Buổi 1 - Tải Oracle

2007 : Hãng The SecureWorks: 8000 vụ tấn công cơ sở dữ liệu mỗi ngày

1 trong các vụ: CardSystems Solutions

Sử dụng Sql Injection chiếm quyền điều khiển hệ thống CSDL, chuyển toàn bộ CSDL ra ngoài

Khoảng 40 triệu thẻ tín dụng bị đánh cắp gây thiệt hại hàng triệu USD

2008: Hãng Heartland Payment

Hơn 40 triệ chi tiết các tìa khoản ngân hàng bị lấy cắp

Gây ra bởi Albert Gonzalez, sau đó bị bắt 20 năm

2010: Hacker VN

Lấy cắp khoảng 100.000 thẻ tín dụng ở Anh trị giá 6 triệu Bảng Anh

2010: Wikileaks.org

Tất cả thông tin tuyệt mật chưa được tiết lộ của các nước được công bố trên Web

Gồm:

Các báo cáo mật về cuộc chiến Afghanistan, Iraq

Tài liệ mật của Bộ ngoại giao Mỹ

Các cơ sở hạ tầng và nguồn lực ảnh hưởng đến Mỹ

2011: Vietnamnet

Cuối ngày 4/1/2011, bị tấn công DDOS quy mô lớn

Hoạt động tình báo mạng phát triển mạnh

2/2013: Mandiant công bố báo cáo nhóm hacker APT1 (đơn vị 61398 của PLA)

Tấn công APT: <https://quantrimang.com/phuong-thuc-tan-cong-mang-apt-la-gi-156569>

Đơn vị 61398 của PLA: <https://vi.wikipedia.org/wiki/%C4%90%C6%A1n_v%E1%BB%8B_61398_c%E1%BB%A7a_qu%C3%A2n_%C4%91%E1%BB%99i_Trung_Qu%E1%BB%91c>

5/2015: FireEye công bố báo cáo về APT20 the dõi báo VN suốt 10 năm

6/2015: Kaspersky bị tấn công suốt 1 năm

Bí mật nhà nước bị tiết lộ với quy mô lớn

2010: Chelsea Manning (Mỹ)

- 400.000 báo cáo tại chiến sụ Iraq

- 91.000 báo cáo chiến sự tại Afganistan

- 250.000 công điện ngoại giao

- 1 video trực thăng Mỹ tấn công người Iraq

2013: Eedward Showden (Mỹ)

- Chương trình nghe lén PRISM

- Mỹ do thám cả đồng minh

- Hệ thông tấn công mạng

Tính thời sự của ATTT

Dự thảo luật An Toàn thông tin mạng (từ 2012)

Phê duyệt “Đề án đoà toạ và phát triển nguồn nhân lực an toàn

Luật an toàn thông tin mạng

**10 tấn công hàng đầu vào CSDL**

1. Excessive privileges (đặc quyền quá lớn)
   1. Người quản trị gán cho User quá nhiều quyền
2. Privilege abuse (lạm dụng quyền)
   1. Hacker bán các thông tin từ quyền mà User được cấp
3. Unauthorized privilege elevation (nâng quyền bất hợp pháp) (Stored procedure, weak function)
   1. Hacker có tk thông thường và dựa vào các quyền mà User đó có mà leo thang đặc quyền
4. Platform vunerabilities (sâu Blaster - Windows 2000 - DoS)
   1. Hacker lợi dụng các điểm yếu xâm phạm vào HĐH và CSDl
5. SQL Injection
   1. Admin không lọc đầu vào, hacker lợi dụng tiêm vào các ký tự đặc biệt hợp lệ để lấy các thông tin
   2. Điều kiện cần
      1. Hệ QTCSDL sử dụng SQL
   3. Điều kiện đủ
      1. Admin không loại bỏ những ký tự đặc biệt đầu vào
6. Weak audit
   1. Kiểm toán yếu
7. Denial of service
   1. Tại 1 thời điểm, Hacker thức hiện rất nhiều request đến Server, từ đó ko thể trả lời request của những người dùng hợp pháp
8. Database protocol vulnerabilities (sâu SQL Slammer2 - SQL Server - DoS)
9. Weak authentication
10. Exposure Of backup data (lộ dữ liệu dự phòng)
    1. Tấn công vét cạn
    2. Tấn công từ điển