



HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG



BÀI GIẢNG MÔN HỌC
AN TOÀN ỨNG DỤNG WEB & CSDL
CHƯƠNG 5 – TỔNG QUAN VỀ
BẢO MẬT CƠ SỞ DỮ LIỆU

Giảng viên:

E-mail:

Khoa:

PGS.TS. Hoàng Xuân Dậu

dauhx@ptit.edu.vn

An toàn thông tin

Phần II – An toàn cơ sở dữ liệu

- 5. Tổng quan về an toàn cơ sở dữ liệu
- 6. Các cơ chế bảo mật cơ sở dữ liệu
- 7. Sao lưu, khôi phục dự phòng, kiểm toán và giám sát hoạt động CSDL

NỘI DUNG CHƯƠNG 5

1. Các khái niệm chung
2. Các yêu cầu bảo mật cơ sở dữ liệu
3. Mô hình tổng quát bảo mật cơ sở dữ liệu
4. Các lớp bảo mật cơ sở dữ liệu
5. Các dạng tấn công thường gặp lên CSDL
6. Top 10 lỗ hổng bảo mật CSDL trên thực tế

5.1 Các khái niệm chung

- ❖ Cơ sở dữ liệu (Database) là một trong các ứng dụng đặc biệt quan trọng, được sử dụng rất phổ biến để:
 - Hỗ trợ các ứng dụng lưu trữ và quản lý thông tin: Hầu hết các ứng dụng trong các cơ quan, tổ chức và doanh nghiệp đều sử dụng các CSDL để lưu trữ và quản lý các thông tin.
 - Lưu trữ an toàn các thông tin nhạy cảm: Các CSDL quan hệ hỗ trợ nhiều kỹ thuật an toàn, tin cậy để lưu trữ các thông tin quan trọng.
 - Xử lý các giao dịch trực tuyến: Các CSDL hỗ trợ các thao tác xem, cập nhật dữ liệu nhanh chóng, hiệu quả.
 - Quản lý các kho dữ liệu: Hỗ trợ lưu trữ và quản lý các dữ liệu rất lớn.

5.1 Các khái niệm chung

- ❖ Một cơ sở dữ liệu là một tập hợp các dữ liệu có quan hệ với nhau:
 - Các dữ liệu có thể có quan hệ logic/vật lý chặt chẽ hoặc lỏng lẻo;
 - Dữ liệu trong các CSDL quan hệ có quan hệ logic tương đối chặt chẽ (thông qua các trường khóa).
 - Dữ liệu trong bảng tính Excel có thể có quan hệ lỏng lẻo.

5.1 Các khái niệm chung

- Kích thước CSDL có thể rất lớn:
 - Trang Amazon.com – nhà bán lẻ lớn nhất thế giới
 - 59 triệu khách hàng hoạt động
 - Lưu trữ khoảng hơn 20 triệu mục dữ liệu (Sách, CDs, trò chơi,...);
 - 250.000 sách trực tuyến;
 - Tổng lượng dữ liệu lưu trữ là hơn 42 TB (42.000 GB).
 - CSDL của Facebook.com lưu trữ hồ sơ của hơn 2,7 tỷ người dùng thường xuyên trong tháng (tính đến tháng 8.2020).
 - Trong đó có 1,79 tỷ người dùng hàng ngày.

5.1 Các khái niệm chung

- ❖ Hệ quản trị CSDL (Database Management System - DBMS) là một tập các chương trình cho phép người dùng tạo lập và duy trì các CSDL:
 - Cho phép thực hiện các thao tác CSDL:
 - Định nghĩa: Khai báo các kiểu, cấu trúc và ràng buộc dữ liệu;
 - Xây dựng: Liên quan đến việc lưu trữ dữ liệu trên các phương tiện lưu trữ do DBMS quản lý;
 - Xử lý: Cho phép thực hiện các thao tác truy vấn, thêm, sửa, xóa dữ liệu;
 - Chia sẻ: Cho phép nhiều người dùng cùng truy nhập, chia sẻ dữ liệu.

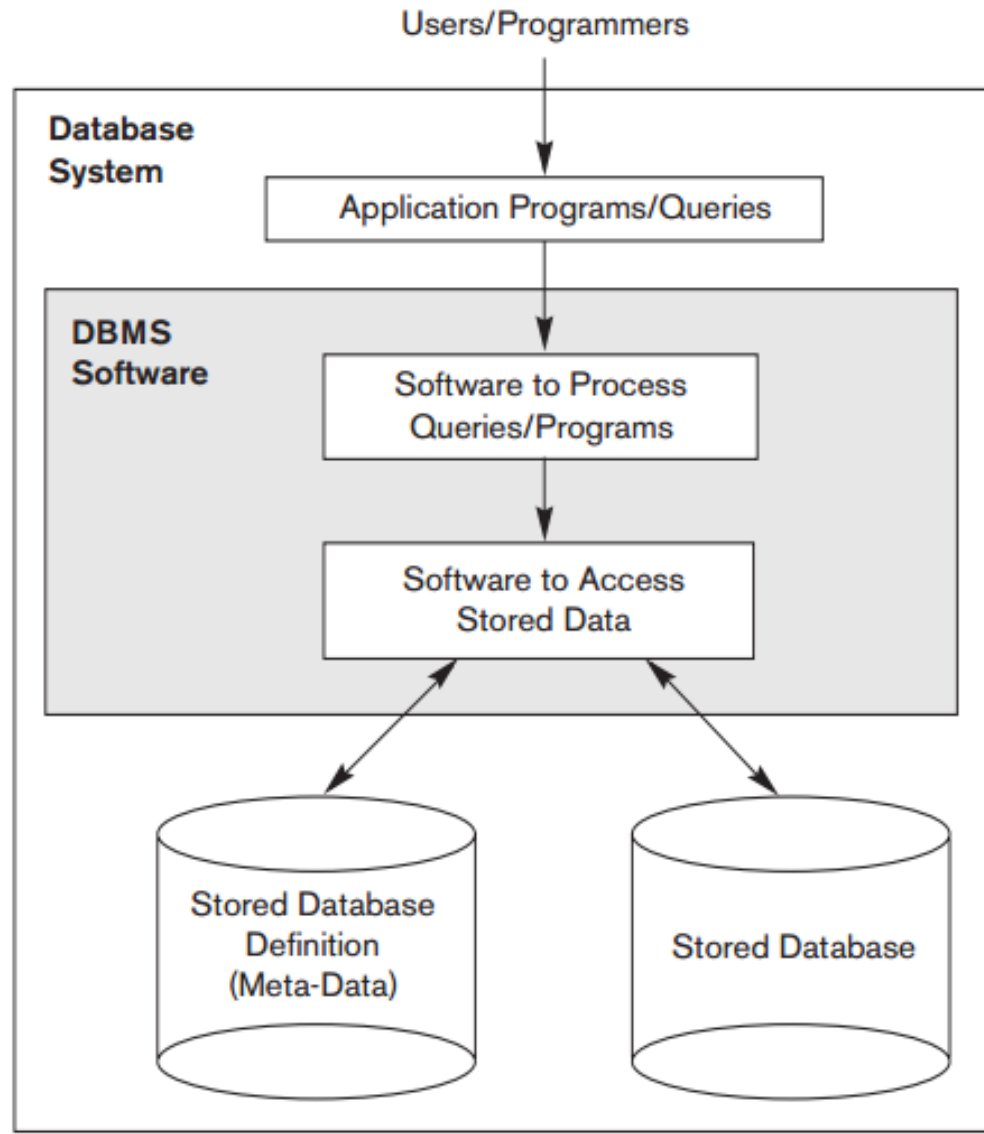
5.1 Các khái niệm chung

- Các hệ quản trị CSDL quan hệ phổ biến:
 - Oracle RDBMS
 - IBM DB2
 - Microsoft SQL Server
 - MySQL
 - SAP Sybase
 - Informix
 - PostgreSQL
 - SQLite
 - MariaDB
 - Microsoft Access,...

5.1 Các khái niệm chung

❖ Hệ thống CSDL (Database System) bao gồm:

- Các CSDL và
- Hệ quản trị CSDL.



5.1 Các khái niệm chung

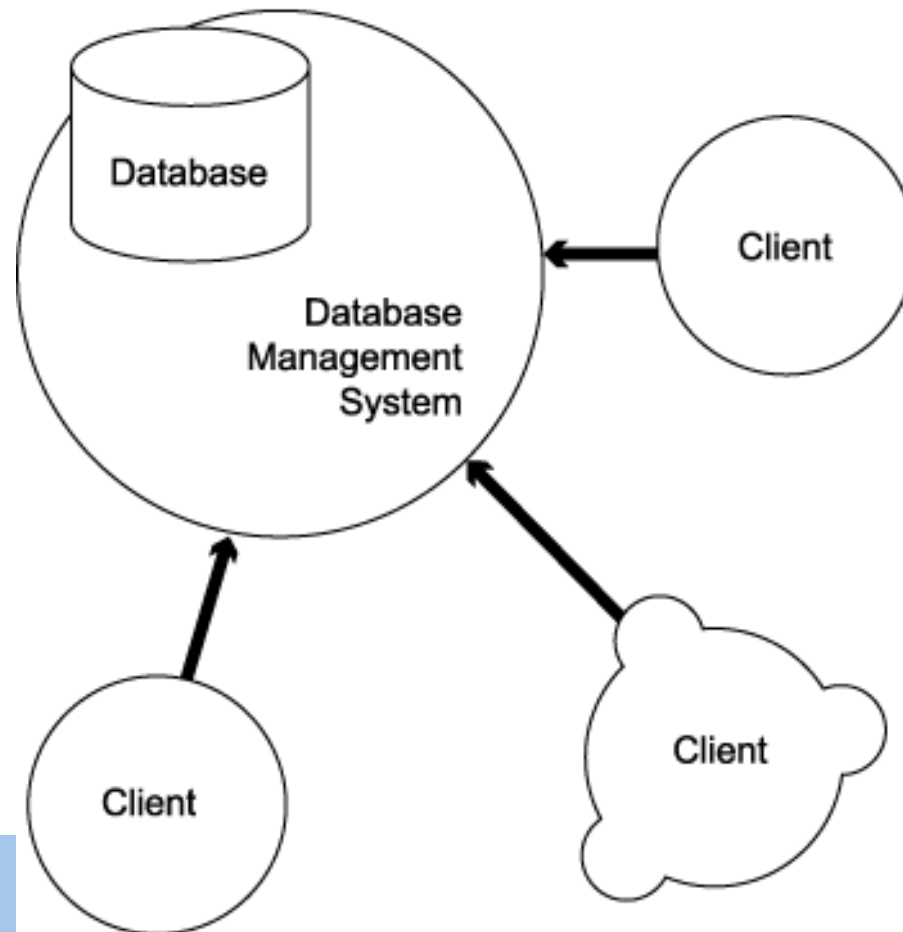
❖ Các mô hình truy nhập CSDL:

- Người dùng/máy khách truy nhập trực tiếp CSDL
- Người dùng/máy khách truy nhập gián tiếp CSDL
- Người dùng/máy khách truy nhập gián tiếp CSDL (có tường lửa riêng).

5.1 Các khái niệm chung

❖ Các mô hình truy nhập CSDL:

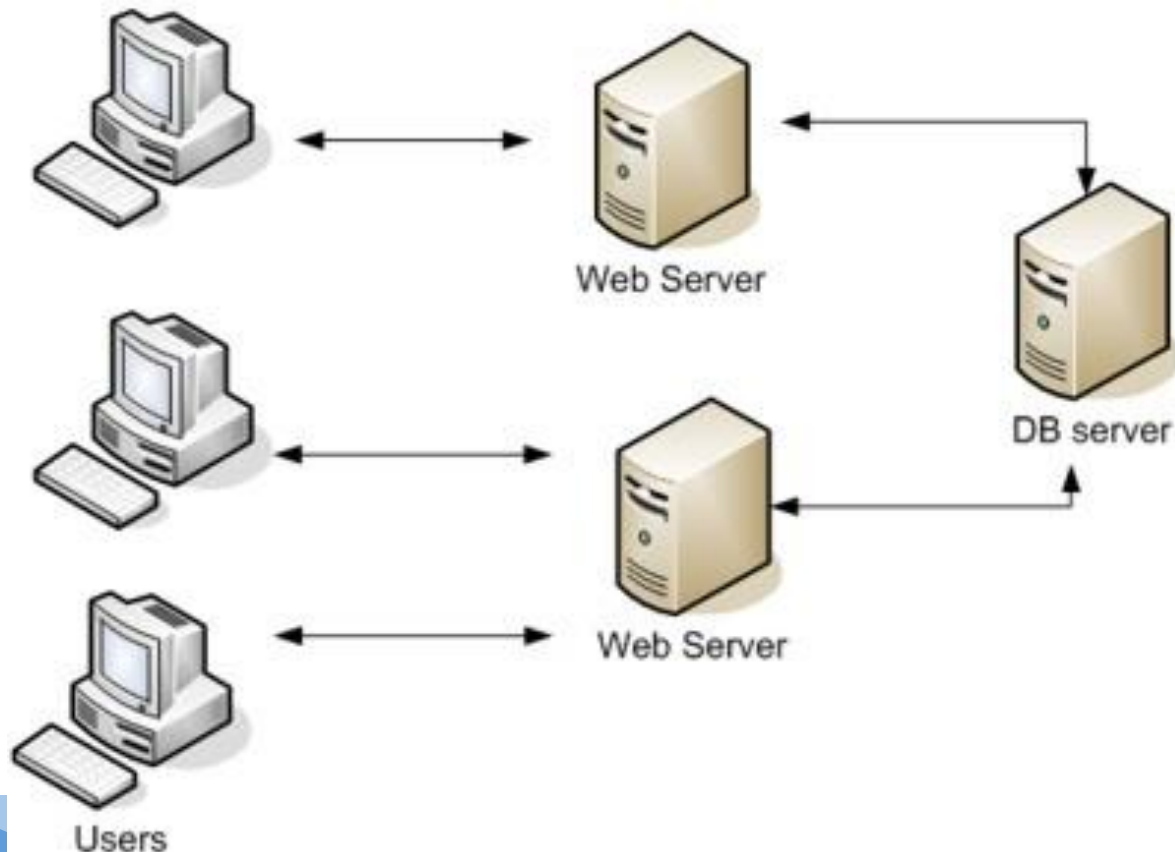
- Người dùng/máy khách truy nhập trực tiếp CSDL:



5.1 Các khái niệm chung

❖ Các mô hình truy nhập CSDL:

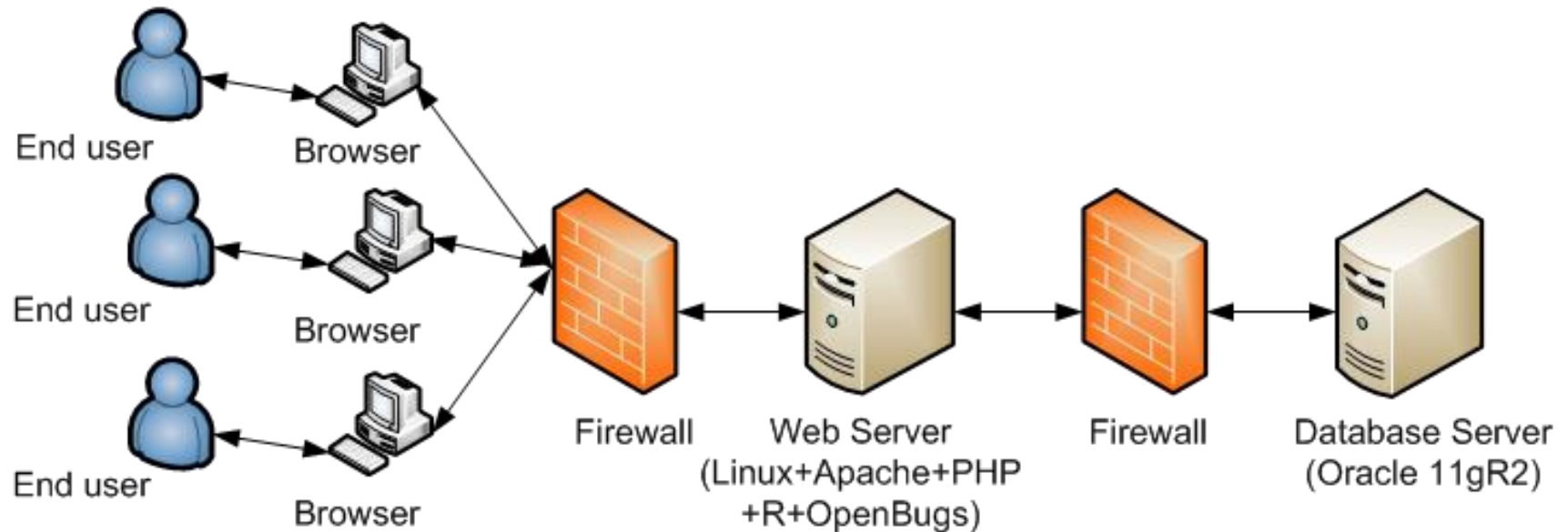
- Người dùng/máy khách truy nhập gián tiếp CSDL:



5.1 Các khái niệm chung

❖ Các mô hình truy nhập CSDL:

- Người dùng/máy khách truy nhập gián tiếp CSDL (có tường lửa riêng cho CSDL):

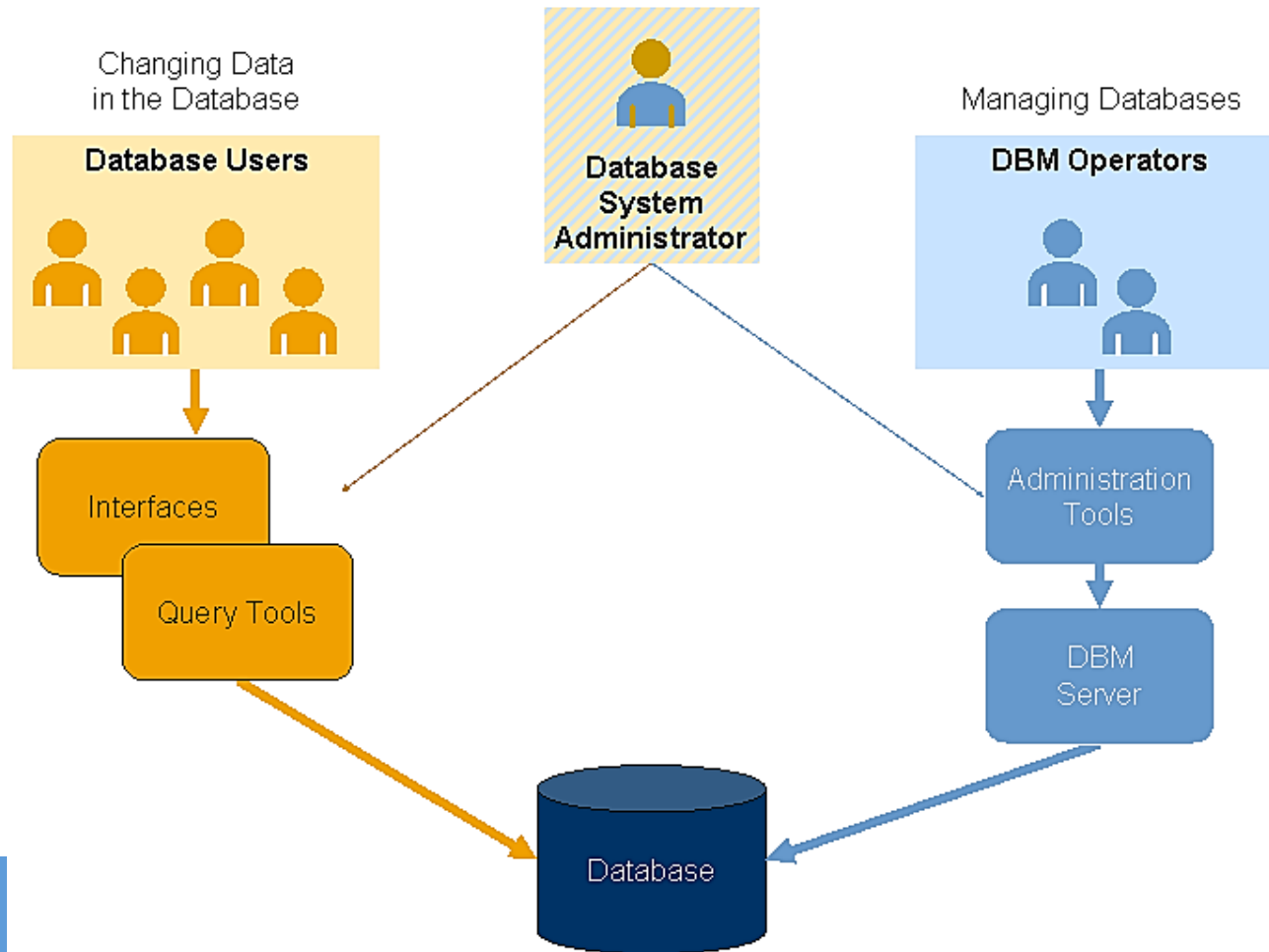


5.1 Các khái niệm chung

- ❖ Các đối tượng (objects) chính trong CSDL:
 - User (Người dùng)
 - Table (Bảng)
 - View (Khung nhìn)
 - Stored Procedure (Thủ tục)
 - Function (Hàm)

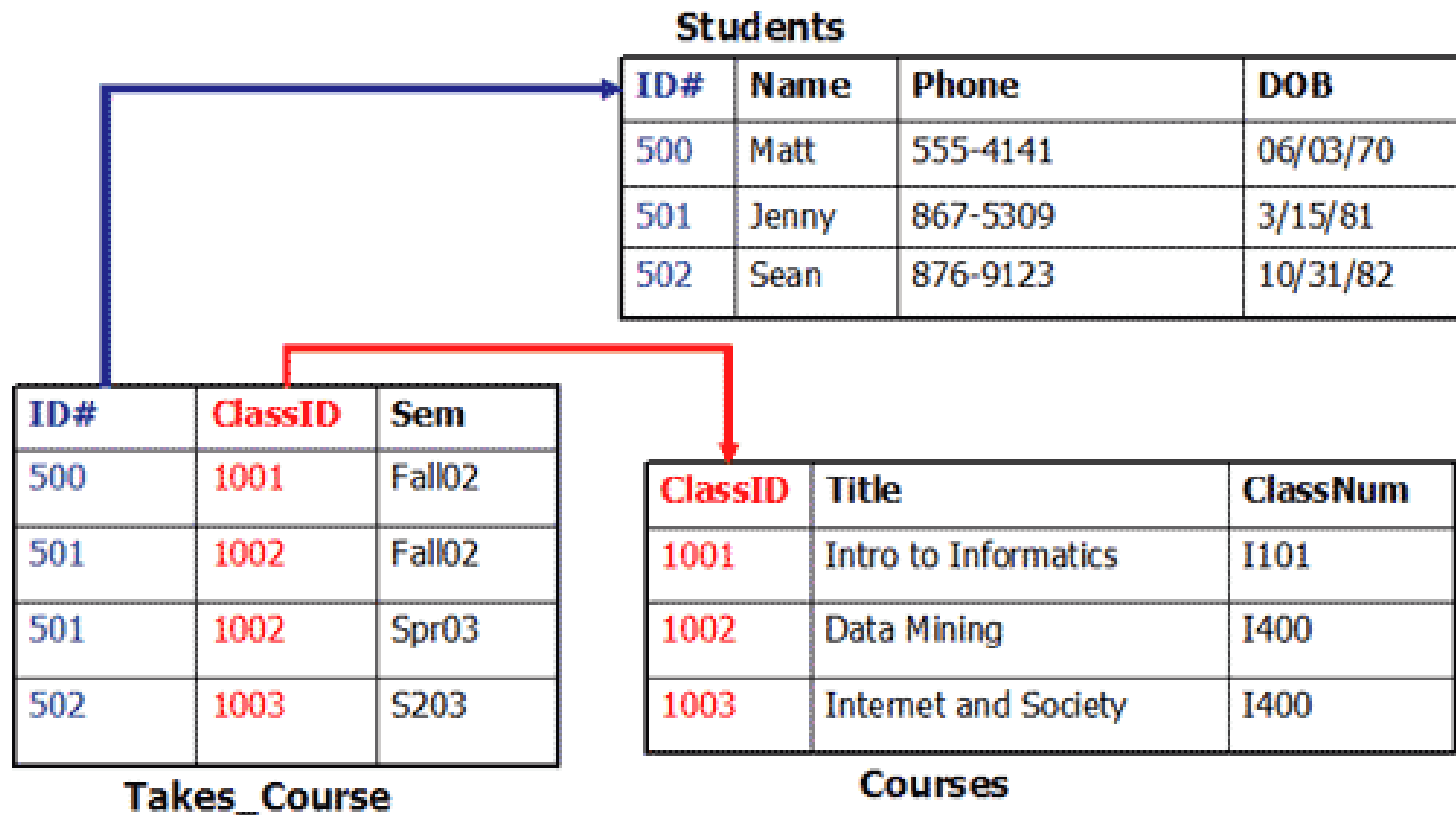
5.1 Các khái niệm chung

- User (Người dùng): Là người dùng CSDL, được phép truy nhập và thực hiện các thao tác dữ liệu theo vai trò (role) được gán sẵn.



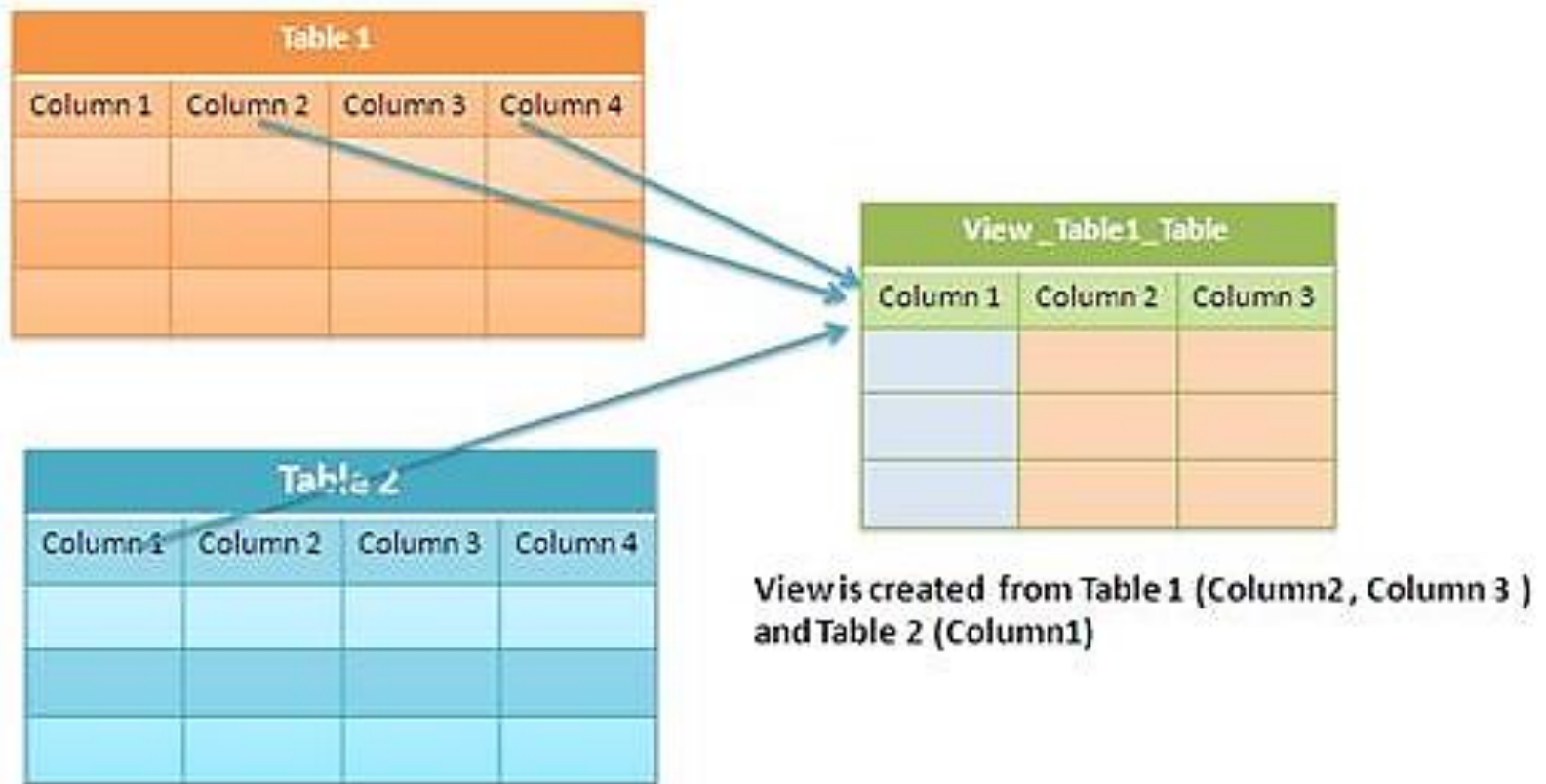
5.1 Các khái niệm chung

- Table (Bảng): Gồm các cột (thuộc tính, trường) và các dòng (bản ghi) để quản lý và lưu trữ dữ liệu.



5.1 Các khái niệm chung

- View (Khung nhìn): Là các bảng logic được tạo bởi các câu lệnh truy vấn dữ liệu.



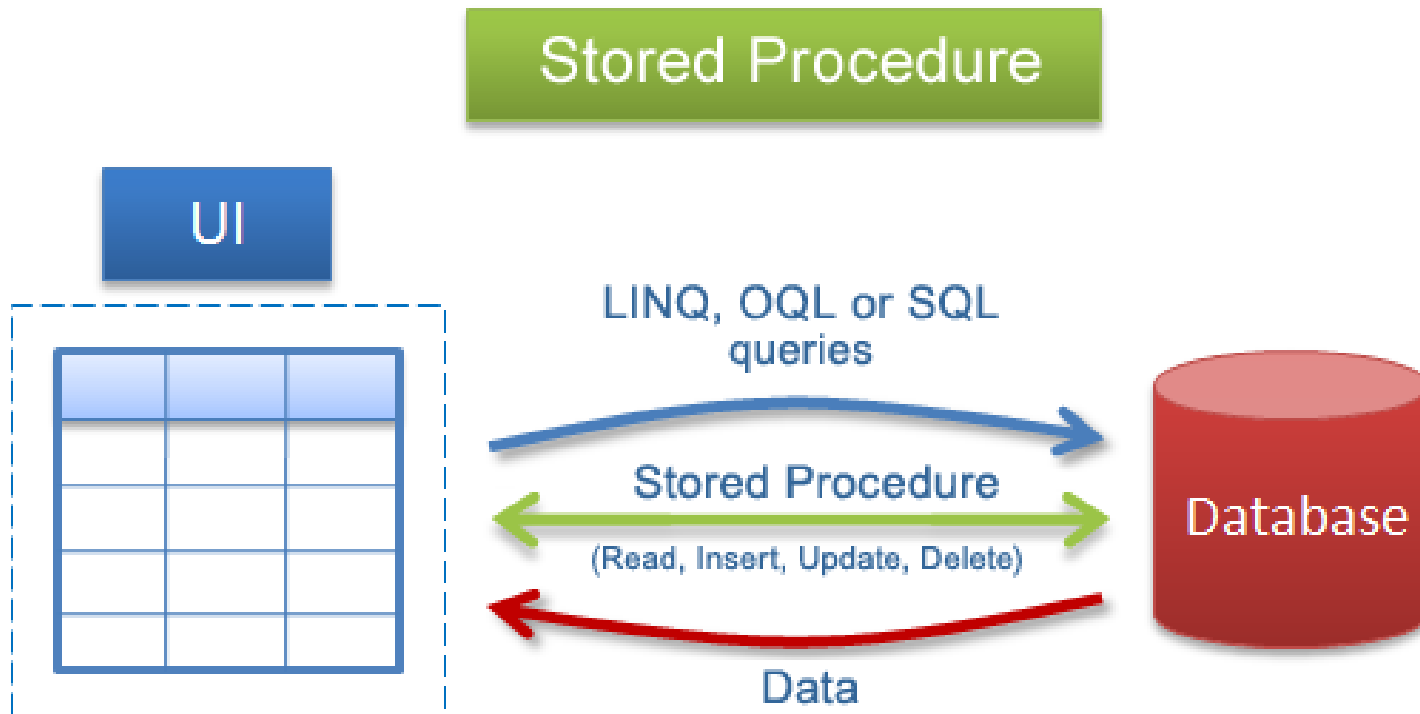
5.1 Các khái niệm chung

- Stored Procedure (Thủ tục): Gồm một tập các câu lệnh xử lý dữ liệu;
 - Thủ tục chấp nhận các tham số đầu vào;
 - Thủ tục được lưu trong CSDL và đã được dịch nên nhanh hơn các câu truy vấn trực tiếp/truy vấn động.

```
SET ANSI_NULLS ON
GO
SET QUOTED_IDENTIFIER ON
GO
-- =====
-- Author:      <Author,,Name>
-- Create date: <Create Date,,>
-- Description: <Description,,>
-- =====
ALTER PROCEDURE <ProcedureName>
    -- Add the parameters for the stored procedure here
    <@Parameter1> <Datatype_For_Parameter1> = <Default_Value>,
    <@Parameter1> <Datatype_For_Parameter1> = <Default_Value>
AS
BEGIN
    -- Insert statements for procedure here
    SELECT * FROM TableName
END
GO
```

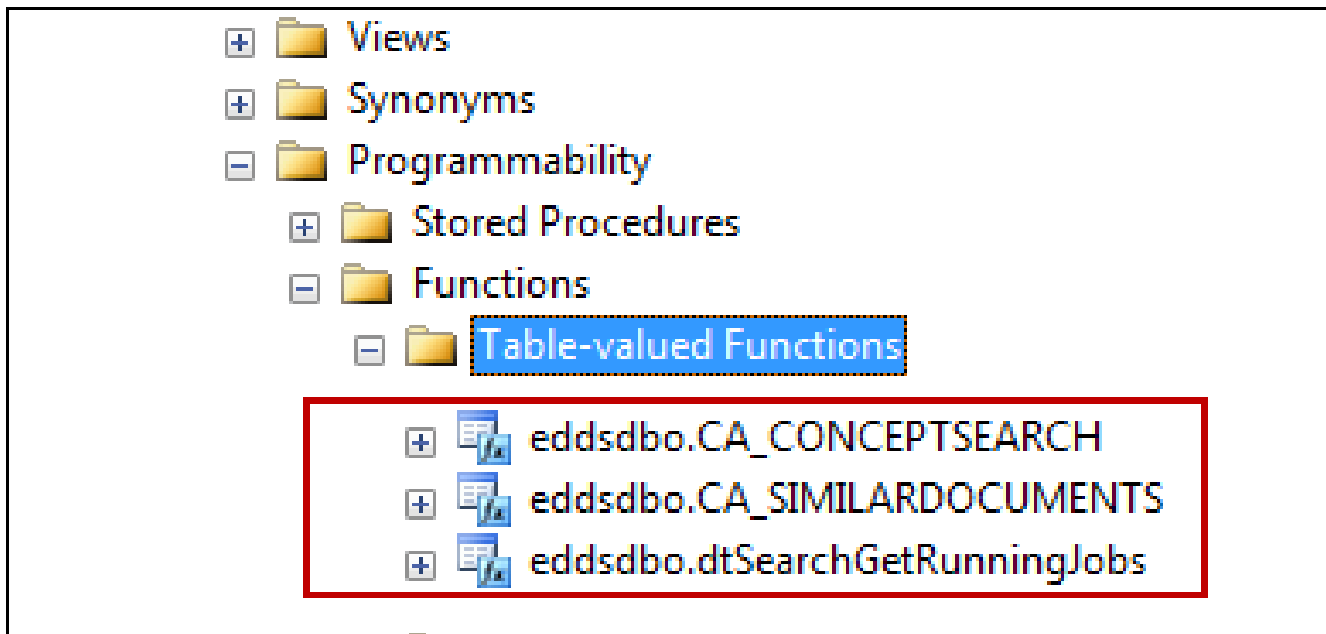
5.1 Các khái niệm chung

- Stored Procedure (Thủ tục): Gọi thực hiện thủ tục từ ứng dụng



5.1 Các khái niệm chung

- Function (Hàm): Gồm một tập các câu lệnh xử lý dữ liệu;
 - Hàm chấp nhận các tham số đầu vào;
 - Hàm nhận giá trị trả về (có thể là giá trị đơn hoặc một bảng).



5.2 Các yêu cầu bảo mật CSDL

❖ Bảo mật cơ sở dữ liệu (Database security) là một tập hợp các thủ tục, chuẩn, chính sách và công cụ được sử dụng để bảo vệ dữ liệu tránh bị:

- Trộm cắp,
- Lạm dụng
- Các hành động không mong muốn
- Đột nhập
- Tấn công.



5.2 Các yêu cầu bảo mật CSDL

❖ Một cách khác, mục đích của bảo mật cơ sở dữ liệu là đảm bảo 3 thuộc tính cơ bản của an toàn cơ sở dữ liệu:

- Bí mật (Confidentiality)
- Toàn vẹn (Integrity)
- Sẵn dùng (Availability)



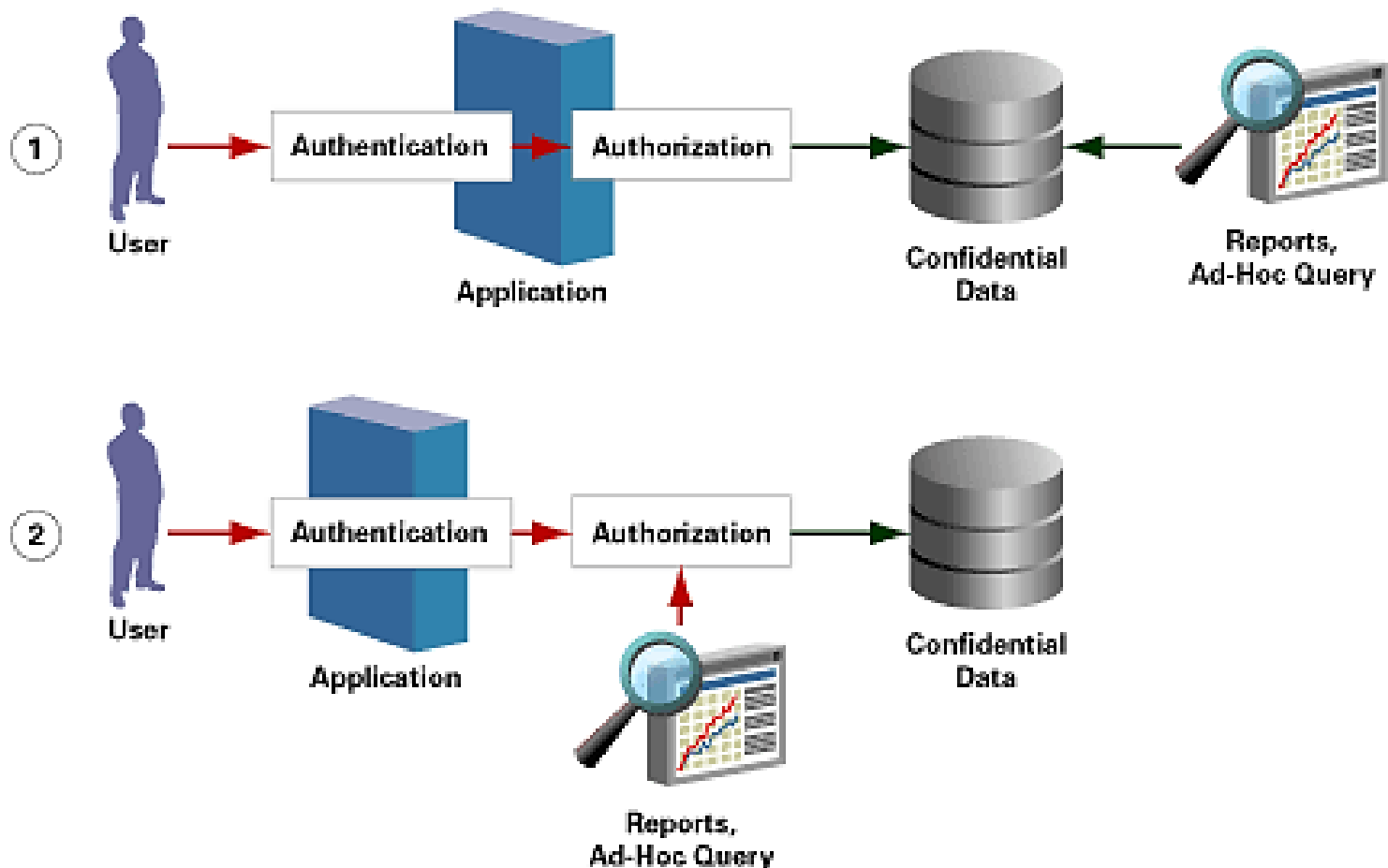
5.2 Các yêu cầu bảo mật CSDL

❖ Bí mật (Confidentiality):

- Chỉ người dùng có thẩm quyền (Authorised users) mới có thể truy nhập và thực hiện các thao tác trên CSDL;
- Tính bí mật có thể được đảm bảo thông qua kiểm soát truy nhập (ở mức hệ quản trị CSDL);
 - Xác thực (Authetication) và;
 - Trao quyền (Authorisation).
- Ngoài ra, tính bí mật có thể được đảm bảo bởi nhiều biện pháp bảo mật bổ sung:
 - Bảo vệ vật lý
 - Tường lửa
 - Mã hóa,...

5.2 Các yêu cầu bảo mật CSDL

❖ Bí mật (Confidentiality):

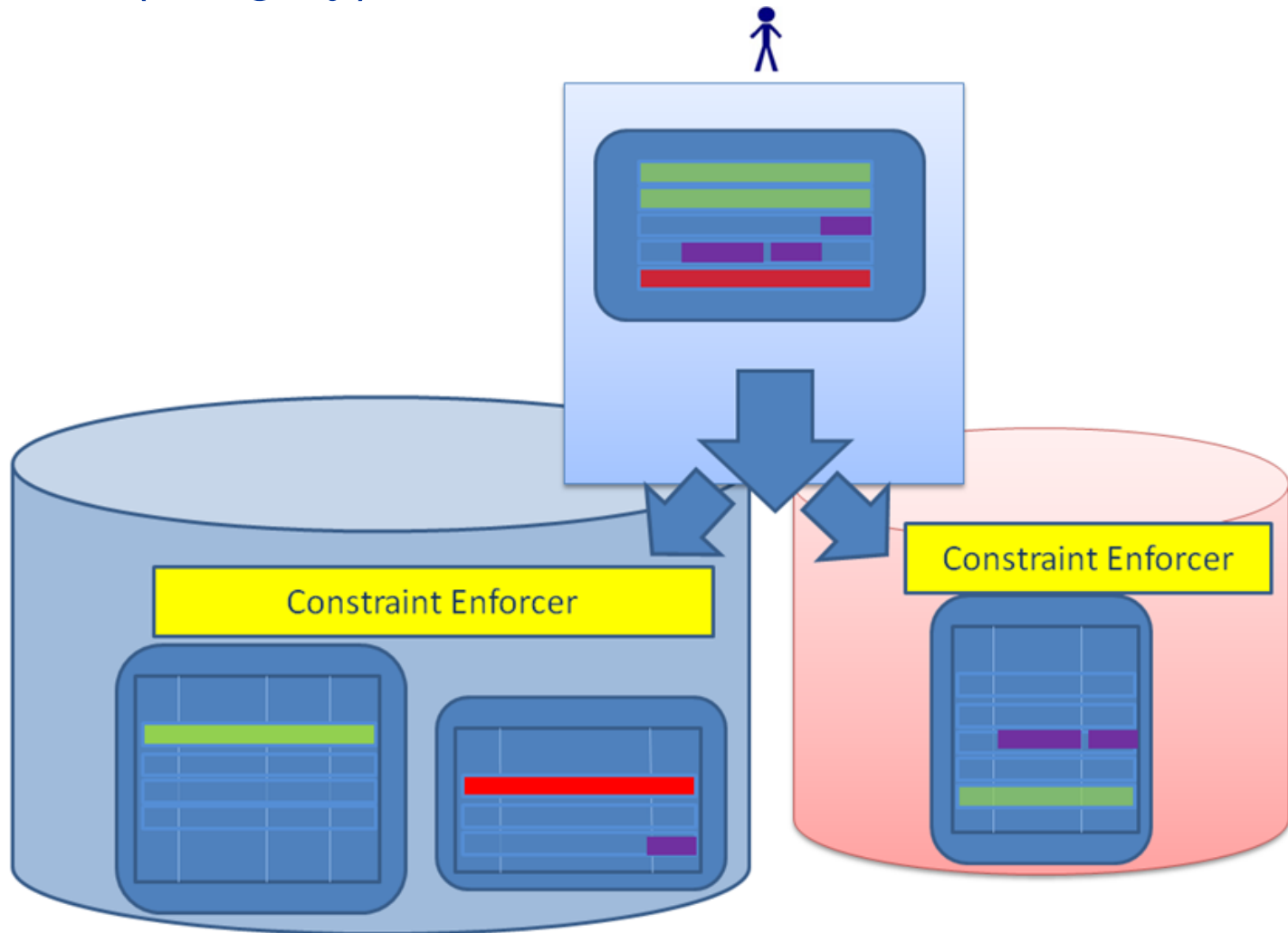


5.2 Các yêu cầu bảo mật CSDL

- ❖ Toàn vẹn (Integrity): dữ liệu chỉ có thể được sửa đổi bởi những người dùng có thẩm quyền.
 - Tính toàn vẹn liên quan đến tính hợp lệ (validity), tính nhất quán (Consistency) và chính xác (accuracy) của dữ liệu.
 - Dữ liệu là toàn vẹn nếu:
 - Dữ liệu không bị thay đổi;
 - Dữ liệu hợp lệ;
 - Dữ liệu chính xác.
 - Tính toàn vẹn có thể được đảm bảo bởi:
 - Các ràng buộc dữ liệu (Constraints)
 - Các phép kiểm tra;
 - Các cơ chế xử lý dữ liệu.

5.2 Các yêu cầu bảo mật CSDL

❖ Toàn vẹn (Integrity):



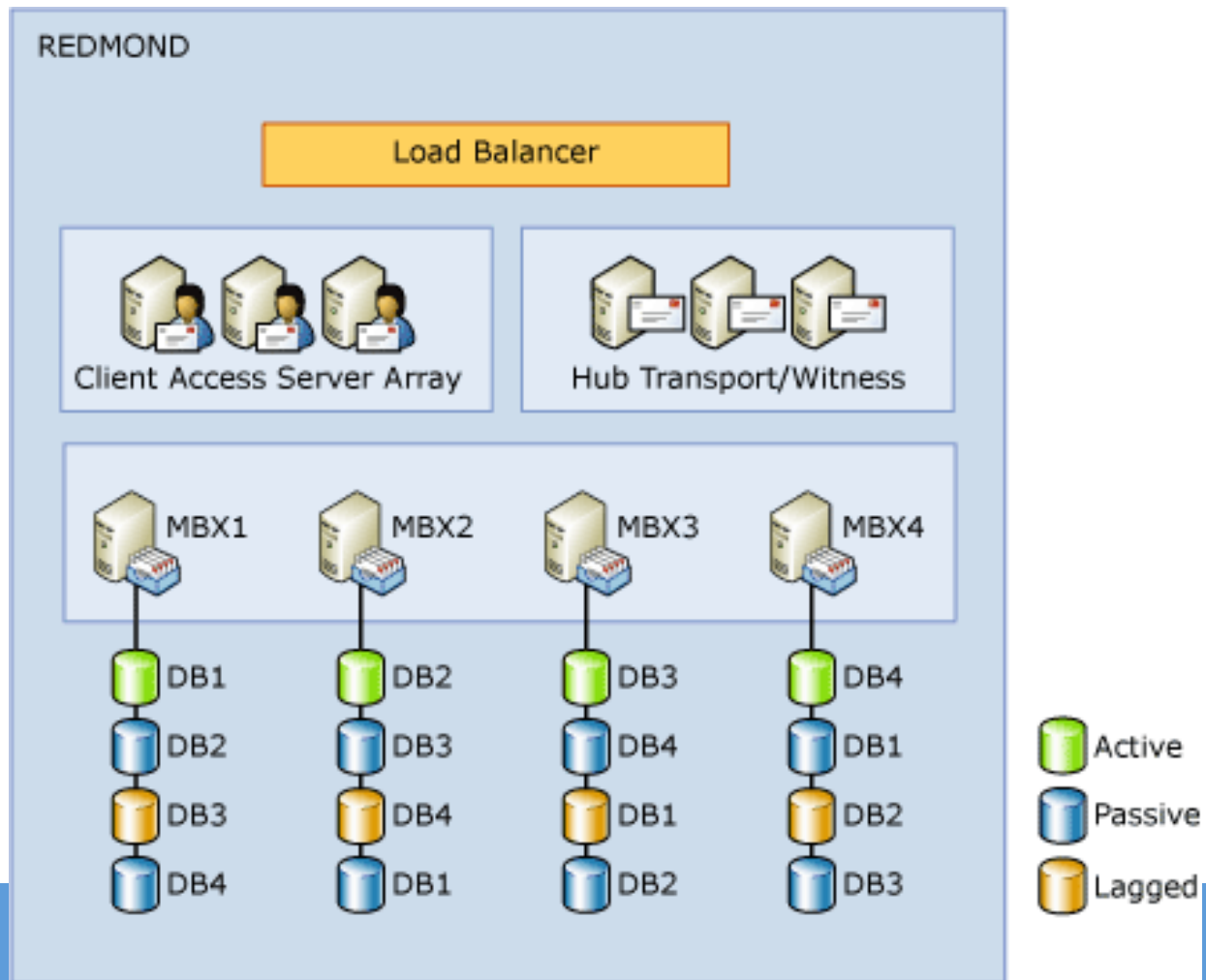
5.2 Các yêu cầu bảo mật CSDL

❖ Sẵn dùng/sẵn sàng (Availability):

- CSDL có thể truy nhập bởi người dùng hợp pháp bất cứ khi nào họ có yêu cầu.
- Tính sẵn dùng có thể được đo bằng các yếu tố:
 - Thời gian cung cấp dịch vụ (Uptime);
 - Thời gian ngừng cung cấp dịch vụ (Downtime);
 - Tỷ lệ phục vụ: $A = (\text{Uptime}) / (\text{Uptime} + \text{Downtime})$;
 - Thời gian trung bình giữa các sự cố;
 - Thời gian trung bình ngừng để sửa chữa;
 - Thời gian khôi phục sau sự cố.

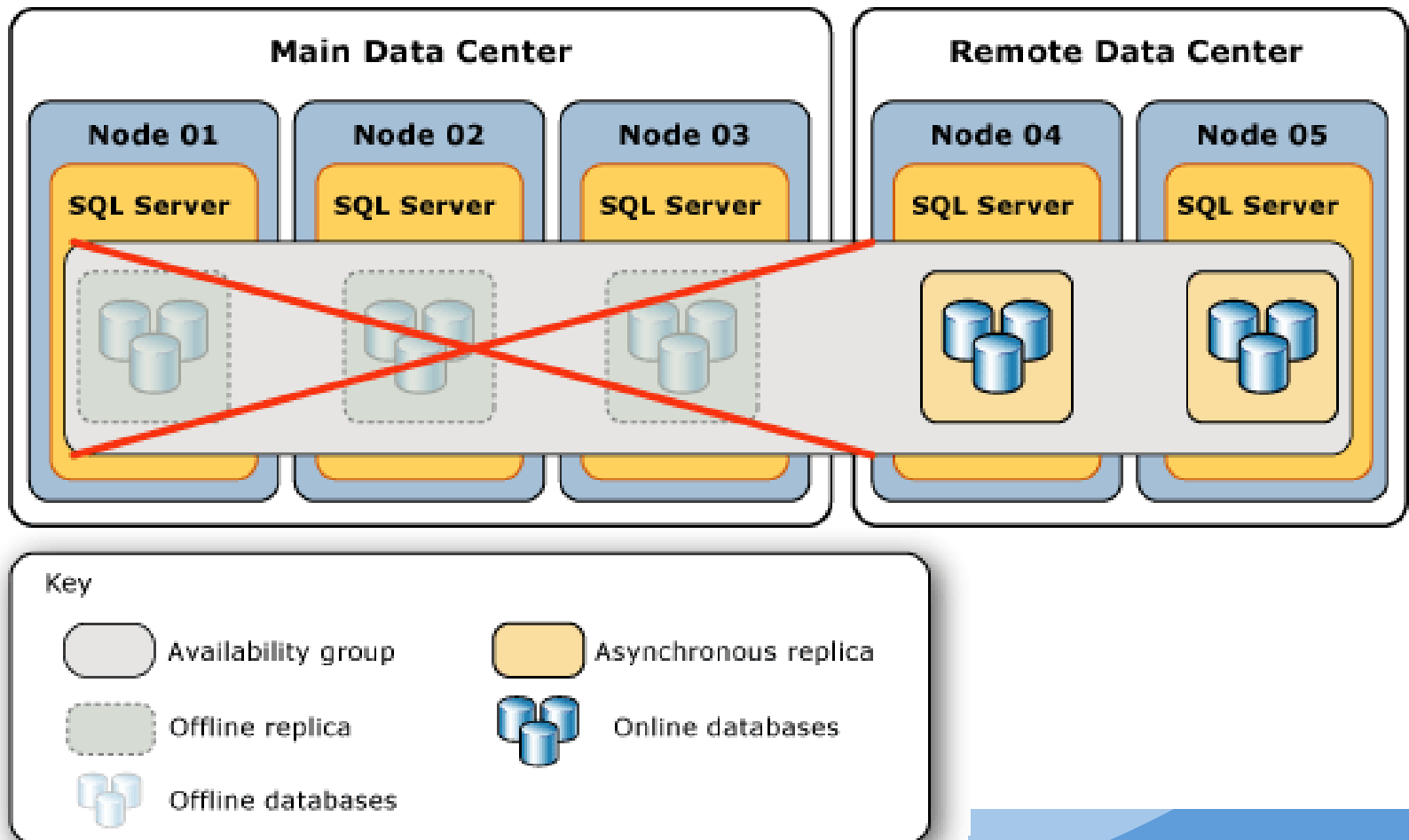
5.2 Các yêu cầu bảo mật CSDL

❖ Sẵn dùng/sẵn sàng (Availability):



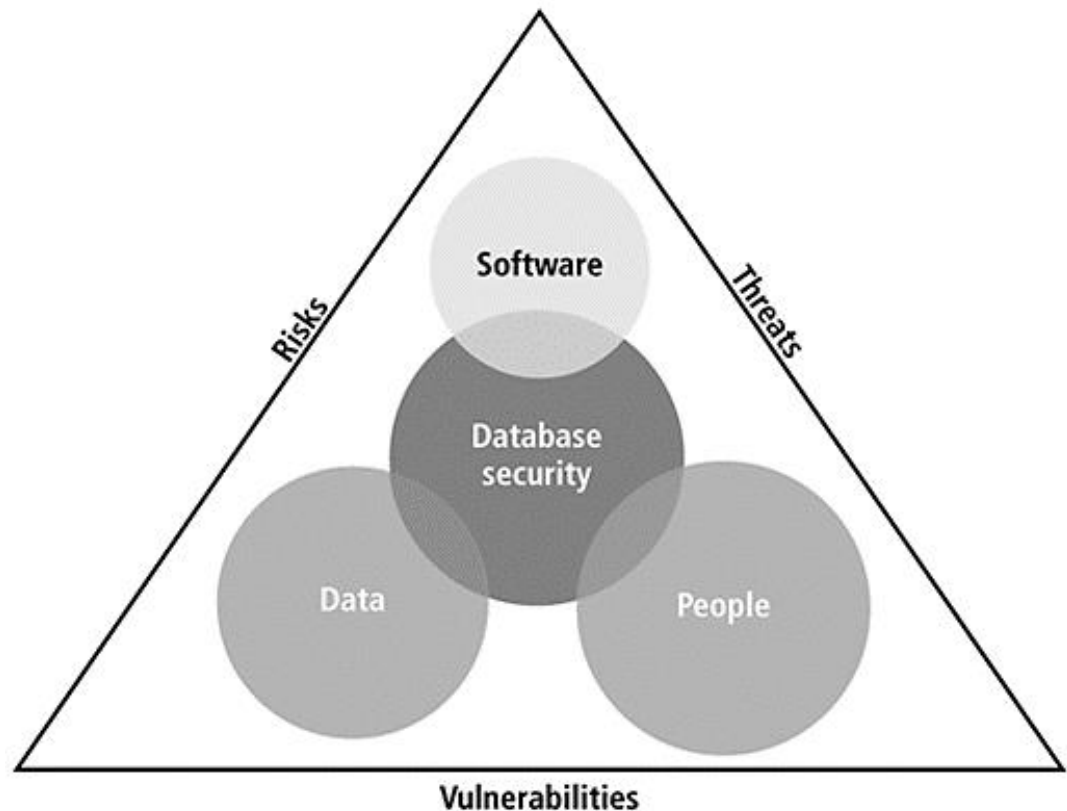
5.2 Các yêu cầu bảo mật CSDL

❖ Sẵn dùng/sẵn sàng (Availability):



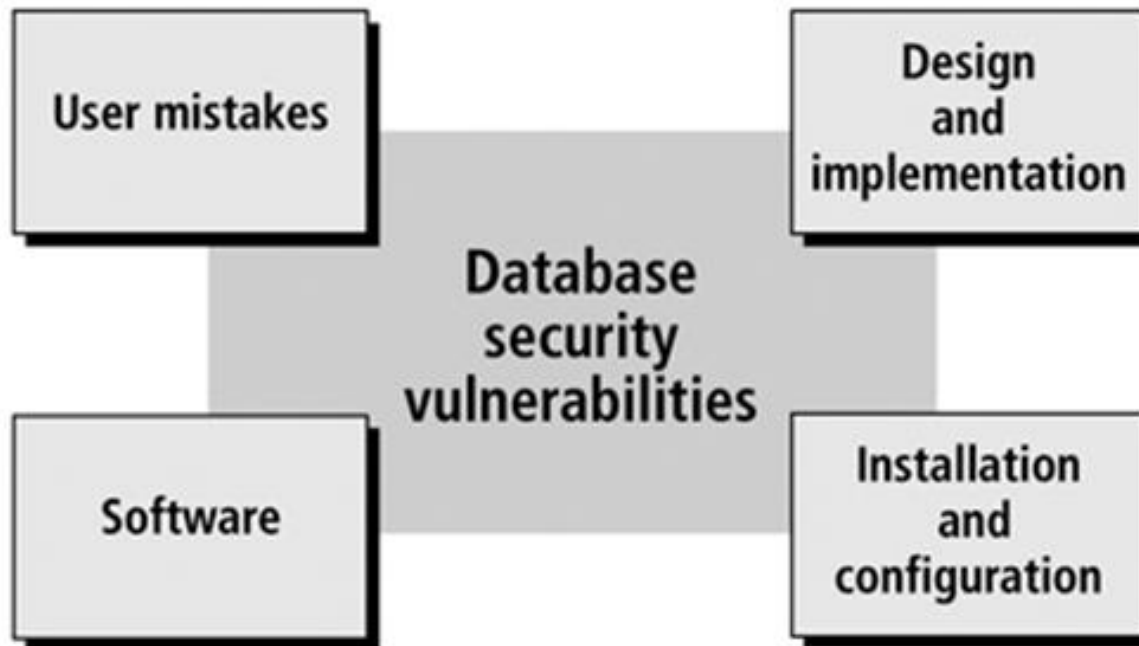
5.3 Mô hình tổng quát bảo mật CSDL

- ❖ Mô hình bảo mật CSDL tổng quát gồm 3 yếu tố:
 - Con người (people)
 - Phần mềm (Software)
 - Dữ liệu (Data).
- ❖ Các nhân tố liên quan đến bảo mật CSDL:
 - Các rủi ro (Risks)
 - Các đe dọa (Threats)
 - Các lỗ hổng (Vulnerabilities)



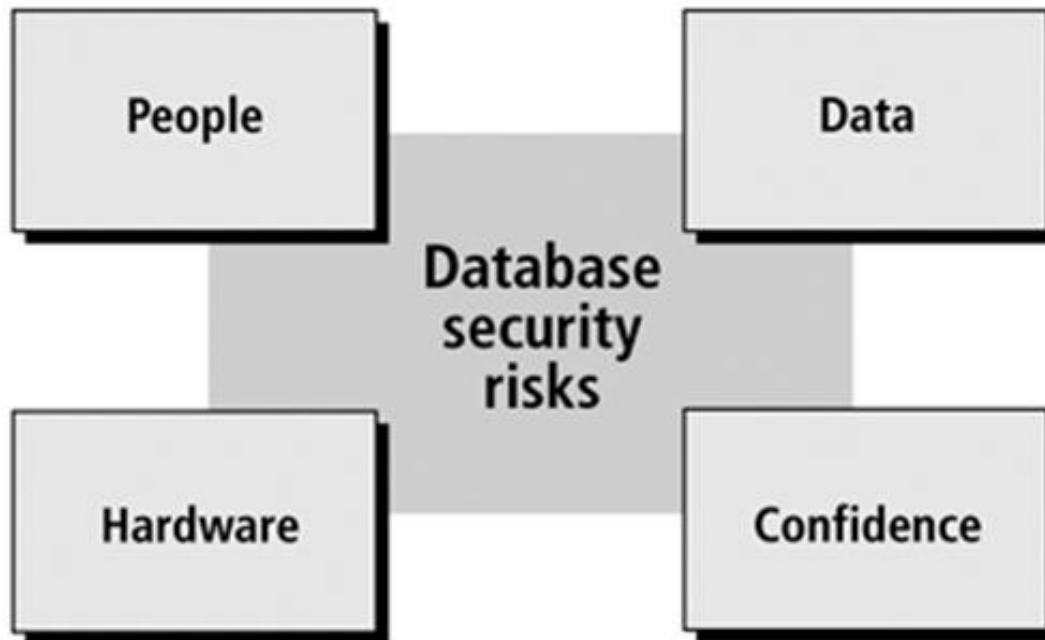
5.3 Mô hình tổng quát bảo mật CSDL

❖ Các lỗ hổng (Vulnerabilities)



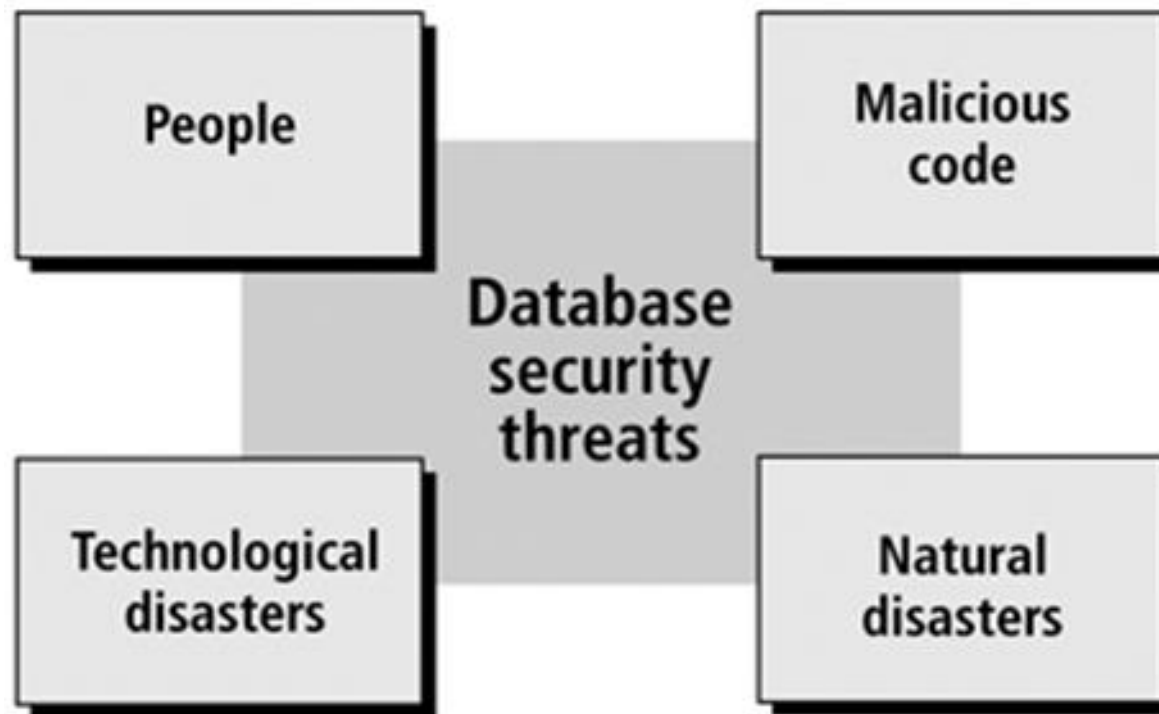
5.3 Mô hình tổng quát bảo mật CSDL

❖ Các rủi ro (Risks)



5.3 Mô hình tổng quát bảo mật CSDL

❖ Các đe dọa (Threats)



5.3 Mô hình tổng quát bảo mật CSDL

❖ Top 10 đe dọa đối với bảo mật CSDL (Theo Imperva 2015):

1. Excessive and Unused Privileges
2. Privilege Abuse
3. Input Injection
4. Malware
5. Weak Audit Trail
6. Storage Media Exposure
7. Exploitation of Vulnerabilities and Misconfigured Databases
8. Unmanaged Sensitive Data
9. Denial of Service
10. Limited Security Expertise and Education

Top 10 đe dọa đối với bảo mật CSDL (Theo Imperva 2015)

Threat		Excessive and Unused Privileges	Privilege Abuse	Input Injection	Malware	Weak Audit Trail	Storage Exposure	Vulnerability Exploitation	Unmanaged Sensitive Data	Denial of Service	Limited Security Knowledge
Solution											
Discovery and Assessment	Scan for Vulnerabilities			•	•					•	
	Calculate Risk Scores			•				•			
	Mitigate Vulnerabilities			•				•		•	
	Identify Compromised Endpoints				•			•			
	Analyze Risk and Prioritize Remediation Efforts							•			
	Discover Database Servers								•		
	Analyze Discovery Results								•		
	Identify and Classify Sensitive Data	•							•		
User Rights Management	Aggregate Access Rights	•	•								
	Enrich Access Rights Information	•	•								
	Identify and Remove Excessive Rights	•	•		•						
	Review and Approve/Reject Individual User Rights	•									
	Extract "Real" User Identity					•					

BÀI GIẢNG AN TOÀN UD WEB & CSDL

CHƯƠNG 5 – TỔNG QUAN VỀ BẢO MẬT CSDL

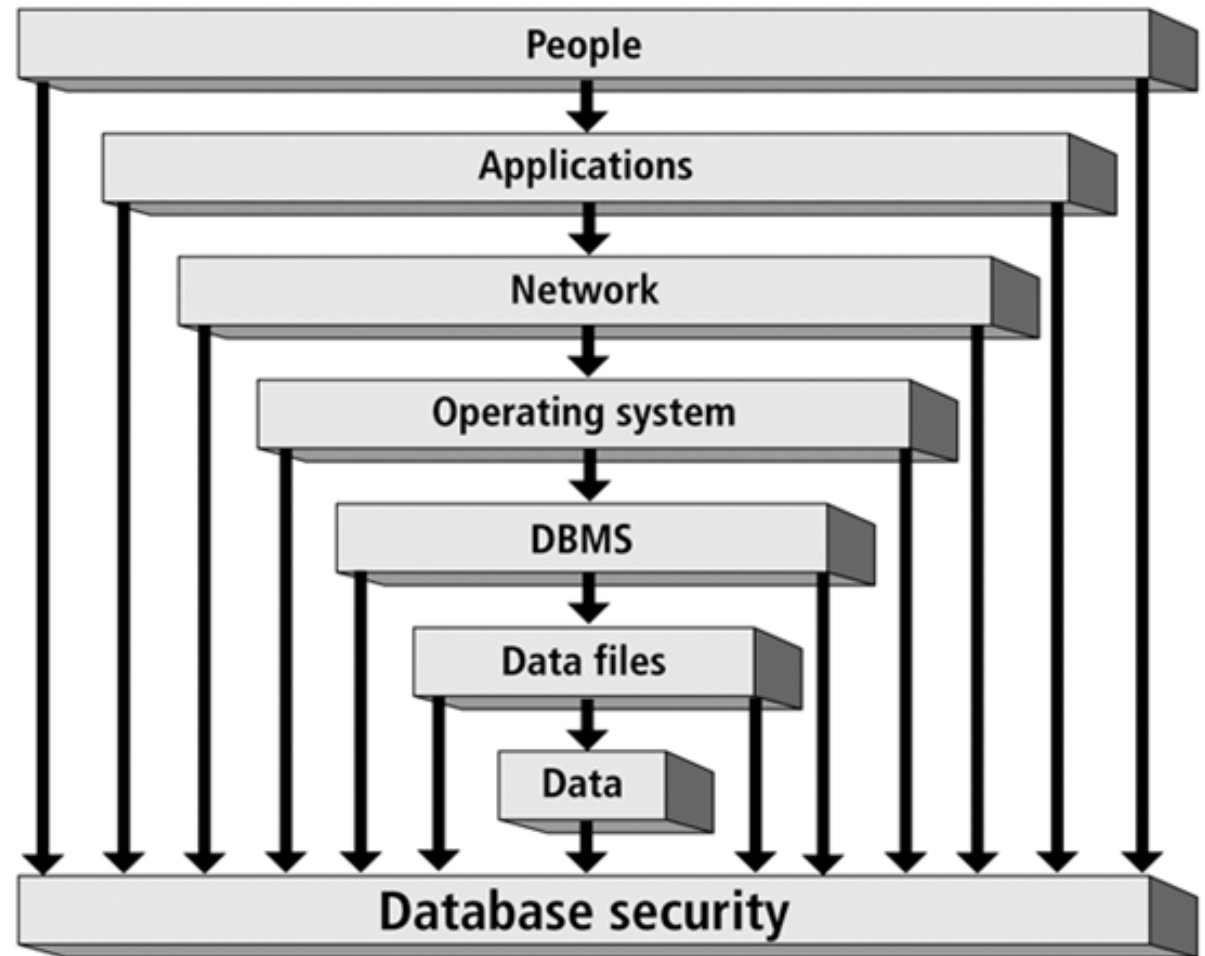
Top 10 đe dọa đối với bảo mật CSDL (Theo Imperva 2015)

[illegible]

5.3 Mô hình tổng quát bảo mật CSDL

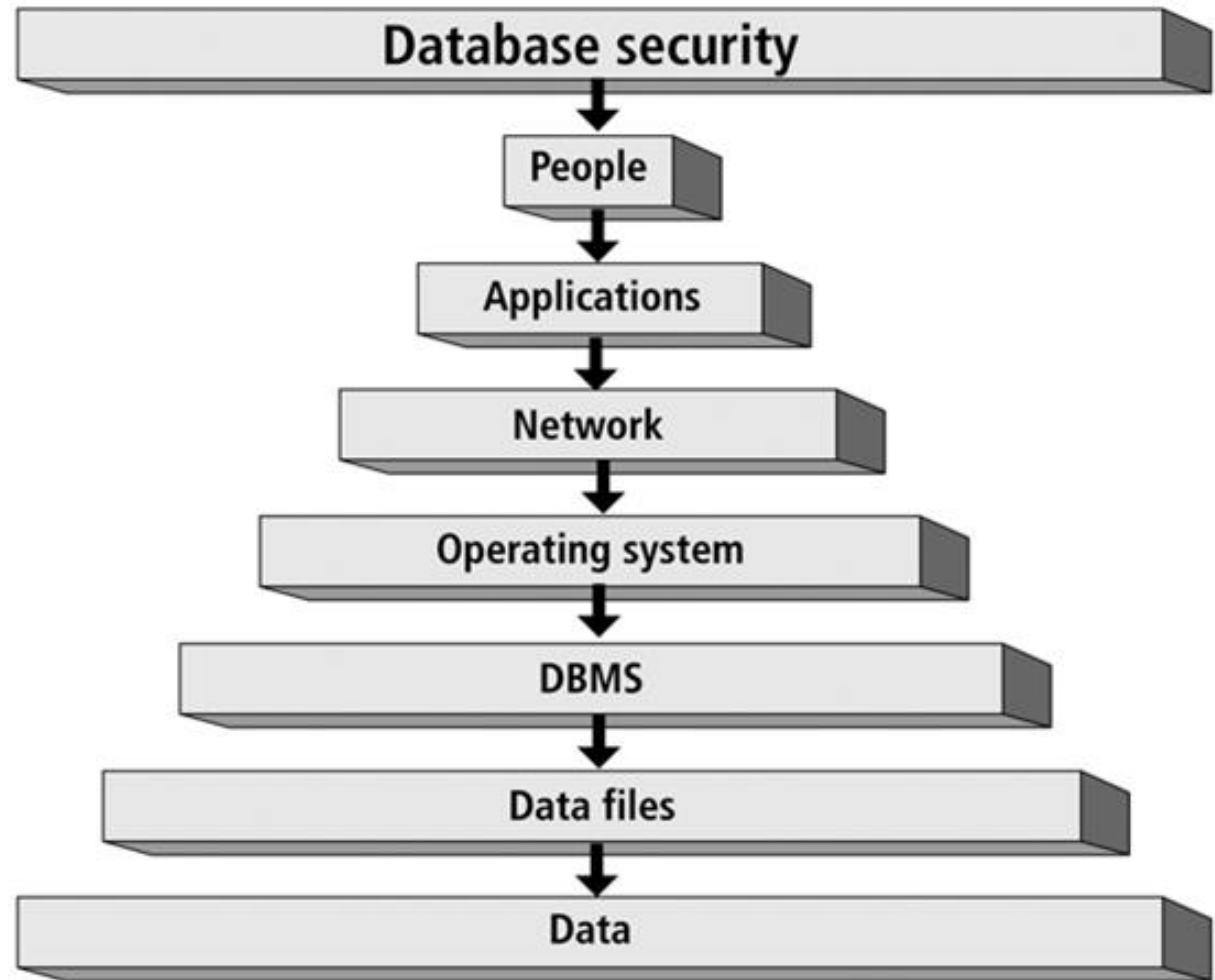
❖ Các điểm truy
nhập hệ thống
bảo mật
CSDL;

- Nhiều điểm
truy nhập →
Bảo mật phức
tạp, khó khăn.



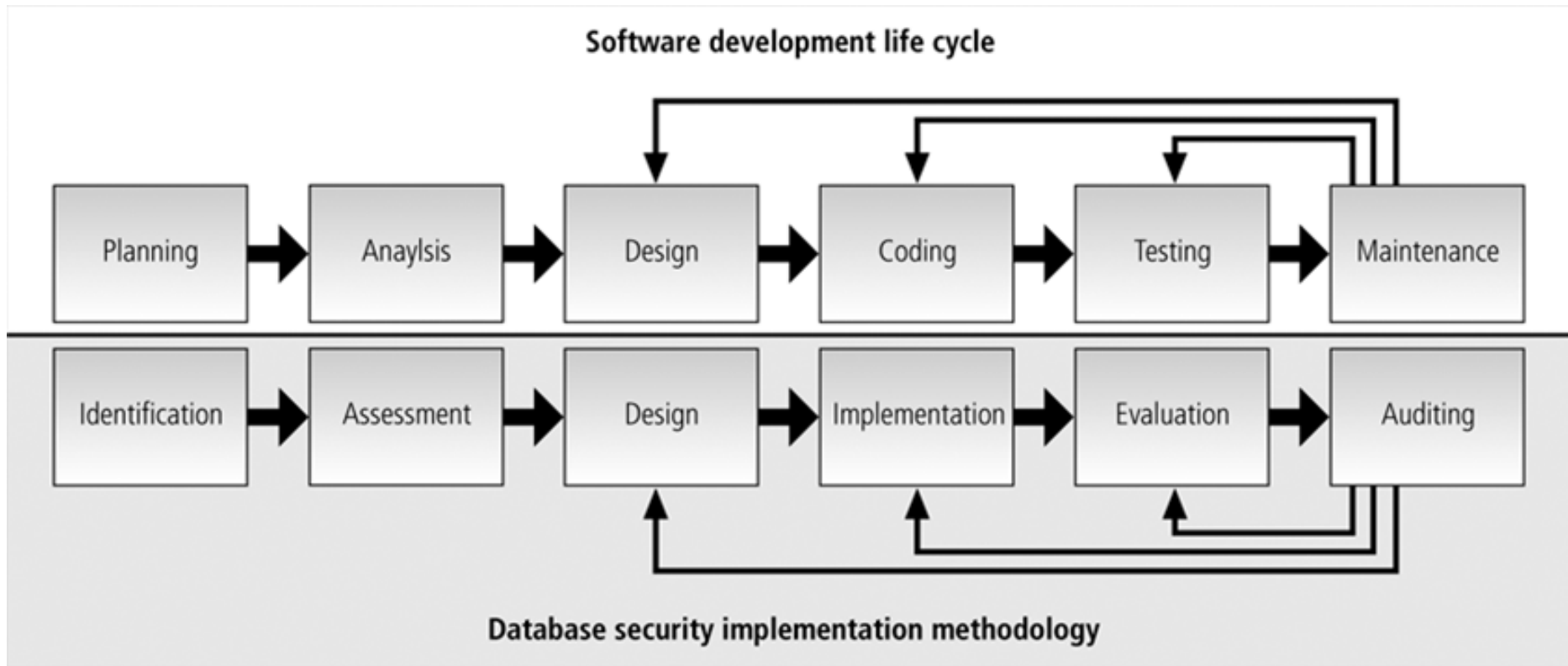
5.3 Mô hình tổng quát bảo mật CSDL

- ❖ Giới hạn, giảm thiểu các điểm truy nhập hệ thống bảo mật CSDL.



5.3 Mô hình tổng quát bảo mật CSDL

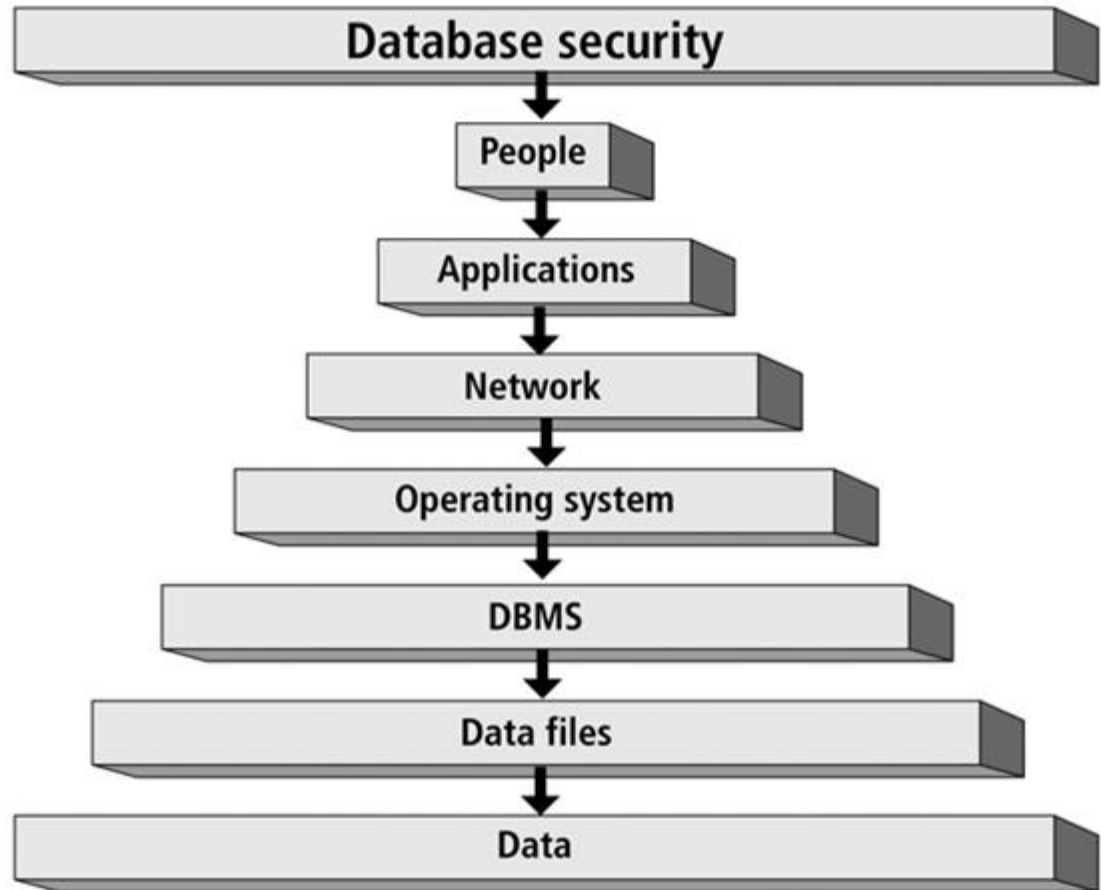
❖ Phương pháp thực hiện bảo mật CSDL



5.4 Các lớp bảo mật cơ sở dữ liệu

❖ Các lớp bảo mật cơ sở dữ liệu bao gồm:

- Con người
- Ứng dụng
- Mạng
- Hệ điều hành
- Hệ quản trị CSDL
- File dữ liệu
- Dữ liệu.



5.4 Các lớp bảo mật cơ sở dữ liệu

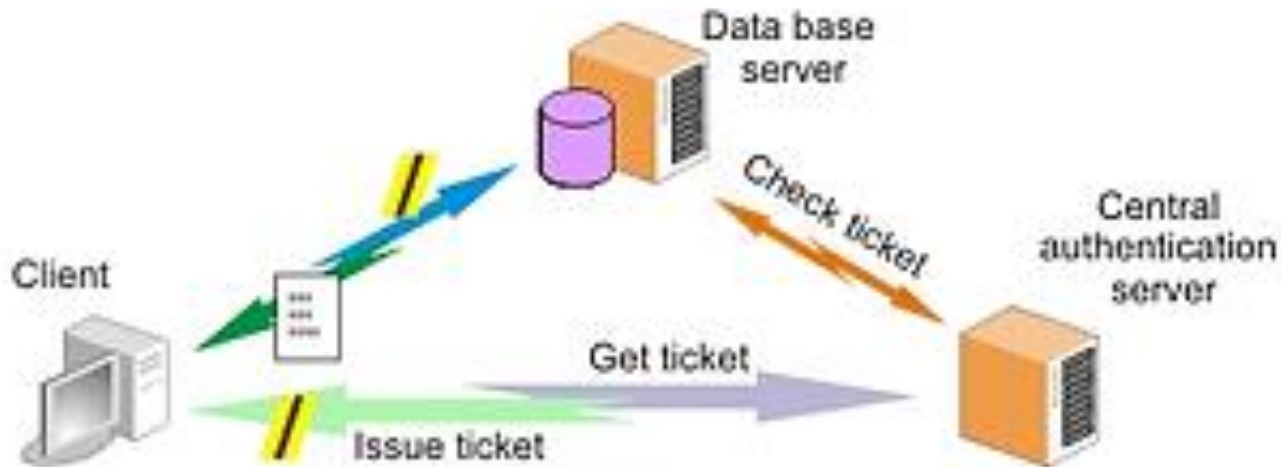
❖ Lớp bảo mật Con người

- Hạn chế truy nhập vật lý đến phần cứng hệ thống và các tài liệu;
- Sử dụng các biện pháp nhận dạng và xác thực thông tin nhận dạng của người dùng;
 - Dựa trên ID card;
 - PIN/mật khẩu.
 - Các đặc điểm sinh trắc học: vân tay, tròng mắt;
- Đào tạo người quản trị, người dùng về tầm quan trọng của bảo mật và các biện pháp bảo vệ tài sản;
- Thiết lập các chính sách và thủ tục kiểm soát an ninh.

5.4 Các lớp bảo mật cơ sở dữ liệu

❖ Lớp bảo mật Ứng dụng:

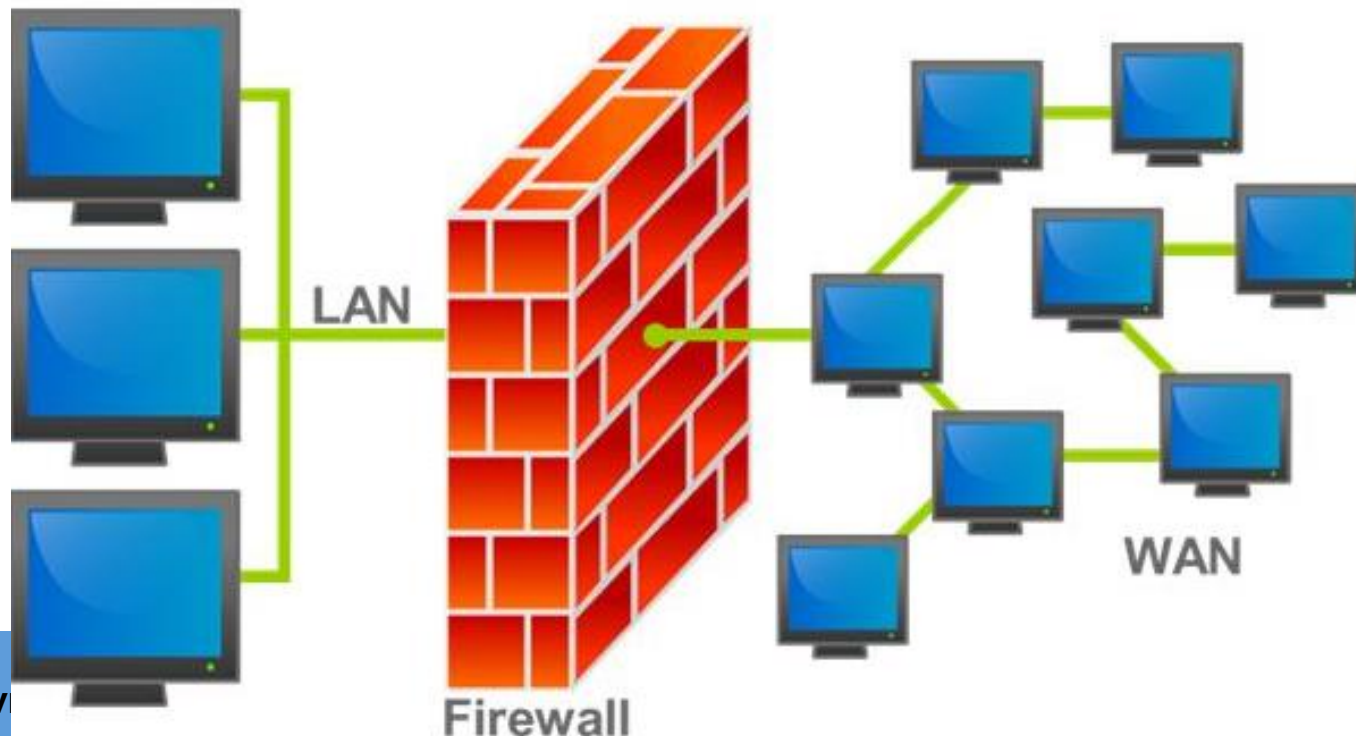
- Xác thực người dùng truy nhập ứng dụng;
- Áp dụng chính xác quy trình xử lý công việc;
- Sử dụng cơ chế đăng nhập một lần (Single Sing On) cho nhiều ứng dụng hoặc website có liên kết.



5.4 Các lớp bảo mật cơ sở dữ liệu

❖ Lớp bảo mật Mạng:

- Sử dụng tường lửa để ngăn chặn xâm nhập trái phép;
- Sử dụng VPN để bảo mật thông tin/dữ liệu trên đường truyền;
- Sử dụng xác thực.



5.4 Các lớp bảo mật cơ sở dữ liệu

❖ Lớp bảo mật Hệ điều hành:

- Xác thực người dùng;
- Phát hiện xâm nhập;
- Áp dụng chính sách quản lý mật khẩu chặt chẽ;
- Vấn đề tài khoản người dùng.



5.4 Các lớp bảo mật cơ sở dữ liệu

❖ Lớp bảo mật File dữ liệu:

- Quyền truy nhập file;
- Giám sát truy nhập file.



5.4 Các lớp bảo mật cơ sở dữ liệu

❖ Lớp bảo mật Dữ liệu:

- Kiểm tra dữ liệu;
- Các ràng buộc dữ liệu;
- Mã hóa dữ liệu.



5.5 Các dạng tấn công thường gặp lên CSDL

1. Tấn công chèn mã SQL (đã học)
2. Tấn công tràn bộ đệm (đã học)
3. Tấn công từ chối dịch vụ
4. Trojan trên cơ sở dữ liệu

5.5.3 Tấn công từ chối dịch vụ CSDL

- ❖ Tấn công từ chối dịch vụ CSDL không được biết đến nhiều như tấn công DoS/DDoS vào mạng và các dịch vụ mạng;
- ❖ Tin tặc thường lợi dụng hoặc khai thác các tính năng, lỗi hoặc lỗ hổng trong hệ thống CSDL làm tiêu tốn tài nguyên hoặc giảm hiệu năng CSDL.

5.5.3 Tấn công từ chối dịch vụ CSDL

- ❖ Tấn công từ chối dịch vụ CSDL gồm các dạng:
 - Lạm dụng các tính năng của CSDL
 - Sử dụng các câu truy vấn phức tạp
 - Khai thác các lỗi hoặc khiếm khuyết
 - Tấn công thông qua lớp ứng dụng.

5.5.3 Tấn công từ chối dịch vụ CSDL

❖ Lạm dụng các tính năng của CSDL

- Tin tặc thường lợi dụng các tính năng của CSDL để tấn công DoS.
- Thường các tính năng này không an toàn với truy nhập từ bên ngoài.
- Ví dụ 1:
 - Nếu ta giới hạn số lần login sai với một người dùng, kẻ tấn công nếu biết tên người dùng sẽ thử login nhiều lần với mật khẩu sai. Kết quả là người dùng thực sự sẽ bị khóa tài khoản trong một khoảng thời gian.

5.5.3 Tấn công từ chối dịch vụ CSDL

❖ Lạm dụng các tính năng của CSDL

▪ Ví dụ 2:

- Nếu ta cài đặt CSDL cho phép tự tăng năng lực khi số yêu cầu truy vấn tăng, kẻ tấn công sẽ gửi đến rất nhiều yêu cầu giả mạo làm CSDL tăng sử dụng tài nguyên đến tối đa, có thể dẫn đến máy chủ sập đổ và ngừng hoạt động.
- Tin tặc có thể tạo các yêu cầu đặc biệt gây lỗi trong xử lý dữ liệu đầu vào, có thể làm máy chủ CSDL ngừng hoạt động.

5.5.3 Tấn công từ chối dịch vụ CSDL

❖ Sử dụng các câu truy vấn phức tạp:

- Tin tặc tạo các câu truy vấn phức tạp nhằm làm máy chủ CSDL sử dụng nhiều tài nguyên (bộ nhớ, CPU time, đĩa,...), làm giảm hiệu năng hoặc ngừng hoạt động máy chủ CSDL.
- Tạo câu truy vấn với các trường tính toán và view với số lượng nhiều trường và nhiều bản ghi, làm máy chủ CSDL tiêu thụ nhiều bộ nhớ.
- Sử dụng các câu truy vấn lồng nhau hoặc đệ quy.

5.5.3 Tấn công từ chối dịch vụ CSDL

❖ Sử dụng các câu truy vấn phức tạp:

- Sử dụng các phép toán có chi phí tính toán lớn như IN với danh sách so sánh rất dài.

select * from <table1> from where <column1> **IN** (select <column2> from table2....)

- Sử dụng phép JOIN để tạo các câu truy vấn cho kết quả rất lớn.

Select * from table1 a **inner join** table2 b on a.c1 = b.c2....

- Sử dụng hàm do người dùng định nghĩa: Tin tặc có thể tự viết các hàm để tấn công CSDL.

5.5.3 Tấn công từ chối dịch vụ CSDL

❖ Khai thác các lỗi và khiếm khuyết:

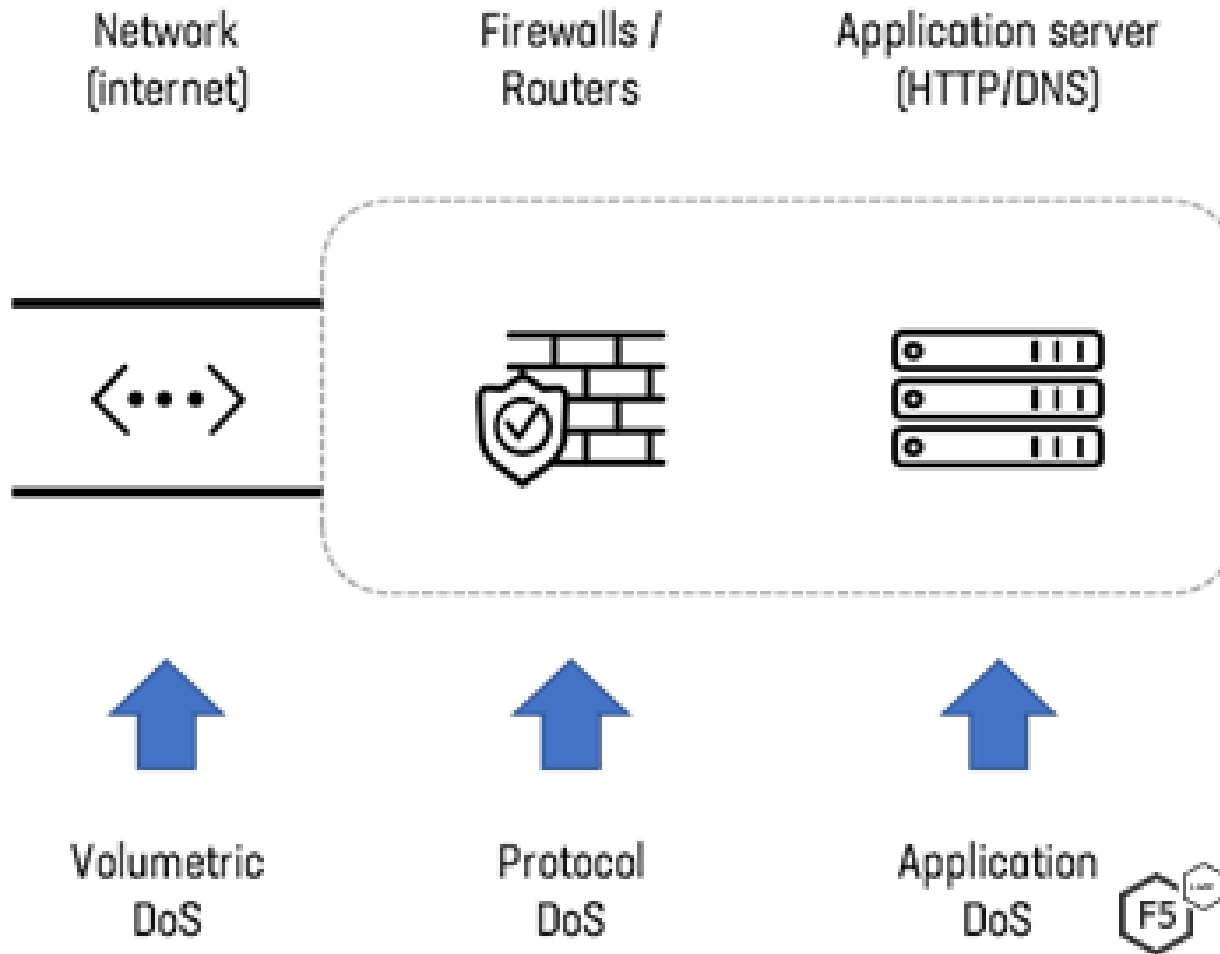
- Lỗi tràn bộ đệm
 - Sâu Slammer khai thác lỗi tràn bộ đệm tấn công MS-SQL 2000
- Lỗi chèn mã SQL
 - Lỗi chèn mã SQL có thể giúp tin tặc tấn công đánh cắp dữ liệu cũng như có thể phá hủy toàn bộ nội dung CSDL, gây gián đoạn hoạt động của hệ thống.
- Lỗi thiết lập quyền truy nhập
 - Lỗi thiết lập quyền truy nhập (quyền quản trị) và chèn mã có thể giúp tin tặc thực hiện các thao tác chiếm quyền điều khiển hệ thống.

5.5.3 Tấn công từ chối dịch vụ CSDL

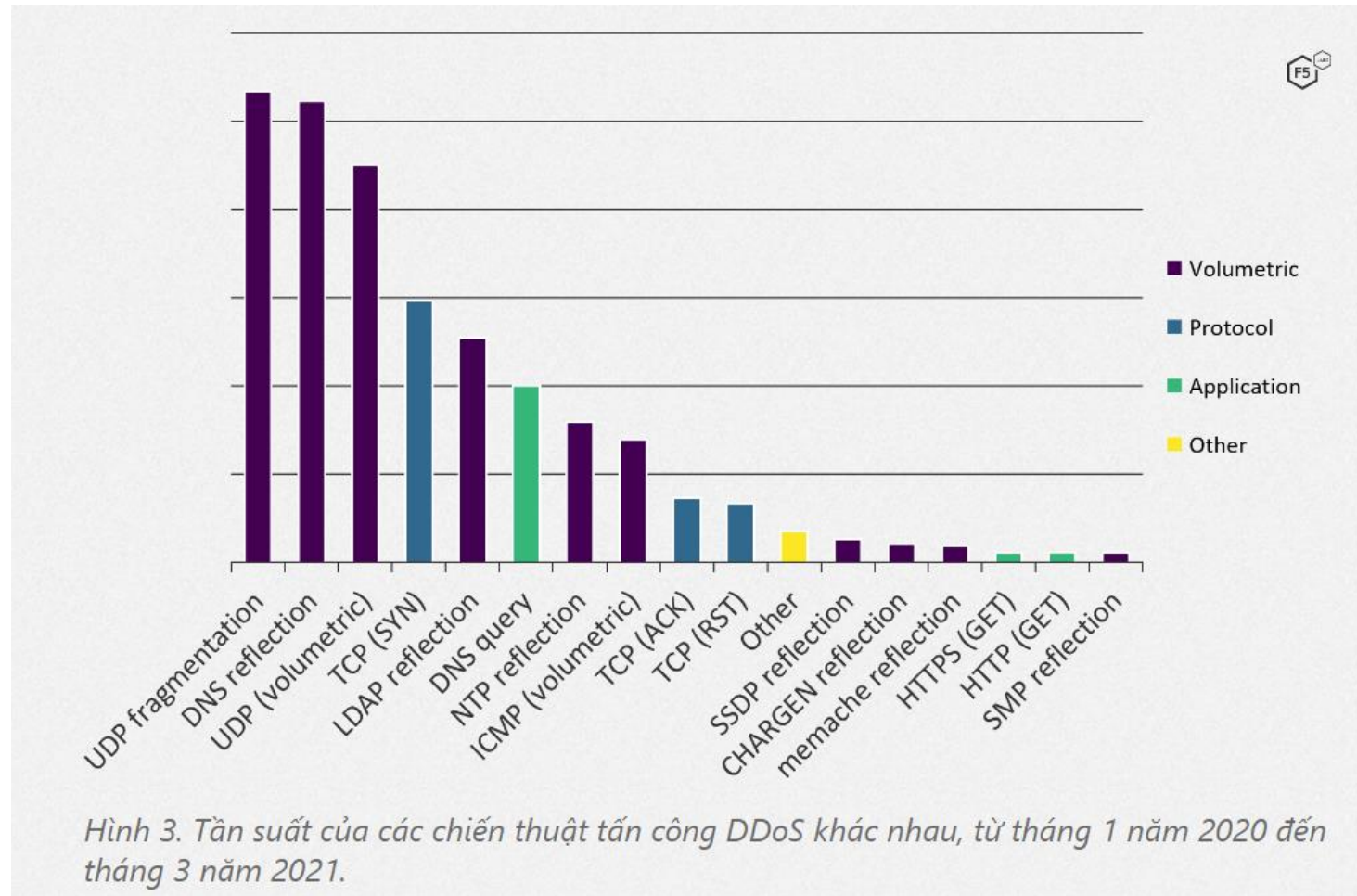
❖ Tấn công thông qua lớp ứng dụng

- Tin tặc có thể tấn công CSDL thông qua ứng dụng có kết nối và sử dụng CSDL.
- VD:
 - Tin tặc có thể thêm hàng ngàn sản phẩm vào 1 giỏ hàng trên một website bán hàng, sau đó liên tục thêm sản phẩm và xem lại toàn bộ giỏ hàng. Khi lượng sản phẩm đủ lớn có thể gây chậm hoặc đình trệ hoạt động của CSDL của website.
 - Tin tặc có thể sử dụng scripts để liên tục yêu cầu các trang phức tạp có mức truy vấn CSDL lớn gây quá tải cho máy chủ CSDL.

5.5.3 Tấn công từ chối dịch vụ CSDL



5.5.3 Tấn công từ chối dịch vụ CSDL



5.5.3 Tấn công từ chối dịch vụ CSDL – Phòng chống

- ❖ Cấu hình máy chủ và CSDL
- ❖ Đặt giới hạn sử dụng tài nguyên
- ❖ Cập nhật các bản vá
- ❖ Giám sát hoạt động của CSDL
- ❖ Tường lửa
 - Tường lửa cho ứng dụng web
 - Tường lửa cho CSDL

5.5.3 Tấn công từ chối dịch vụ CSDL – Phòng chống

❖ Cấu hình máy chủ và CSDL :

- Giảm thiểu các vị trí mà tin tặc có thể tấn công CSDL:
 - Xóa bỏ hoặc vô hiệu hóa các tài khoản, các tính năng và các dịch vụ không sử dụng;
- Hạn chế người dùng bên ngoài trực tiếp kết nối đến CSDL;
 - Sử dụng mô hình người dùng website/hệ thống truy nhập CSDL gián tiếp.
- Áp dụng chính sách quản lý người dùng, quản lý mật khẩu, phân quyền truy nhập chặt chẽ:
 - Mật khẩu phải đảm bảo an toàn và phải đổi mật khẩu định kỳ;
 - Quyền truy nhập được cấp cho các đối tượng phù hợp;
 - Hạn chế cho phép thực hiện các lệnh SQL trực tiếp trên các bảng;
 - Chỉ cấp quyền thực hiện các thủ tục.

5.5.3 Tấn công từ chối dịch vụ CSDL – Phòng chống

❖ Đặt giới hạn (threshold) sử dụng tài nguyên:

- Đặt giới hạn sử dụng tài nguyên cho mỗi người dùng, như số lượng câu truy vấn/phút, thời gian hết hạn (Timed-out) với câu truy vấn lớn, ngưỡng sử dụng bộ nhớ và CPU,...
- Giới hạn số người dùng CSDL có thể đăng nhập và truy vấn dữ liệu đồng thời.
- Giới hạn giúp giảm nguy cơ CSDL bị tấn công DoS.

5.5.3 Tấn công từ chối dịch vụ CSDL – Phòng chống

❖ Cập nhật các bản vá:

- Cần cập nhật thường xuyên các bản vá cho HĐH, các hệ quản trị CSDL và các ứng dụng để giảm thiểu các tấn công khai thác các lỗi, lỗ hổng đã biết.
 - Các lỗ hổng bảo mật đã biết không được khắc phục kịp thời có thể bị tin tặc khai thác.
- Trong điều kiện có thể, cần nâng cấp HĐH và hệ quản trị CSDL lên phiên bản mới, ổn định và an toàn hơn.

5.5.3 Tấn công từ chối dịch vụ CSDL – Phòng chống

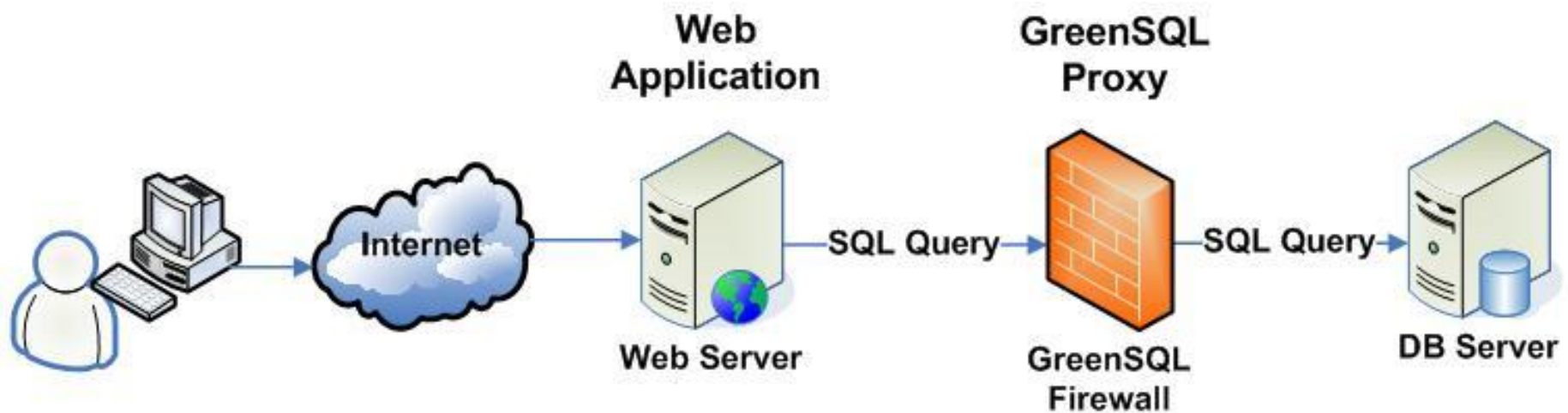
❖ Giám sát hoạt động của CSDL:

- Sử dụng hệ thống giám sát để phát hiện và cảnh báo về các hành vi bất thường, hoặc các truy vấn không hợp lệ.
- Các thông tin có thể giám sát:
 - Tần suất đăng nhập, kết nối đến CSDL
 - Việc truy nhập các đối tượng quan trọng
 - Mức sử dụng CPU, bộ nhớ, đĩa và tài nguyên mạng
 - Các yêu cầu không hợp lệ hoặc bị cấm.

5.5.3 Tấn công từ chối dịch vụ CSDL – Phòng chống

❖ Tường lửa/proxy cho CSDL:

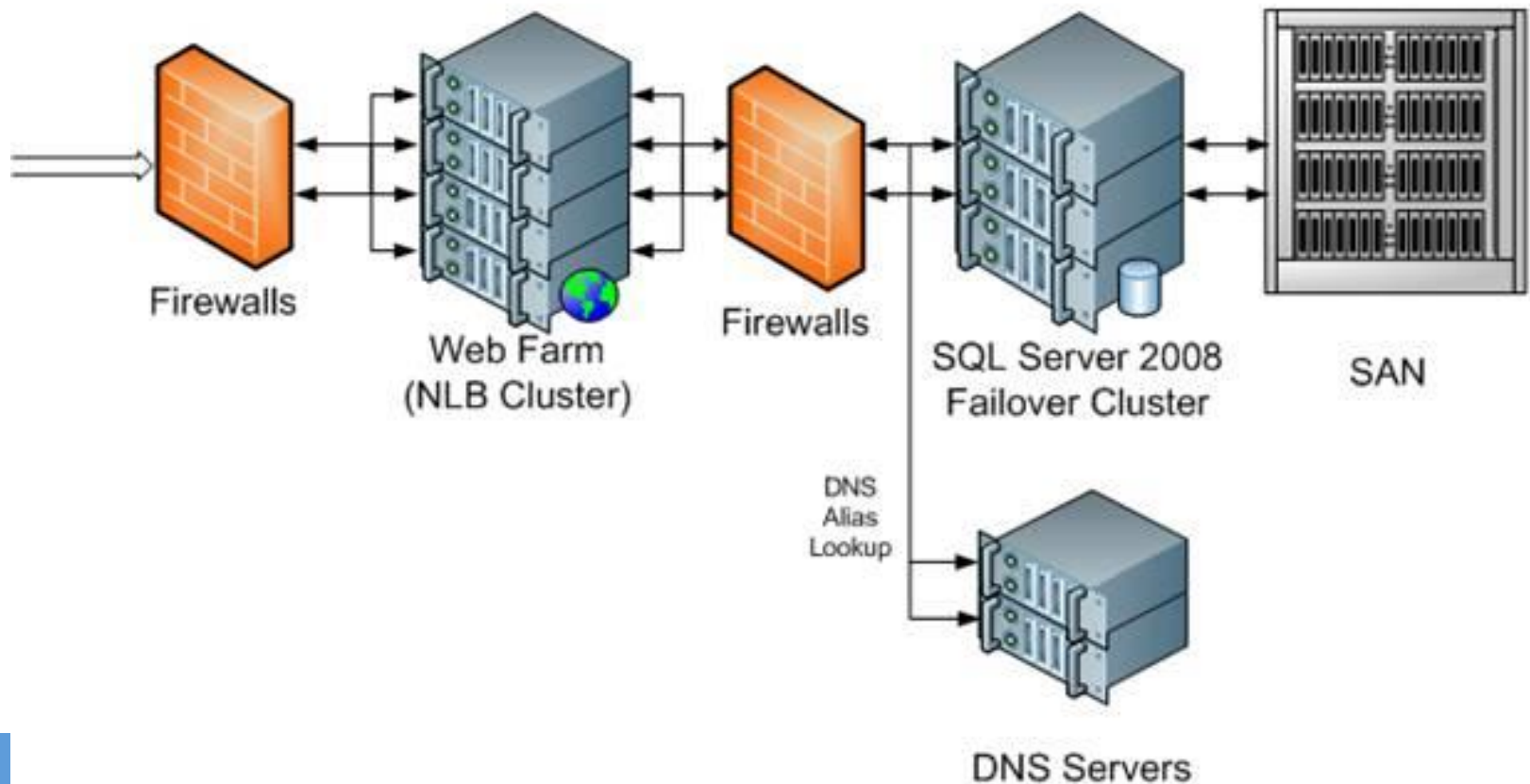
- Dùng để lọc và phát hiện các câu truy vấn độc hại.



5.5.3 Tấn công từ chối dịch vụ CSDL – Phòng chống

❖ Tường lửa cho ứng dụng web:

- Dùng để lọc các yêu cầu gửi đến máy chủ ứng dụng web.



5.5.4 Trojan trên cơ sở dữ liệu

- ❖ Trojan (hoặc Trojan horses) lấy tên theo tích "Con ngựa thành Tơ roa"



5.5.4 Trojan trên cơ sở dữ liệu

- ❖ Trojans là các phần mềm chứa mã độc, thường giả danh những chương trình có ích, nhằm lừa người dùng kích hoạt chúng.
- ❖ Trojans thường được sử dụng để thực thi gián tiếp các tác vụ, mà tác giả của chúng không thể thực hiện trực tiếp do không có quyền truy nhập.
- ❖ Trojans thường khai thác cơ chế điều khiển truy nhập tùy quyền (DAC) để thay đổi quyền truy nhập, cho phép tin tặc truy nhập các đối tượng mà chủ thể không hay biết.

5.5.4 Trojan trên cơ sở dữ liệu

- ❖ Các trojans CSDL thường là các đoạn mã độc SQL được nhúng vào các thủ tục CSDL, được chia thành 4 dạng:
 1. Một tấn công thực hiện cả việc chèn mã và gọi thực hiện Trojan;
 2. Một tấn công sử dụng một người dùng hoặc tiến trình thực hiện việc chèn mã Trojan và sau đó gọi thực hiện Trojan nhằm trích xuất thông tin hoặc thực hiện một hành động nào đó trong CSDL;

5.5.4 Trojan trên cơ sở dữ liệu

- ❖ Các trojans CSDL thường là các đoạn mã độc SQL được nhúng vào các thủ tục CSDL, được chia thành 4 dạng:
 3. Một tấn công thực hiện việc chèn mã Trojan và sau đó sử dụng một người dùng hoặc một tiến trình khác gọi thực hiện Trojan;
 4. Một tấn công sử dụng một người dùng hoặc tiến trình này thực hiện việc chèn mã Trojan và sau đó sử dụng một người dùng hoặc một tiến trình khác gọi thực hiện Trojan.

5.5.4 Trojan trên cơ sở dữ liệu

❖ Ví dụ 1:

- Tin tặc sử dụng 1 người dùng hoặc 1 tiến trình nào đó để chèn mã SQL Trojan vào thủ tục:
 - Một lập trình viên ít kinh nghiệm lấy 1 đoạn mã thủ tục trên mạng hoặc từ các nguồn không rõ ràng đưa vào CSDL mà không hiểu rõ đoạn mã đó thực hiện những công việc gì;
 - Khi thủ tục được gọi, trojan được kích hoạt.

5.5.4 Trojan trên cơ sở dữ liệu

❖ Ví dụ 2:

- Trojan được gọi thực hiện sử dụng 1 người dùng hoặc 1 tiến trình nào đó:
 - Một thủ tục CSDL được đặt chạy định kỳ vào cuối tháng để tính lương cho tất cả nhân viên trong công ty;
 - Tin tặc nắm được điều này có thể tìm cách chèn mã trojan vào thủ tục này và nó sẽ được kích hoạt khi thủ tục được chạy.

5.5.4 Trojan trên cơ sở dữ liệu – Phòng chống

❖ Kiểm soát việc tạo và sửa các thủ tục CSDL:

- Hạn chế quyền truy nhập của user thao tác dữ liệu:
 - Không cho phép tạo và sửa các thủ tục/hàm CSDL trong môi trường máy chủ sản xuất (production server) sử dụng người dùng thao tác dữ liệu;
 - Các thủ tục cần được tạo, sửa và test kỹ trong môi trường máy chủ phát triển (development server) và triển khai trên chủ sản xuất sử dụng người dùng quản trị.
- Không sử dụng code SQL từ các nguồn không rõ ràng;
 - Đặc biệt code SQL từ mạng Internet mà không được kiểm tra kỹ.
- Ghi logs và lưu phiên bản của mã nguồn các thủ tục và hàm.

5.5.4 Trojan trên cơ sở dữ liệu – Phòng chống

❖ Giám sát việc thực hiện các thủ tục:

- Cần ghi logs và giám sát chặt chẽ việc thực hiện các thủ tục quan trọng, có độ phức tạp cao, các thủ tục được chạy định kỳ hoặc được kích hoạt bởi trigger;
- Cấm hoặc hạn chế quyền thực hiện các thủ tục mở rộng hoặc thủ tục hệ thống – là những thủ tục chứa những đoạn mã có thể can thiệp vào CSDL, máy chủ CSDL và hệ điều hành.

5.6 Top 10 lỗ hổng CSDL trên thực tế

1. Default and Weak Passwords
2. SQL Injection in the DBMS
3. Excessive User & Group Privileges
4. Unnecessary Enabled DBMS Features
5. Broken Configuration Management
6. Buffer Overflows
7. Privilege Escalation
8. Denial of Service (DoS)
9. Unpatched Database
10. Unencrypted Data

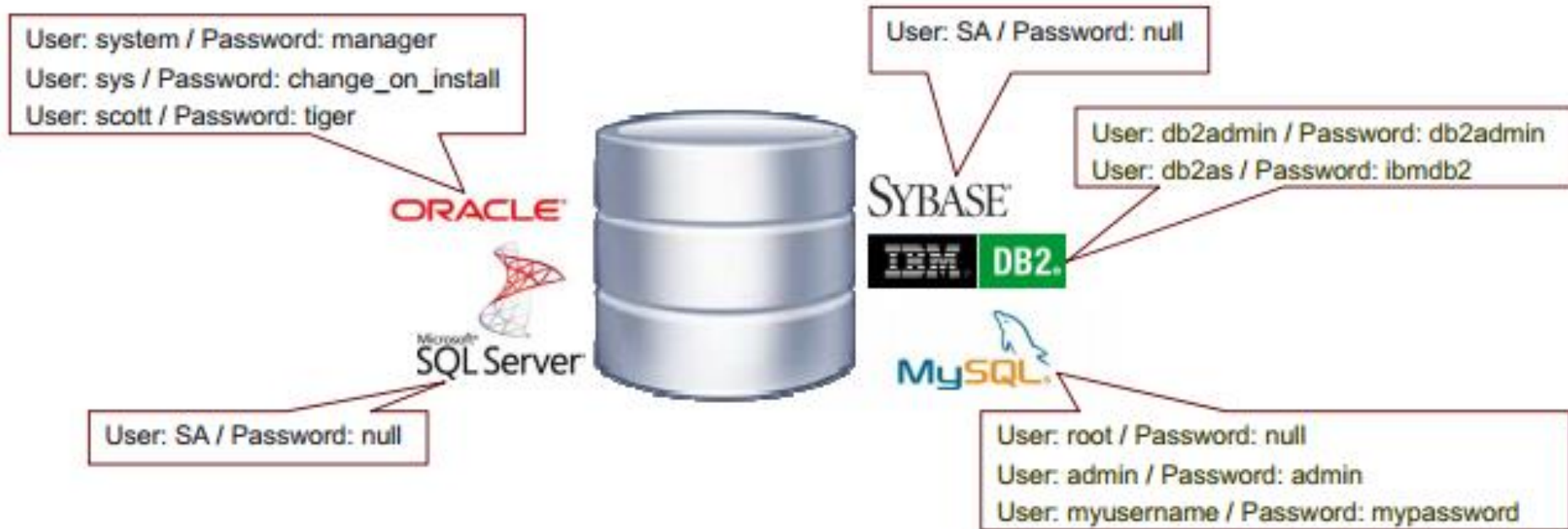
5.6 Top 10 lỗ hổng CSDL trên thực tế (tiếp)

1. Default and Weak Passwords (Sử dụng mật khẩu ngầm định và mật khẩu yếu)

- Nhiều DBMS (hệ quản trị CSDL) sử dụng tài khoản quản trị với mật khẩu ngầm định đơn giản hoặc rỗng;
 - MS SQL Server (2000 trở về trước): user – sa, password: rỗng
 - MySQL: user – root, password: rỗng
- Trong quá trình cài đặt, nhiều tài khoản sử dụng mật khẩu giống tên truy nhập hoặc rất dễ đoán.
 - user – root, password: root
 - user – admin, password: admin

5.6 Top 10 lỗ hổng CSDL trên thực tế (tiếp)

❖ Một số ví dụ về các tài khoản ngầm định:



5.6 Top 10 lỗi hồng CSDL trên thực tế (tiếp)

2. SQL Injection in the DBMS (Lỗi chèn mã SQL) có thể giúp tin tặc thực hiện:
- Vượt qua xác thực người dùng
 - Sửa đổi, xóa dữ liệu
 - Đánh cắp dữ liệu
 - Chiếm quyền điều khiển hệ thống.

5.6 Top 10 lỗi hồng CSDL trên thực tế (tiếp)

3. Excessive User & Group Privileges (Cấp quyền truy nhập cho người dùng/nhóm người dùng cao quá mức cần thiết)
 - Nhiều người dùng/nhóm người dùng được cấp quyền truy nhập cao quá mức cần thiết để thực hiện công việc được giao → dẫn tới lạm dụng quyền, hoặc tin tặc khai thác;
 - Thực tế: Người dùng CSDL chỉ để truy nhập dữ liệu nhưng lại được cấp quyền quản trị, hoặc là chủ sở hữu CSDL.

5.6 Top 10 lỗ hổng CSDL trên thực tế (tiếp)

- ❖ Excessive User & Group Privileges: Tấn công khai thác lỗi DBMS JVM EXP PERMS trên Oracle 11g R1: Ban đầu Public (không có tài khoản) không có quyền truy nhập.

The image shows a terminal window with a black background and red text. The title is "Exploiting Excessive Privileges" in large red font, followed by "Oracle 11g PUBLIC Privileges on SYS.DBMS_JVM_EXP_PERMS" in smaller red font. The terminal prompt is "SQL>". To the right of the terminal, there are two white boxes with red borders and red arrows pointing to the terminal. The top box contains the text "No users have 'ALL FILES' - full OS access". The bottom box contains the text "Attempt to execute OS command fails".

Exploiting Excessive Privileges
Oracle 11g PUBLIC Privileges on SYS.DBMS_JVM_EXP_PERMS

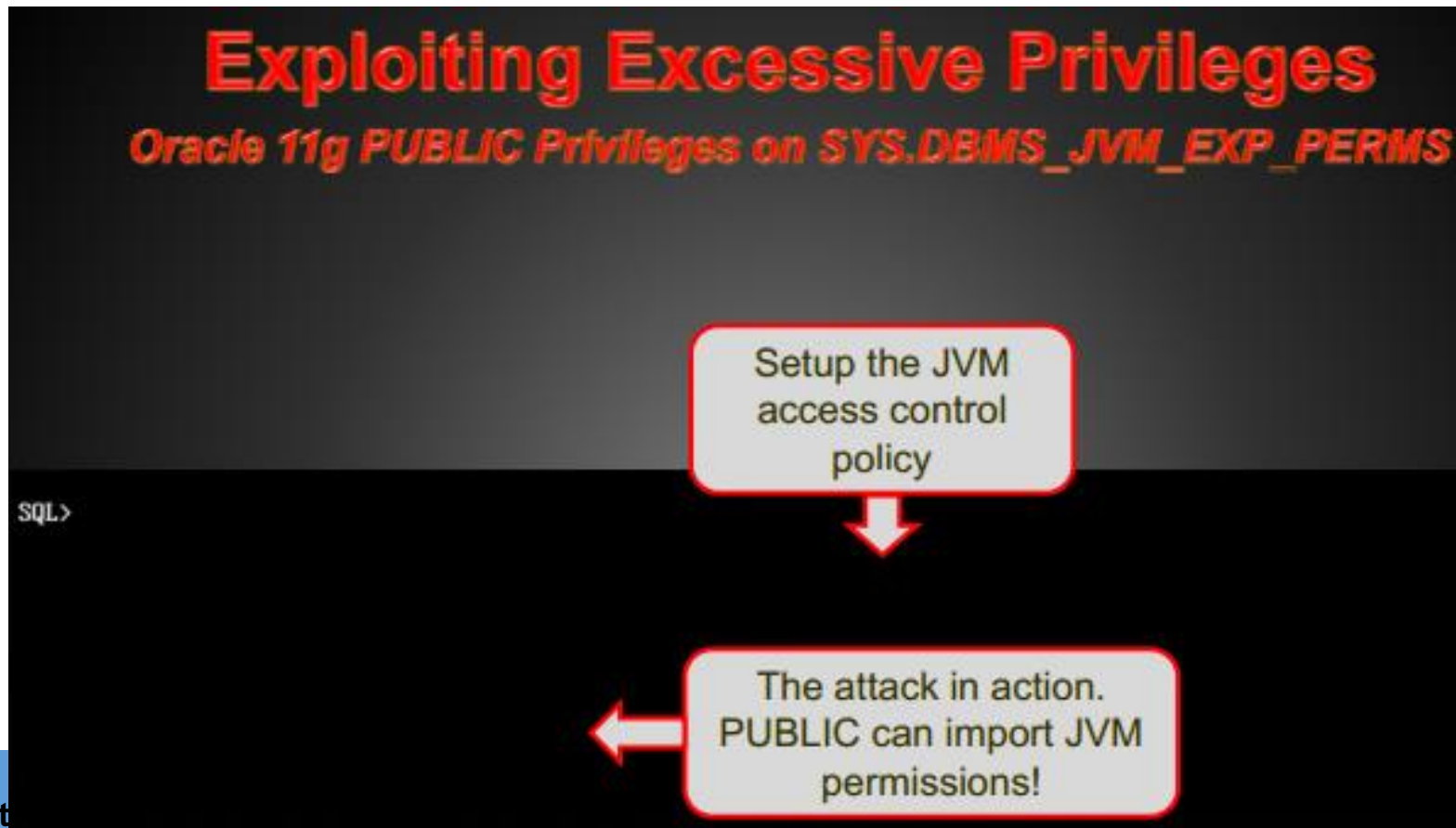
SQL>

No users have 'ALL FILES' - full OS access

Attempt to execute OS command fails

5.6 Top 10 lỗ hổng CSDL trên thực tế (tiếp)

- ❖ Excessive User & Group Privileges: Tấn công khai thác lỗi DBMS JVM EXP PERMS trên Oracle 11g R1: Thiết lập chính sách điều khiển truy nhập cho JVM.



5.6 Top 10 lỗ hổng CSDL trên thực tế (tiếp)

- ❖ Excessive User & Group Privileges: Tấn công khai thác lỗi DBMS JVM EXP PERMS trên Oracle 11g R1: Sau khi thay đổi chính sách điều khiển truy nhập, Public có toàn quyền truy nhập vào hệ điều hành.



5.6 Top 10 lỗ hổng CSDL trên thực tế (tiếp)

- ❖ Excessive User & Group Privileges: Tấn công khai thác lỗi DBMS JVM EXP PERMS trên Oracle 11g R1: dễ dàng tìm được mã khai thác trên Google.

About 586 results (0.11 seconds)

[Advanced search](#)

Everything

Images

Videos

News

Shopping

Geo

Char

Show

Oracle 11g 0day exploit published Alexander Kornbrust Oracle Feb 4, 2010 ... According to Repscan this new 11.2.0.1 is no longer vulnerable against the DBMS_JVM_EXP_PERMS exploit and this is correct ... [blog.red-database-security.com/.../oracle-11g-0day-exploit-published/](#) - Cached - Similar

Securing Java In Oracle Introduction The DBMS_JVM_EXP_PERMS File Format: PDF(Adobe Acrobat) - Quick View Feb 26, 2010 ... lowest CREATE SESSION privilege to DBA via the ... [http://www.oracle.com/technet/magazine/201002/SecuringJavaInOracle.html](#)

Oracle 11g 0day exploit published

I just read on Sumit Siddarth's (Sid) [blog](#) that the video recording from David Uchfield's 0th presentation is [online](#).

... to escape Java privileges using UTLR_JVM_EXP_PERMS.

```

POL DBMS_JVM_EXP_PERMS.TEMP_JAVA_POLICY;
CURSOR C1 IS SELECT 'GRANT',USER(), 'SYS','java.io.FilePermission','<<ALL
FILES>>','execute','ENABLED' from dual;
BEGIN
OPEN C1;
FETCH C1 BULK COLLECT INTO POL;
CLOSE C1;
DBMS_JVM_EXP_PERMS.IMPORT_JVM_PERMS(POL);
END;

```

... it is possible to run OS commands using a simple ...

```

runJava('oracle/aurora/utl/Wrapper.c()|windows()system32
s()|&C1st()from dual)

```

... you should)

... dbms_java from PUBLIC)

... create or replace dbms_java_test from PUBLIC)

... create or replace dbms_java_test from PUBLIC)

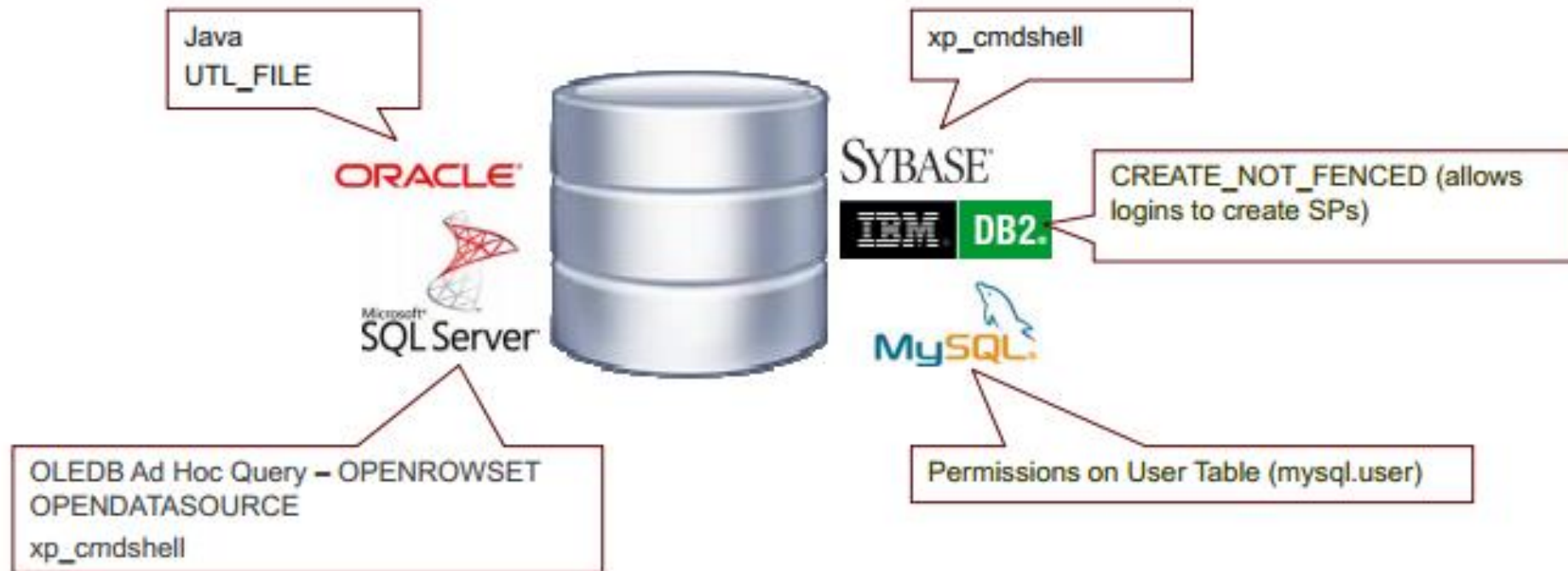
... grant execute on dbms_java_test to SYS,ALL

5.6 Top 10 lỗ hổng CSDL trên thực tế (tiếp)

4. Unnecessary Enabled DBMS Features (Cho phép chạy những tính năng không cần thiết)
 - Tin tặc có nhiều lựa chọn vị trí tấn công CSDL do những tính năng không cần thiết của CSDL làm tăng số điểm đầu vào.
 - Một số tính năng không cần thiết, nhưng lại có khả năng truy nhập sâu vào CSDL và hệ thống.

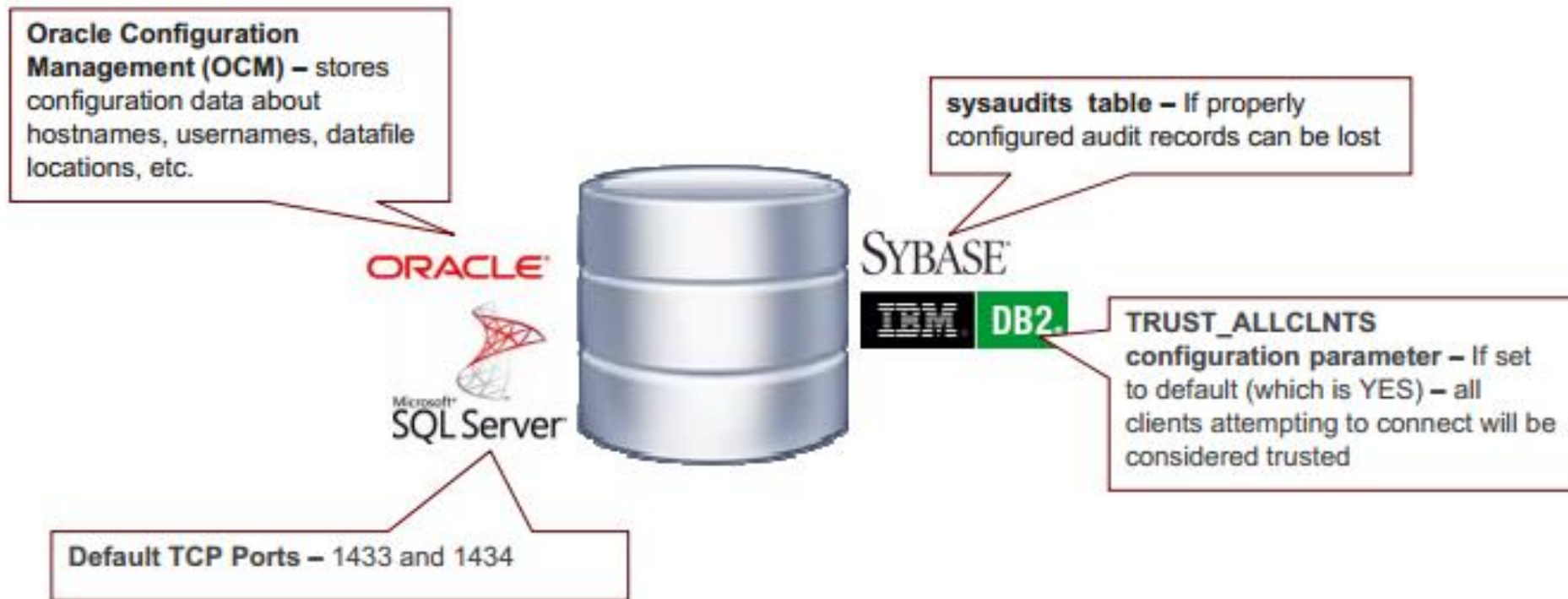
5.6 Top 10 lỗ hổng CSDL trên thực tế (tiếp)

❖ Unnecessary Enabled DBMS Features: Ví dụ



5.6 Top 10 lỗ hổng CSDL trên thực tế (tiếp)

5. Broken Configuration Management (Quản lý cấu hình bị lỗi): tiềm ẩn nguy cơ bị tấn công.



5.6 Top 10 lỗi hồng CSDL trên thực tế (tiếp)

6. Buffer Overflow (Lỗi tràn bộ đệm):

- Có thể làm máy chủ ngừng hoạt động
- Nạp và thực hiện mã độc
- VD:
 - Sâu Slammer khai thác lỗi tràn bộ đệm trên MS SQL 2000
 - Lỗi tràn bộ đệm Heap trong hàm REPEAT trên IBM DB2

5.6 Top 10 lỗi hồng CSDL trên thực tế (tiếp)

7. Privilege Escalation (Leo thang đặc quyền)

- Lỗi có thể giúp người dùng với quyền truy nhập thấp giành được quyền truy nhập cao hơn;
- Từ user bình thường có thể trở thành DBO (Database Owner), hoặc DBA (Database Admin);

5.6 Top 10 lỗ hổng CSDL trên thực tế (tiếp)

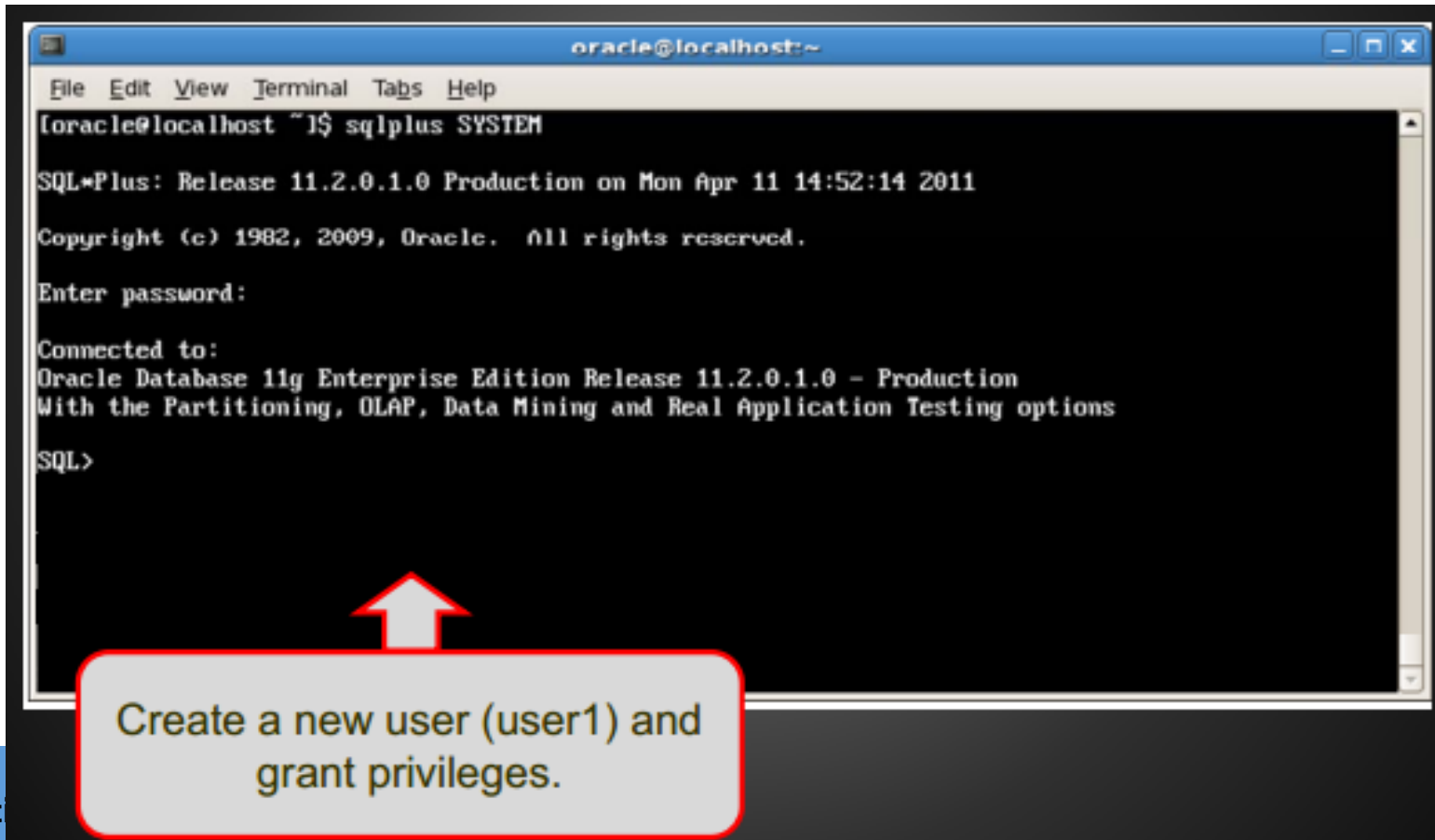
- ❖ Privilege Escalation (Leo thang đặc quyền): Lỗi trong MDSYS.RESET_INPROG_INDEX của Oracle11g R2 cho phép leo thang đặc quyền.
- ❖ Cài đặt:
 - Tạo 1 thủ tục *myproc* chứa mã cấp quyền cho người dùng hiện tại thành DBA;
 - Tạo hàm *myfn* chứa mã để tạo 1 trigger trong system schema. Trigger chứa lệnh gọi thực hiện *myproc*.

5.6 Top 10 lỗ hổng CSDL trên thực tế (tiếp)

- ❖ Privilege Escalation (Leo thang đặc quyền): Lỗi trong MDSYS.RESET_INPROG_INDEX của Oracle11g R2 cho phép leo thang đặc quyền.
- ❖ Khai thác:
 - Khai thác lỗi trong MDSYS.RESET_INPROG_INDEX, yêu cầu MDSYS thực hiện *myfn* để tạo trigger;
 - Sử dụng người dùng có quyền PUBLIC để chạy 1 lệnh SQL để kích hoạt việc thực hiện trigger đã tạo. Hệ thống sẽ thực hiện trigger và trigger sẽ gọi thực hiện *myproc* cấp quyền DBA cho người dùng.

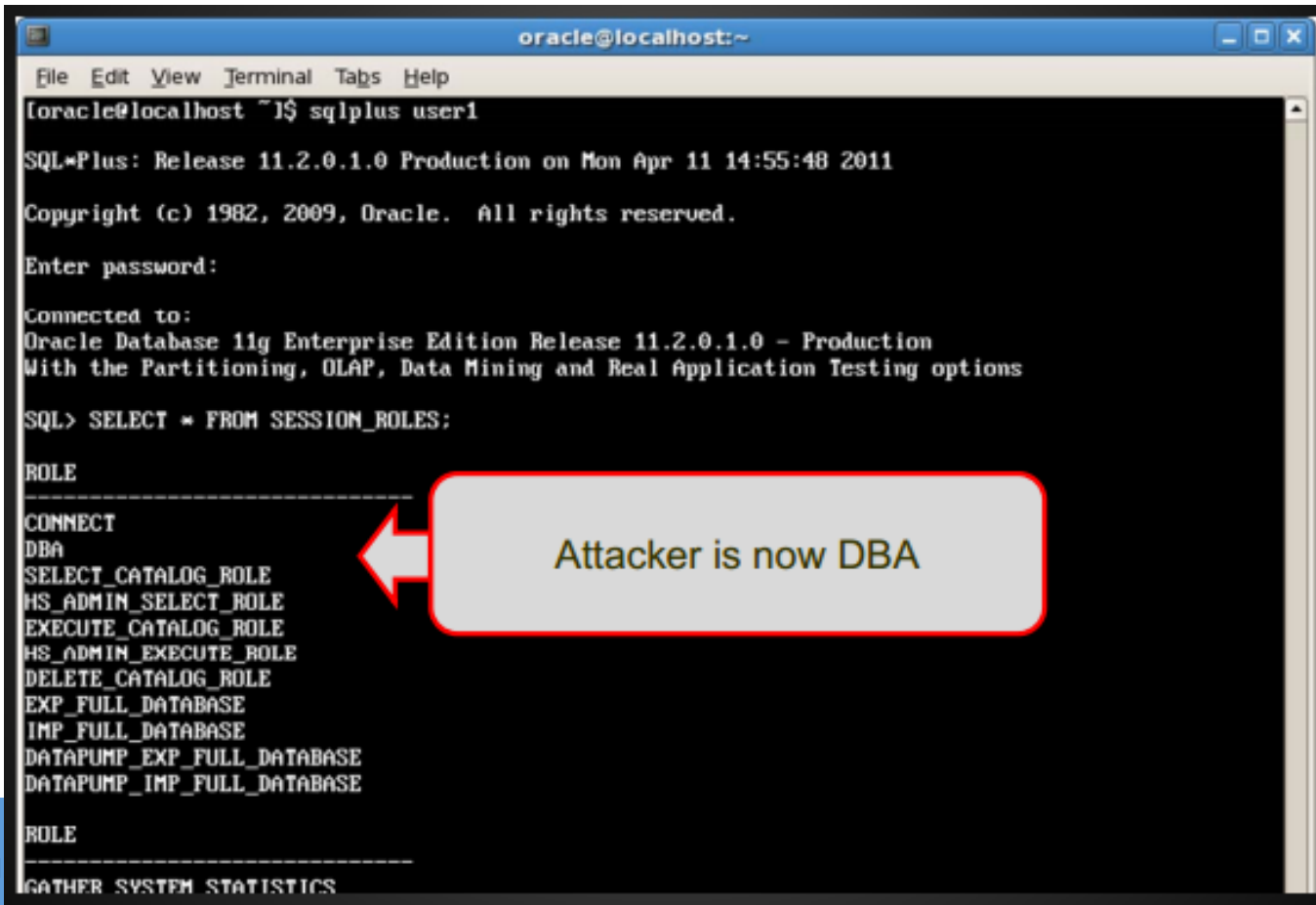
5.6 Top 10 lỗ hổng CSDL trên thực tế (tiếp)

- ❖ Privilege Escalation (Leo thang đặc quyền): Lỗi trong MDSYS.RESET_INPROG_INDEX của Oracle11g R2 cho phép leo thang đặc quyền.



5.6 Top 10 lỗ hổng CSDL trên thực tế (tiếp)

- ❖ Privilege Escalation (Leo thang đặc quyền): Lỗi trong MDSYS.RESET_INPROG_INDEX của Oracle11g R2 cho phép leo thang đặc quyền.



```
oracle@localhost:~  
File Edit View Terminal Tabs Help  
[oracle@localhost ~]$ sqlplus user1  
  
SQL*Plus: Release 11.2.0.1.0 Production on Mon Apr 11 14:55:48 2011  
  
Copyright (c) 1982, 2009, Oracle. All rights reserved.  
  
Enter password:  
  
Connected to:  
Oracle Database 11g Enterprise Edition Release 11.2.0.1.0 - Production  
With the Partitioning, OLAP, Data Mining and Real Application Testing options  
  
SQL> SELECT * FROM SESSION_ROLES;  
  
ROLE  
-----  
CONNECT  
DBA  
SELECT_CATALOG_ROLE  
HS_ADMIN_SELECT_ROLE  
EXECUTE_CATALOG_ROLE  
HS_ADMIN_EXECUTE_ROLE  
DELETE_CATALOG_ROLE  
EXP_FULL_DATABASE  
IMP_FULL_DATABASE  
DATAPUMP_EXP_FULL_DATABASE  
DATAPUMP_IMP_FULL_DATABASE  
  
ROLE  
-----  
GATHER_SYSTEM_STATISTICS
```

Attacker is now DBA

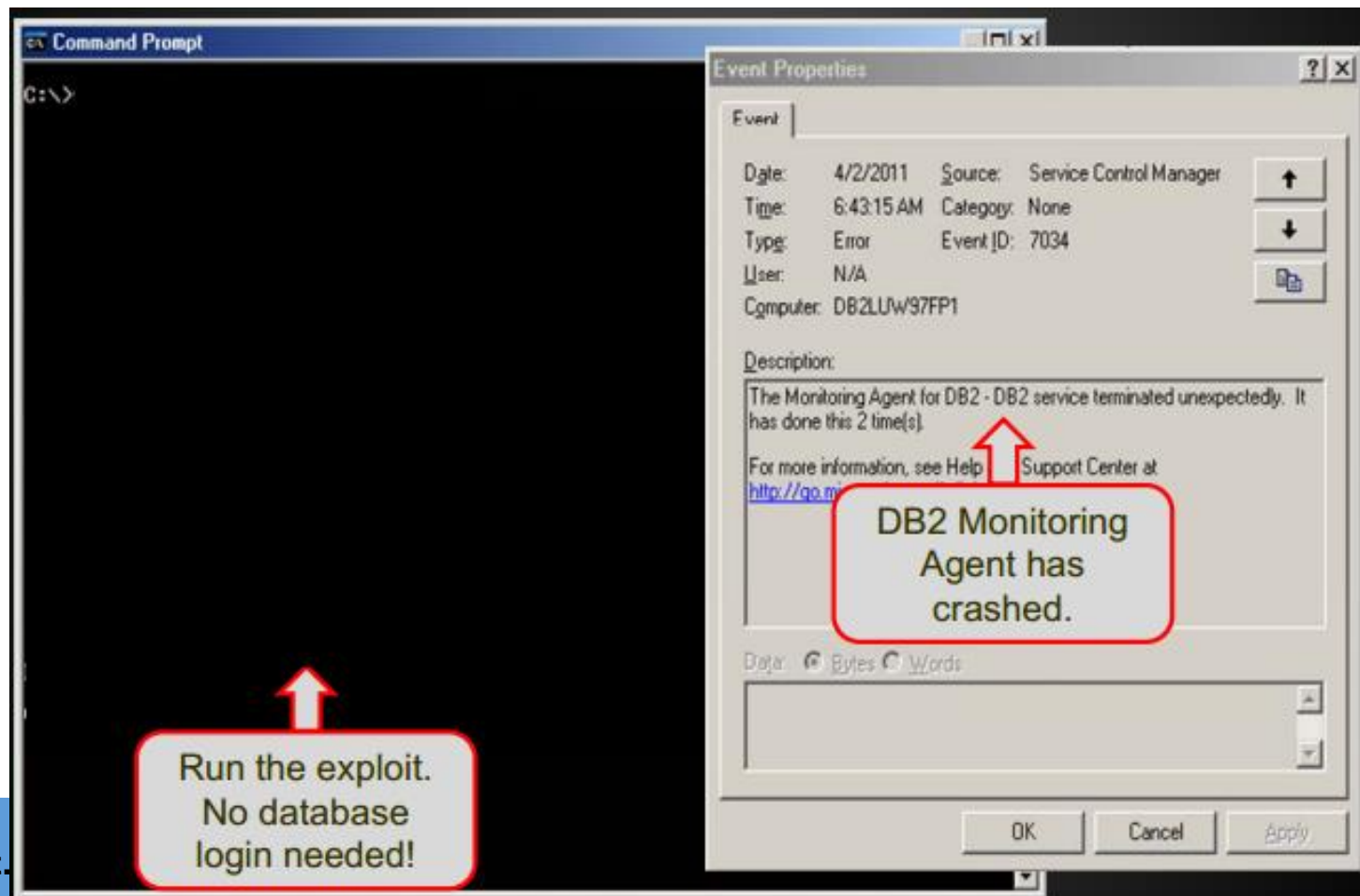
5.6 Top 10 lỗi hồng CSDL trên thực tế (tiếp)

8. Denial of Service (DoS): tấn công từ chối dịch vụ

- Có thể làm máy chủ CSDL hoặc cả hệ thống ngừng hoạt động;
- Có thể gây ngập lụt đường truyền;
- VD:
 - Sâu Slammer khai thác lỗi tràn bộ đệm để tấn công DoS, lây lan đến 75.000 máy chủ MS SQL 2000 trong 10 phút;
 - Lỗi trong Tivoli DB2 monitoring agent của IBM DB2 LUW 9.7 cho phép tin tặc tấn công DoS vào CSDL.

5.6 Top 10 lỗi hỏng CSDL trên thực tế (tiếp)

- ❖ Denial of Service (DoS): Lỗi trong Tivoli DB2 monitoring agent của IBM DB2 LUW 9.7 cho phép tin tặc tấn công DoS vào CSDL.



5.6 Top 10 lỗ hổng CSDL trên thực tế (tiếp)

9. Unpatched Database (CSDL không được vá)

- Các mã khai thác các lỗi đã biết xuất hiện rất nhanh trên mạng Internet;
- Cần có cơ chế cập nhật/vá lỗi phù hợp.

5.6 Top 10 lỗi hỏng CSDL trên thực tế (tiếp)

10. Unencrypted Data (Không mã hóa dữ liệu)

- Dữ liệu nhạy cảm (tại chỗ hoặc trên đường truyền) không được mã hóa có thể bị nghe trộm, đánh cắp;
- Với dữ liệu lưu:
 - Mã hóa hệ thống file
 - Mã hóa dữ liệu kiểu trong suốt (TDE)
- Với dữ liệu trên đường truyền:
 - Sử dụng SSL/TLS
 - Kerberos
 - Oracle ASO.

5.6 Top 10 lỗi hỏng CSDL trên thực tế (tiếp)

❖ Not Doing Anything (Không làm gì cả)

- Chỉ dựa vào các lớp bảo vệ bên ngoài, như tường lửa,... là không đủ;
- Không có lớp bảo vệ nào có thể đảm bảo an toàn tuyệt đối cho CSDL;
- Không làm gì cả có tác hại tương đương như hành động phá hoại của tin tặc.