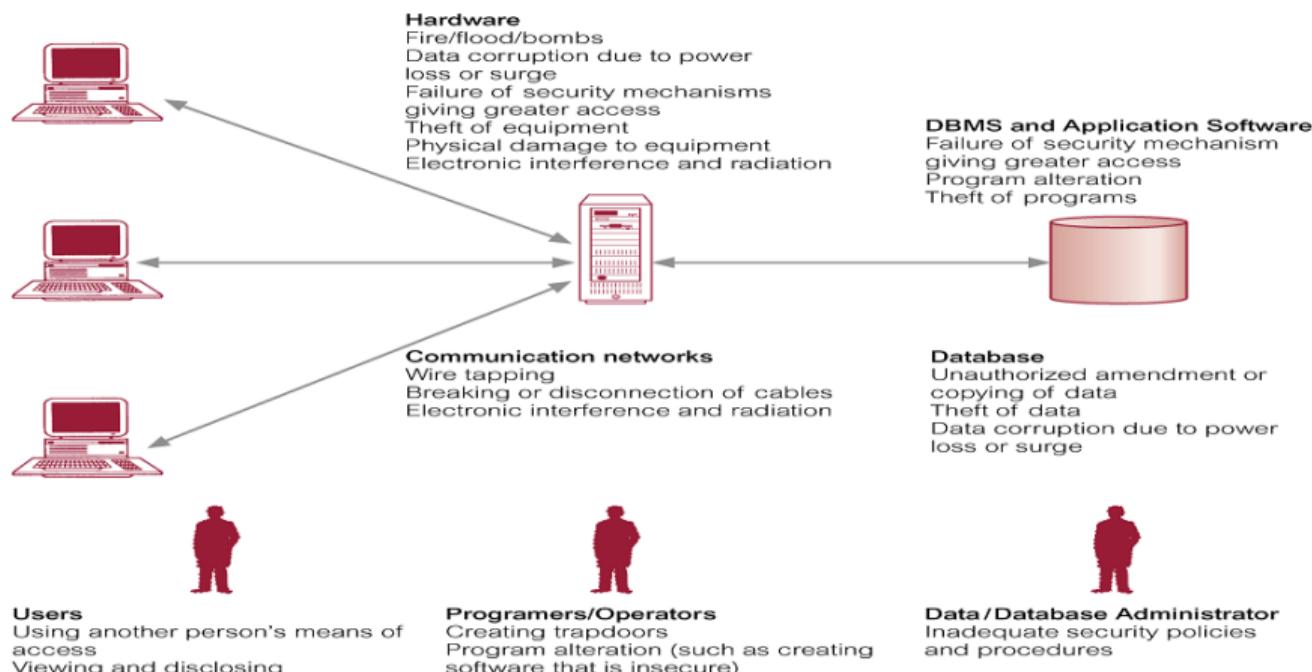
Các thành phần cần bảo vệ trong HTTT

- Phần cứng
- Mạng
- Cơ sở dữ liệu (CSDL)
- Hệ quản trị CSDL (database management system - DMBS), các ứng dụng
- Người dùng
- Người lập trình hệ thống
- Người quản trị CSDL



3. Các bước cơ bản trong ATBMTT

Các thành phần cần bảo vệ trong HTTT





Câu 1

Cách nào sau đây là tốt nhất để chống lại điểm yếu bảo mật trong phần mềm HDH ?

- A Cài đặt bản service pack mới nhất .
- B Cài đặt lại HDH thông dụng .
- C Sao lưu hệ thống thường xuyên .
- D Shut down hệ thống khi không sử dụng .



Câu 1

Cách nào sau đây là tốt nhất để chống lại điểm yếu bảo mật trong phần mềm HDH ?

- A Cài đặt bản service pack mới nhất .
- B Cài đặt lại HDH thông dụng .
- C Sao lưu hệ thống thường xuyên .
- D Shut down hệ thống khi không sử dụng .

Lời giải.



Câu 1

Cách nào sau đây là tốt nhất để chống lại điểm yếu bảo mật trong phần mềm HDH ?

- A Cài đặt bản service pack mới nhất .
- B Cài đặt lại HDH thông dụng .
- C Sao lưu hệ thống thường xuyên .
- D Shut down hệ thống khi không sử dụng .

Lời giải.

A



Câu 2

Các tập tin nào sau đây có khả năng chứa virus nhất ?

- (A) database.dat .
- (B) bigpic.jpeg .
- (C) note.txt .
- (D) picture.gif.exe .



Câu 2

Các tập tin nào sau đây có khả năng chứa virus nhất ?

- A database.dat .
- B bigpic.jpeg .
- C note.txt .
- D picture.gif.exe .

Lời giải.



Câu 2

Các tập tin nào sau đây có khả năng chứa virus nhất ?

- (A) database.dat . (B) bigpic.jpeg . (C) note.txt . (D) picture.gif.exe .

Lời giải.

D



Câu 3

Mật khẩu nào sau đây là khó phá nhất đối với một hacker ?

- A password83 .
- B reception .
- C !\$aLtNb83 .
- D LaT3r .



Câu 3

Mật khẩu nào sau đây là khó phá nhất đối với một hacker ?

- A password83 .
- B reception .
- C !\$aLtNb83 .
- D LaT3r .

Lời giải.



Câu 3

Mật khẩu nào sau đây là khó phá nhất đối với một hacker ?

- A password83 .
- B reception .
- C !\$aLtNb83 .
- D LaT3r .

Lời giải.

C



Câu 4

Chiều dài tối thiểu của mật khẩu cần phải là

- (A) 12 đến 15 ký tự .
- (B) 3 đến 5 ký tự .
- (C) 8 ký tự .
- (D) 1 đến 3 ký tự .



Câu 4

Chiều dài tối thiểu của mật khẩu cần phải là

- (A) 12 đến 15 ký tự . (B) 3 đến 5 ký tự . (C) 8 ký tự . (D) 1 đến 3 ký tự .

Lời giải.



Câu 4

Chiều dài tối thiểu của mật khẩu cần phải là

- (A) 12 đến 15 ký tự . (B) 3 đến 5 ký tự . (C) 8 ký tự . (D) 1 đến 3 ký tự .

Lời giải.

C



Câu 5

Bạn mới nhận cuộc gọi từ một user trong văn phòng mà user này đang ghé thăm một website quảng cáo. User này đang phàn nàn rằng hệ thống của anh ta không phản ứng và hàng triệu trang web đang mở trên màn hình của anh ta. Loại tấn công này là gì ?

- A DoS .
- B Mã nguồn độc hại .
- C Giả mạo IP .
- D Khảo sát định vị .



Câu 5

Bạn mới nhận cuộc gọi từ một user trong văn phòng mà user này đang ghé thăm một website quảng cáo. User này đang phàn nàn rằng hệ thống của anh ta không phản ứng và hàng triệu trang web đang mở trên màn hình của anh ta. Loại tấn công này là gì ?

- A DoS .
- B Mã nguồn độc hại .
- C Giả mạo IP .
- D Khảo sát định vị .

Lời giải.



Câu 5

Bạn mới nhận cuộc gọi từ một user trong văn phòng mà user này đang ghé thăm một website quảng cáo. User này đang phàn nàn rằng hệ thống của anh ta không phản ứng và hàng triệu trang web đang mở trên màn hình của anh ta. Loại tấn công này là gì ?

- A DoS .
- B Mã nguồn độc hại .
- C Giả mạo IP .
- D Khảo sát định vị .

Lời giải.

A



Câu 6

Chính sách tài khoản nào nên được thiết lập để ngăn chặn các cuộc tấn công ác ý vào tài khoản của user?

- A Disable tài khoản không dùng đến .
- B Hạn chế thời gian .
- C Ngày hết hạn tài khoản .
- D Giới hạn số lần logon .



Câu 6

Chính sách tài khoản nào nên được thiết lập để ngăn chặn các cuộc tấn công ác ý vào tài khoản của user?

- A Disable tài khoản không dùng đến .
- B Hạn chế thời gian .
- C Ngày hết hạn tài khoản .
- D Giới hạn số lần logon .

Lời giải.



Câu 6

Chính sách tài khoản nào nên được thiết lập để ngăn chặn các cuộc tấn công ác ý vào tài khoản của user?

- A Disable tài khoản không dùng đến .
- B Hạn chế thời gian .
- C Ngày hết hạn tài khoản .
- D Giới hạn số lần logon .

Lời giải.

D



Câu 7

Sau khi một user đã được định danh (identified), điều gì cần phải làm trước khi họ log vào một mạng máy tính ?

- A Xác thực với mật khẩu .
- B Họ phải nhập user ID đã được mã hóa .
- C Được phép truy cập với mức ưu tiên được thiết lập.
- D Người quản trị phải enable để gõ vào .



Câu 7

Sau khi một user đã được định danh (identified), điều gì cần phải làm trước khi họ log vào một mạng máy tính ?

- A Xác thực với mật khẩu .
- B Họ phải nhập user ID đã được mã hóa .
- C Được phép truy cập với mức ưu tiên được thiết lập.
- D Người quản trị phải enable để gõ vào .

Lời giải.



Câu 7

Sau khi một user đã được định danh (identified), điều gì cần phải làm trước khi họ log vào một mạng máy tính ?

- A Xác thực với mật khẩu .
- B Họ phải nhập user ID đã được mã hóa .
- C Được phép truy cập với mức ưu tiên được thiết lập.
- D Người quản trị phải enable để gõ vào .

Lời giải.

A



Câu 8

Ở hệ mật mã nào người gửi và người nhận thông điệp sử dụng cùng một khóa mã khi mã hóa và giải mã ?

- A Không đối xứng
- B Đối xứng .
- C RSA .
- D Diffie-Hellman .



Câu 8

Ở hệ mật mã nào người gửi và người nhận thông điệp sử dụng cùng một khóa mã khi mã hóa và giải mã ?

- (A) Không đối xứng (B) Đối xứng . (C) RSA . (D) Diffie-Hellman .

Lời giải.



Câu 8

Ở hệ mật mã nào người gửi và người nhận thông điệp sử dụng cùng một khóa mã khi mã hóa và giải mã ?

- (A) Không đối xứng (B) Đối xứng . (C) RSA . (D) Diffie-Hellman .

Lời giải.

B



Câu 9

Ở hệ mật mã nào người gửi và người nhận thông điệp sử dụng các khóa khác nhau khi mã hóa và giải mã ?

- (A) Skipjack .
- (B) Blowfish .
- (C) Không đối xứng .
- (D) Đối xứng .



Câu 9

Ở hệ mật mã nào người gửi và người nhận thông điệp sử dụng các khóa khác nhau khi mã hóa và giải mã ?

- (A) Skipjack . (B) Blowfish . (C) Không đối xứng . (D) Đối xứng .

Lời giải.



Câu 9

Ở hệ mật mã nào người gửi và người nhận thông điệp sử dụng các khóa khác nhau khi mã hóa và giải mã ?

- (A) Skipjack . (B) Blowfish . (C) Không đối xứng . (D) Đối xứng .

Lời giải.

C



Câu 10

Sau khi một user được định danh và xác thực hệ thống, để cho phép user sử dụng tài nguyên bạn phải thực hiện điều gì?

- A Phải được ủy quyền .
- B Được truyền lại .
- C Được mã hóa .
- D Được enable .



Câu 10

Sau khi một user được định danh và xác thực hệ thống, để cho phép user sử dụng tài nguyên bạn phải thực hiện điều gì?

- A Phải được ủy quyền .
- B Được truyền lại .
- C Được mã hóa .
- D Được enable .

Lời giải.



Câu 10

Sau khi một user được định danh và xác thực hệ thống, để cho phép user sử dụng tài nguyên bạn phải thực hiện điều gì?

- A Phải được ủy quyền .
- B Được truyền lại .
- C Được mã hóa .
- D Được enable .

Lời giải.

A



Câu 11

Một user gọi điện đến cho ta (với tư cách là người quản lý) thông báo họ bị mất mật khẩu và cần truy cập ngay lập tức. Ta nên làm gì ?

- A Cung cấp truy cập ngay lập tức, và sau đó kiểm tra chứng cứ của họ .
- B Tạo một login và mật khẩu tạm thời để họ sử dụng .
- C Xác minh định danh của họ trước khi cấp quyền truy cập .
- D Cho họ một mật khẩu riêng tạm thời .



Câu 11

Một user gọi điện đến cho ta (với tư cách là người quản lý) thông báo họ bị mất mật khẩu và cần truy cập ngay lập tức. Ta nên làm gì ?

- A Cung cấp truy cập ngay lập tức, và sau đó kiểm tra chứng cứ của họ .
- B Tạo một login và mật khẩu tạm thời để họ sử dụng .
- C Xác minh định danh của họ trước khi cấp quyền truy cập .
- D Cho họ một mật khẩu riêng tạm thời .

Lời giải.



Câu 11

Một user gọi điện đến cho ta (với tư cách là người quản lý) thông báo họ bị mất mật khẩu và cần truy cập ngay lập tức. Ta nên làm gì ?

- A Cung cấp truy cập ngay lập tức, và sau đó kiểm tra chứng cứ của họ .
- B Tạo một login và mật khẩu tạm thời để họ sử dụng .
- C Xác minh định danh của họ trước khi cấp quyền truy cập .
- D Cho họ một mật khẩu riêng tạm thời .

Lời giải.

C



Câu 12

Khi một user báo cáo rằng hệ thống của anh ta đã phát hiện một virus mới. Điều gì sau đây cần làm như là bước đầu tiên để xử lý tình huống này ?

- A Kiểm tra lại tập tin diệt virus hiện hành .
- B Định dạng lại đĩa cứng .
- C Cài đặt lại hệ điều hành .
- D Disable tài khoản email của anh ta.



Câu 12

Khi một user báo cáo rằng hệ thống của anh ta đã phát hiện một virus mới. Điều gì sau đây cần làm như là bước đầu tiên để xử lý tình huống này ?

- A Kiểm tra lại tập tin diệt virus hiện hành .
- B Định dạng lại đĩa cứng .
- C Cài đặt lại hệ điều hành .
- D Disable tài khoản email của anh ta.

Lời giải.



Câu 12

Khi một user báo cáo rằng hệ thống của anh ta đã phát hiện một virus mới. Điều gì sau đây cần làm như là bước đầu tiên để xử lý tình huống này ?

- A Kiểm tra lại tập tin diệt virus hiện hành .
- B Định dạng lại đĩa cứng .
- C Cài đặt lại hệ điều hành .
- D Disable tài khoản email của anh ta.

Lời giải.

D



Câu 13

Một chương trình nằm trong một chương trình khác được cài vào hệ thống gọi là một ...

- A Trojan Horse .
- B Polymorphic virus .
- C Sâu .
- D Armored virus .



Câu 13

Một chương trình nằm trong một chương trình khác được cài vào hệ thống gọi là một ...

- (A) Trojan Horse .
- (B) Polymorphic virus .
- (C) Sâu .
- (D) Armored virus .

Lời giải.



Câu 13

Một chương trình nằm trong một chương trình khác được cài vào hệ thống gọi là một ...

- A Trojan Horse .
- B Polymorphic virus .
- C Sâu .
- D Armored virus .

Lời giải.

A



Câu 14

Một máy chủ trên mạng có một chương trình đang chạy vượt quá thẩm quyền. Loại tấn công nào đã xảy ra ?

- A DoS .
- B DDoS .
- C Back door .
- D Social engineering (Khai thác giao tiếp) .



Câu 14

Một máy chủ trên mạng có một chương trình đang chạy vượt quá thẩm quyền. Loại tấn công nào đã xảy ra ?

- A DoS .
- B DDoS .
- C Back door .
- D Social engineering (Khai thác giao tiếp) .

Lời giải.



Câu 14

Một máy chủ trên mạng có một chương trình đang chạy vượt quá thẩm quyền. Loại tấn công nào đã xảy ra ?

- A DoS .
- B DDoS .
- C Back door .
- D Social engineering (Khai thác giao tiếp) .

Lời giải.

C



Câu 15

Loại virus tự che giấu nó bằng cách ẩn trong mã nguồn của các phần mềm antivirus được gọi là gì ?

- A Armored virus .
- B Polymorphic virus .
- C Sâu .
- D Stealth virus (Virus ẩn danh) .



Câu 15

Loại virus tự che giấu nó bằng cách ẩn trong mã nguồn của các phần mềm antivirus được gọi là gì ?

- A Armored virus .
- B Polymorphic virus .
- C Sâu .
- D Stealth virus (Virus ẩn danh) .

Lời giải.



Câu 15

Loại virus tự che giấu nó bằng cách ẩn trong mã nguồn của các phần mềm antivirus được gọi là gì ?

- A Armored virus .
- B Polymorphic virus .
- C Sâu .
- D Stealth virus (Virus ẩn danh) .

Lời giải.

B



Câu 16

Các user nội bộ báo cáo hệ thống của họ bị lây nhiễm nhiều lần. Trong mọi trường hợp virus có vẻ là cùng một loại. Thủ phạm thích hợp nhất là gì ?

- A Máy chủ có thể là vật mang virus .
- B Ta có một sâu virus.
- C Phần mềm antivirus của ta bị sự cố .
- D Tấn công DoS đang thực hiện .



Câu 16

Các user nội bộ báo cáo hệ thống của họ bị lây nhiễm nhiều lần. Trong mọi trường hợp virus có vẻ là cùng một loại. Thủ phạm thích hợp nhất là gì ?

- A Máy chủ có thể là vật mang virus .
- B Ta có một sâu virus.
- C Phần mềm antivirus của ta bị sự cố .
- D Tấn công DoS đang thực hiện .

Lời giải.



Câu 16

Các user nội bộ báo cáo hệ thống của họ bị lây nhiễm nhiều lần. Trong mọi trường hợp virus có vẻ là cùng một loại. Thủ phạm thích hợp nhất là gì ?

- A Máy chủ có thể là vật mang virus .
- B Ta có một sâu virus.
- C Phần mềm antivirus của ta bị sự cố .
- D Tấn công DoS đang thực hiện .

Lời giải.

A



Câu 17

Một đêm làm việc khuya và bạn phát hiện rằng ổ cứng của bạn hoạt động rất tích cực mặc dù bạn không thực hiện bất kỳ thao tác nào trên máy tính. Bạn nghi ngờ điều gì?

- A Khả năng ổ đĩa ngừng hoạt động sắp xảy ra .
- B Một virus đang phát tán rộng trong hệ thống .
- C Hệ thống của bạn đang chịu tác động của tấn công DoS .
- D Tấn công TCP/IP hijacking đang cố gắng thực hiện .



Câu 17

Một đêm làm việc khuya và bạn phát hiện rằng ổ cứng của bạn hoạt động rất tích cực mặc dù bạn không thực hiện bất kỳ thao tác nào trên máy tính. Bạn nghi ngờ điều gì?

- A Khả năng ổ đĩa ngừng hoạt động sắp xảy ra .
- B Một virus đang phát tán rộng trong hệ thống .
- C Hệ thống của bạn đang chịu tác động của tấn công DoS .
- D Tấn công TCP/IP hijacking đang cố gắng thực hiện .

Lời giải.



Câu 17

Một đêm làm việc khuya và bạn phát hiện rằng ổ cứng của bạn hoạt động rất tích cực mặc dù bạn không thực hiện bất kỳ thao tác nào trên máy tính. Bạn nghi ngờ điều gì?

- A Khả năng ổ đĩa ngừng hoạt động sắp xảy ra .
- B Một virus đang phát tán rộng trong hệ thống .
- C Hệ thống của bạn đang chịu tác động của tấn công DoS .
- D Tấn công TCP/IP hijacking đang cố gắng thực hiện .

Lời giải.

B



Câu 18

Khi được hỏi về các mối đe dọa cho công ty từ phía các hacker. Loại thông tin nào sau đây sẽ giúp ích nhiều nhất ?

- A Xác minh tài sản sở hữu .
- B Đánh giá rủi ro .
- C Nhận dạng mối đe dọa .
- D Các điểm yếu .



Câu 18

Khi được hỏi về các mối đe dọa cho công ty từ phía các hacker. Loại thông tin nào sau đây sẽ giúp ích nhiều nhất ?

- A Xác minh tài sản sở hữu .
- B Đánh giá rủi ro .
- C Nhận dạng mối đe dọa .
- D Các điểm yếu .

Lời giải.



Câu 18

Khi được hỏi về các mối đe dọa cho công ty từ phía các hacker. Loại thông tin nào sau đây sẽ giúp ích nhiều nhất ?

- A Xác minh tài sản sở hữu .
- B Đánh giá rủi ro .
- C Nhận dạng mối đe dọa .
- D Các điểm yếu .

Lời giải.

D



Câu 19

Hệ mã Cesar mã hóa $x \in [0; 25]$ thành $y = x + 3 \bmod 26$. Hãy cho biết nếu giá trị bản rõ là 10 thì giá trị bản mã tương ứng là

- (A) 5.
- (B) 7.
- (C) 13.
- (D) 15.



Câu 19

Hệ mã Cesar mã hóa $x \in [0; 25]$ thành $y = x + 3 \bmod 26$. Hãy cho biết nếu giá trị bản rõ là 10 thì giá trị bản mã tương ứng là

- (A) 5. (B) 7. (C) 13. (D) 15.

Lời giải.



Câu 19

Hệ mã Cesar mã hóa $x \in [0; 25]$ thành $y = x + 3 \bmod 26$. Hãy cho biết nếu giá trị bản rõ là 10 thì giá trị bản mã tương ứng là

- (A) 5. (B) 7. (C) 13. (D) 15.

Lời giải.

C



Câu 20

Hệ mã Affine mã hóa $x \in [0; 25]$ thành $y = 3x + 5 \text{ mod } 26$. Hãy cho biết nếu giá trị bản mã là 10 thì giá trị bản rõ tương ứng là

- (A) 9.
- (B) 14.
- (C) 19.
- (D) 23.



Câu 20

Hệ mã Affine mã hóa $x \in [0; 25]$ thành $y = 3x + 5 \text{ mod } 26$. Hãy cho biết nếu giá trị bản mã là 10 thì giá trị bản rõ tương ứng là

- (A) 9. (B) 14. (C) 19. (D) 23.

Lời giải.



Câu 20

Hệ mã Affine mã hóa $x \in [0; 25]$ thành $y = 3x + 5 \text{ mod } 26$. Hãy cho biết nếu giá trị bản mã là 10 thì giá trị bản rõ tương ứng là

- (A) 9. (B) 14. (C) 19. (D) 23.

Lời giải.

C



TRAO ĐỔI