Chương 2

Các rủi ro tiềm tàng

Nội dung

- Tính toán các chiến thuật tấn công
- Các tấn công phổ biến
- Những vấn đề về bảo mật TCP/IP
- Các chương trình nguy hại
- Vấn đề con người

2.1 Tính toán chiến thuật tấn công

- Tấn công xảy ra?

  Một nhóm các cá nhân cố gắng truy xuất, hiệu chỉnh hoặc làm hư hệ thống hoặc môi trường
- Các mục đích tấn công:
  - Tấn công truy xuất: truy xuất tài nguyên
  - Tấn công phản đối hoặc chỉnh sửa: muốn chỉnh sửa thông tin trong hệ thống
  - Tấn công từ chối phục vụ (DoS): phá vỡ hệ thống mạng và các dịch vụ

Tấn công truy xuất

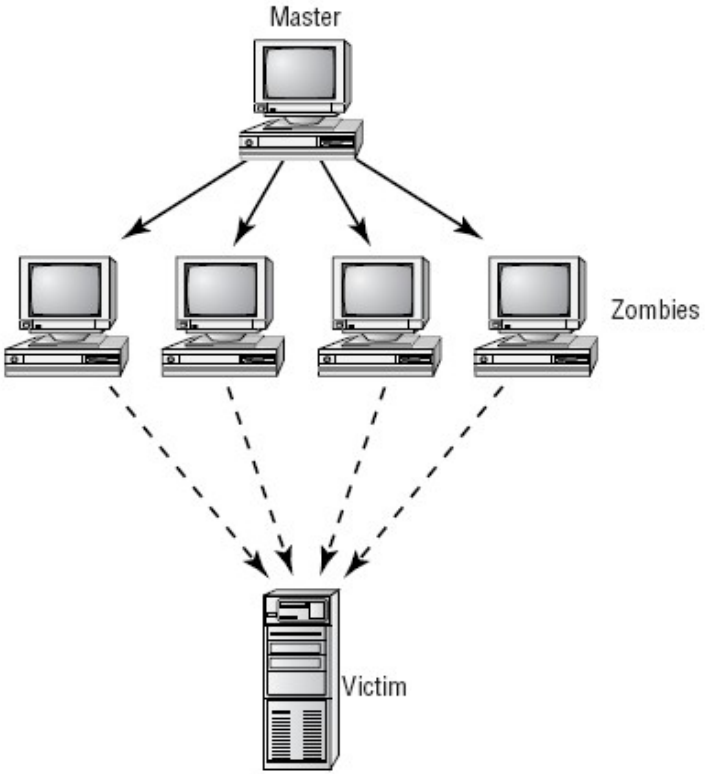
- Tấn công truy xuất từ bên trong và bên ngoài
- Dumpster diving
- Đánh cắp dữ liệu đang truyền qua lại giữa 2 hệ thống:
  - Nghe lén
  - Rình mò
  - Sử dụng thiết bị nghe chặn

Tấn công phản đối hoặc chỉnh sửa

- Tấn công chỉnh sửa: xóa, thêm, thay đổi thông tin không có quyền truy xuất
- Tấn công phản đối: làm thông tin trở nên không có nghĩa hoặc thông tin giả. Ví dụ: gửi email khích động

Tấn công DoS và DDoS

- DoS nhằm ngăn chặn truy xuất tài nguyên bất hợp pháp.
  - DoS trên TCP, gọi là TCP SYN flood
    - Ping of death: gửi gói ICMP có kích thước lớn hơn hệ thống xử lý.
    - Buffer overflow.
- DDoS: distributed DoS

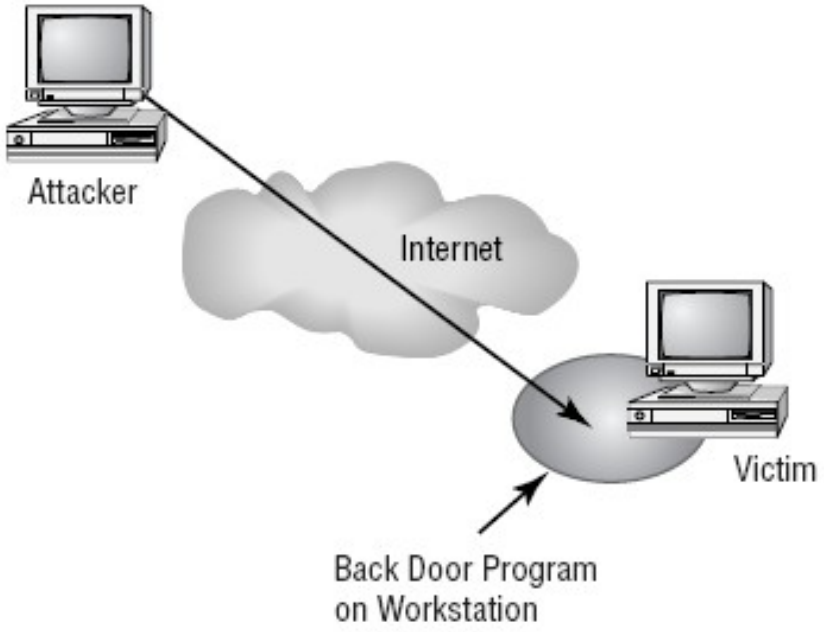


2.2 Các tấn công phổ biến

- Back-door
- Spoofing
- Man-in-the-Middle Attack
- Replay Attack
- Password-Guessing Attacks

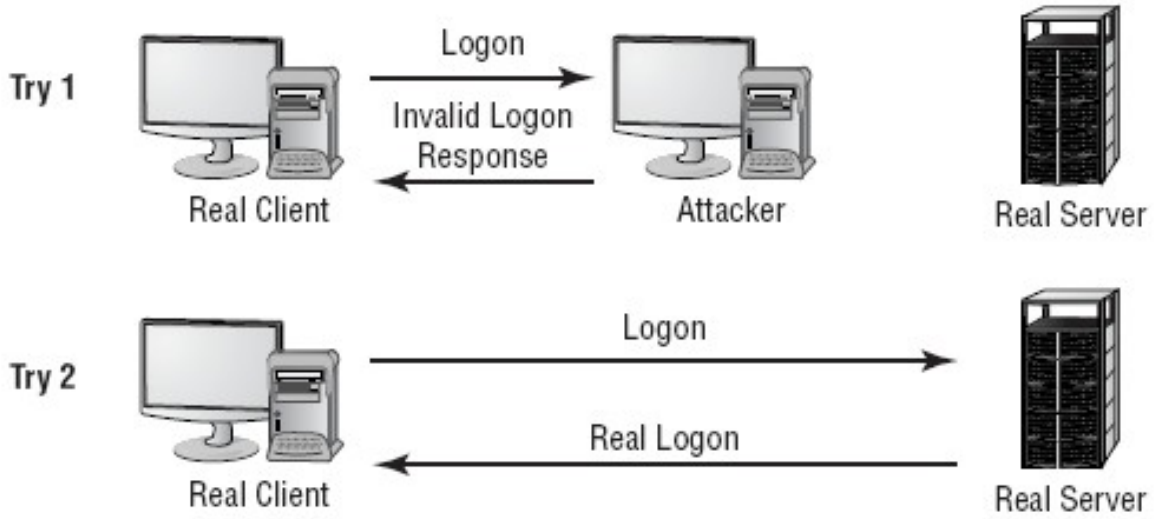
Back-door

- Tấn công truy xuất hoặc tấn công chỉnh sửa
- Debug, sửa lỗi, truy cập vào chương trình
- Giành quyền truy xuất vào hệ thống mạng và chèn thêm chương trình tạo lối sau cho kẻ xâm nhập.



Tấn công Spoofing

- Tấn công truy xuất
- IP spoofing, và DNS spoofing



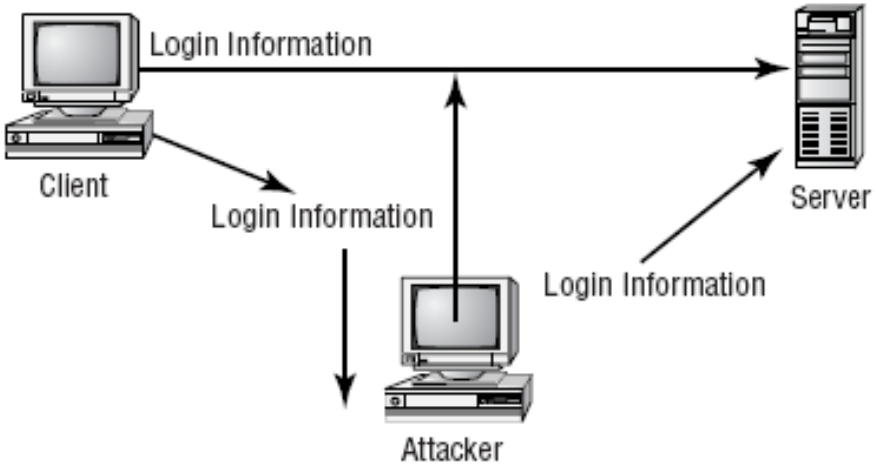
Attacker now has logon and password.

Man-in-the-Middle Attacks

- Khá phức tạp
- Tấn công truy xuất, hoặc tấn công hiệu chỉnh
- Sử dụng chương trình trung gian giữa server và user

Replay Attack

- Tấn công truy xuất hoặc hiệu chỉnh

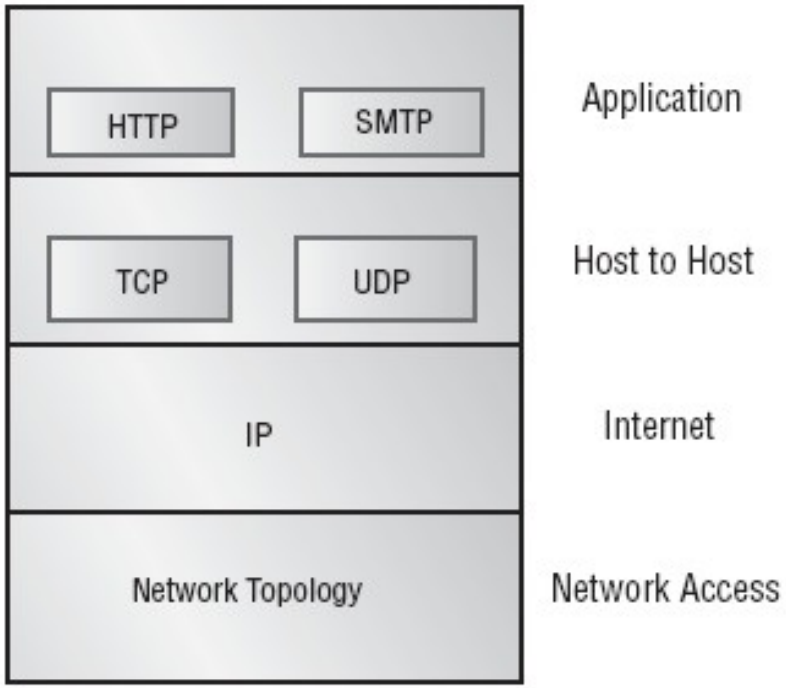


Password-Guessing Attacks

- Xảy ra khi 1 account bị tấn công lặp đi lặp lại
- Brute-Force
- Dictionary

2.3 Những vấn đề bảo mật TCP/IP

- Application layer
- Host-to-Host hoặc Transport lay
- Internet layer
- Network Interface layer



Application layer

- HTTP
- FTP
- SMTP
- Telnet
- DNS
- RIP: cho phép trao đổi thông tin tìm đường giữa các router
- SNMP: là công cụ quản trị cho phép trao đổi thông tin giữa các thiết bị mạng và chương trình quản trị.
- POP

Host-to-host / Transport layer

- TCP
- UDP

Internet Layer

- IP (internet protocol)
- ARP (Address Resolution Protocol)
- ICMP (Internet Control Management Protocol)
- IGMP (Internet Group Management Protocol)

The Network Interface Layer

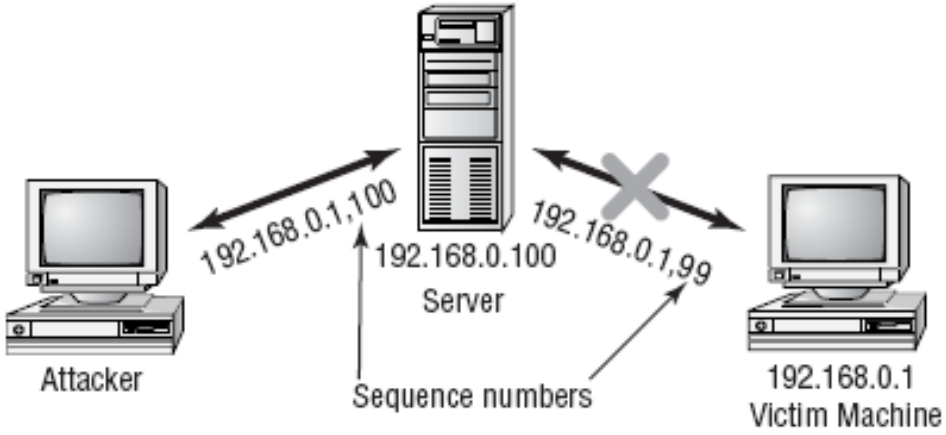
- Đặt và lấy các packets trên đường truyền vật lý thông qua card mạng

Xác định các tấn công TCP/IP

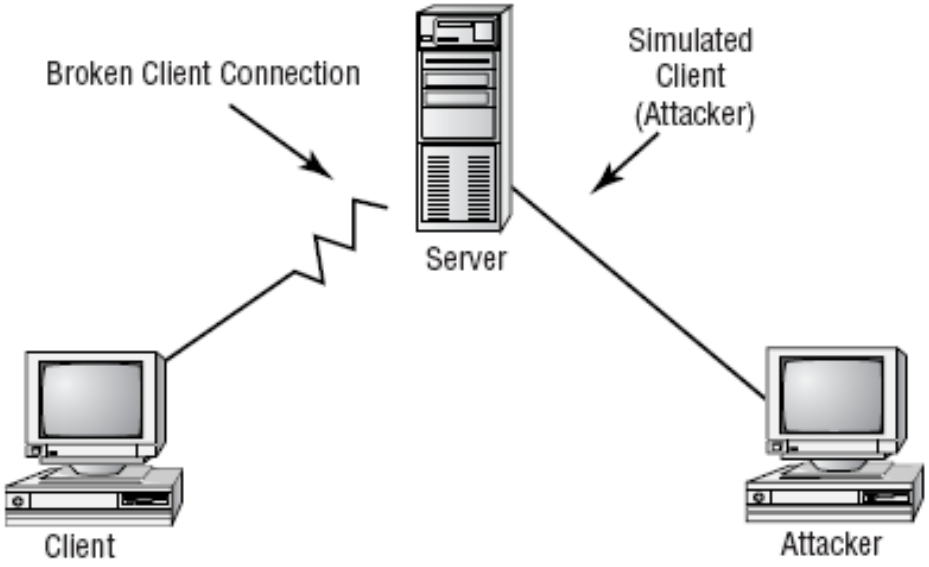
- Thường xảy ra ở lớp Host-to-Host hoặc lớp Internet
- Tấn công từ bên ngoài có thể giới hạn bằng các thiết bị trong mạng
- TCP, UDP, IP dễ bị tấn công
- Tấn công từ bên trong dễ xảy ra khi sử dụng các chương trình có sẵn.
- Sniffing Network
  - Thiết bị bắt và hiển thị luồng thông tin qua mạng: máy tính
  - Network sniffer là gói phần mềm trong System Management Server
  - Nắm bắt được tất cả thông tin truyền trong mạng

- Quét Port
  - TCP/IP có các port có sẵn trong router
  - Sẽ được cung cấp khi có yêu cầu
  - Có thể yêu cầu tra các dịch vụ và port đang mở
- Tấn công TCP
  - TCP SYN or TCP ACK Flood Attack
  - TCP Sequence Number Attack
  - TCP/IP Hijacking: khó nhận biết hơn DoS

- TCP Sequence number attack



- TCP/IP Hijack



- Tấn công UDP
  - *UDP flooding:* UDP flooding làm quá tải các dịch vụ, mạng và server. Lượng lớn các packet UDP nhắm đến mục tiêu tấn công làm dịch vụ UDP tại máy bị tấn công shut down.
  - UDP floods cũng làm quá tải băng thông network và hiện tượng DoS.
  - Tấn công ICMP
  - Tấn công ICMP Tunnel
- Tấn công qua lỗ hổng phần mềm

2.4 Các chương trình gây hại

- Mã gây hại?
- Viruses, Trojan horses, bombs, and worms
- Ví dụ: Melissa, 3/1999
- Virus:
  - Chương trình nhiễm
  - Xóa file, format…
  - polymorphic, stealth, retroviruses, multipartite, armored, companion, phage, and macro viruses

Các triệu chứng khi máy nhiễm virus

- Chương trình khởi động chậm
- Xuất hiện các file bất thường trên máy, hoặc mất file.
- Dung lượng file tăng
- Máy tự động shutdown hoặc tự khởi động lại
- Không truy cập được ổ đĩa hay thư mục
- …

Cơ chế hoạt động của virus

- Thực hiện 1 trong 2 điều:
  - Làm cho máy không hoạt động
  - Hoặc lây nhiễm máy khác
- Cơ chế:
  - Khi máy bị nhiễm, virus tự thêm vào các file, sao chép nhân bản từ máy này sang máy khác, hoặc từ file này sang file khác.
- Phân loại:
  - Virus đa hình: tự thay đổi tránh bị phát hiện, tấn công máy, hiện thông báo, xóa file…
  - Stealth virus: tự ẩn nấp, thường lưu trú ở boot sector. Kích thước file bị nhiễm thường được khai báo lớn hơn nguyên bản
  - Retrovirus: tấn công hoặc vượt qua tầm kiểm soát ct diệt virus

- Phân loại (tt):
  - Multipartite Virus: tấn công nhiều cách. Lây nhiễm boot sector, lây nhiễm tất cả các file thực thi, xóa các tập tin ứng dụng
  - Armored virus: được thiết kế rất khó phát hiện. Chứa đoạn mã ngăn chặn việc dò mã của các chương trình debugger và disassembler
  - Companion virus: tự thêm vào các chương trình hợp pháp và tạo ra chương trình có phần mở rộng khác. Được chạy khi user chạy chương trình có sẵn bị tấn công
  - Phage virus: chỉnh và sửa chữa cơ sở dữ liệu
  - Macro virus

Các chương trình gây hại

- Trojan:
  - File đính kèm
  - Mở port
  - Sử dụng phương pháp scan port
- Logic Bomb
  - Thực hiện tấn công vào 1 thời điểm định sẵn trước
- Worm
  - Khác virus
  - Tự nhân bản
  - Không cần chương trình chủ lây nhiễm

2.5 Vấn đề con người

- Khó quản lý
- Tấn công qua điện thoại, email, tại công sở