

## CHƯƠNG 6.

# An toàn mạng

Các mối đe dọa

Các biện pháp ngăn  
chặn

## 6.1. Các mối đe dọa

- Thăm dò
- Nghe trộm
- Mạo danh, lừa đảo
- Lỗ hổng trang Web
- Từ chối dịch vụ.
- Mã lưu động
- ...

## 6.1.1. Thăm dò

- Quét cổng – Port Scan
  - Thu thập thông tin đối tượng tấn công
    - + Dịch vụ, cổng đang hoạt động.
    - + Phiên bản hệ điều hành.
    - + Phiên bản ứng dụng.
  - Tham khảo danh sách lỗ hổng của các phiên bản
  - Thực hiện tấn công

## 6.1.2. Nghe trộm

- Cáp truyền.
  - Sử dụng “packet sniffer”
  - Lập trình lại card.
- Wireless
  - Sử dụng ăng ten

## 6.1.3. Mạo danh, lừa đảo

- Phỏng đoán thông tin xác thực của đối tượng tấn công.
  - Đoán mật khẩu
- Nghe trộm thông tin xác thực của đối tượng tấn công.
  - Nghe trộm mật khẩu
- Lợi dụng lỗ hổng cơ chế xác thực
  - Tràn bộ đệm
- Thông tin xác thực công cộng
- Man-in-the-middle
- Phishing

## 6.1.4. Lỗ hổng trang web

- Bôi xấu (Defacement)
- Tràn bộ đệm
- Dot-Dot-Slash
- Gọi phương thức phía máy chủ

## 6.1.5. Từ chối dịch vụ

- Tràn kết nối (Connection Flooding)
  - Tấn công giao thức TCP, UDP, ICMP
- DNS (Domain Name Server)
  - Tận dụng lỗi Buffer Overflow để thay đổi thông tin định tuyến
  - DNS cache poisoning
- Từ chối dịch vụ phân tán (DDoS)
  - Dùng các Zombie đồng loạt tấn công

## 6.1.6. Mã lưu động

- ❑ Cookie.
  - Cookie lưu thông tin người dùng (phiên, lâu dài)
- ❑ Scripts.
  - Tấn công các trang ASP, JSP, CGI, PHP
- ❑ ActiveX
- ❑ Mã Java
  - Applet
- ❑ Auto Exec
  - .exe, .doc
- ❑ Bot
  - Trojan Horse

## 6.2. Các biện pháp ngăn chặn

- Mã hóa
- Xác thực
- Tường lửa
- Phát hiện đột nhập
- ...

## 6.2.1. Mã hóa

- Mã hóa liên kết
  - Thông tin được mã hóa ở tầng Data link của mô hình OSI
- Mã hóa end-to-end.
  - Thông tin được mã hóa ở tầng Application của mô hình OSI
- VPN (Virtual Private Network)
  - Trap đổi thông tin giữa người dùng và Firewall qua kênh mã hóa.
- PKI
  - Mật mã công khai và chứng nhận
- Giao thức mật mã
  - SSH, SSL, IPSec

## 6.2.2. Xác thực

- Mật khẩu một lần
  - Password Token
- Hệ Challenge-Response
- Xác thực số phân tán
- Kerberos

### 6.2.3. Tường lửa

- Công cụ để lọc thông tin di chuyển giữa “mạng bên trong” và “mạng bên ngoài”
- Mục tiêu ngăn chặn nguy cơ đến từ “mạng bên ngoài”
- Thực hiện ngăn chặn thông qua chính sách an toàn

# Các loại tường lửa

- Lọc gói (Packet Filtering Gateways)
- Duyệt trạng thái (Stateful Inspection Firewalls)
- Cổng ứng dụng (Application Proxies)
- Gác (Guards)
- Cá nhân (Personal Firewalls)

## 6.2.4. Phát hiện đột nhập

- ❑ Kiểm tra người dùng và hoạt động hệ thống.
- ❑ Ghi lại cấu hình hệ thống để phát hiện nguy cơ
- ❑ Đánh giá tính toàn vẹn của hệ thống và dữ liệu
- ❑ Phát hiện các dạng tấn công
- ❑ Phát hiện các hoạt động bất thường thông qua phân tích thống kê
- ❑ Sửa chữa lỗi cấu hình hệ thống
- ❑ Cài đặt và vận hành các hệ thống bẫy đột nhập

# Các loại hệ thống phát hiện đột nhập

- Hệ thống phát hiện đột nhập dựa trên mẫu
- Hệ thống phát hiện đột nhập dùng Heuristics
- Hệ thống phát hiện đột nhập hoạt động bí mật
- Hệ Tripwire

# Cảm ơn!

