Chương 2

AN TOÀN THÔNG TIN TRÊN INTERNET

41

TRƯỜNG ĐẠI HỌC MỞ TP. HCM
Cơ hội học tập cho mọi người

Nội dung

- Hạ tầng mạng, OSI, TCP/IP.
- TCP/IP, UDP, ICMP,Smurf Attack.
- DDOS
- Mã độc, virus
- Social Engineering
- Các giao thức bảo mật trên mạng internet

42

2.1 Hạ tầng mạng

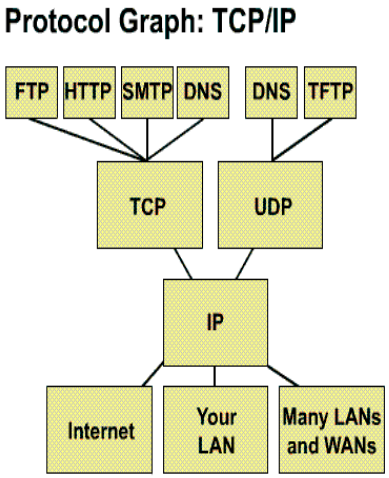
Chuẩn OSI và TCP/IP

Mô hình phân lớp nhằm

- ✓Giảm độ phức tạp
- ✓Tiêu chuẩn hoá các giao diện
- ✓Module hoá các chi tiết kỹ thuật
- ✓Đảm bảo mềm dẻo quy trình công nghệ
- ✓Thúc đẩy quá trình phát triển
- ✓Dễ dàng trong việc giảng dạy ,huấn luyện

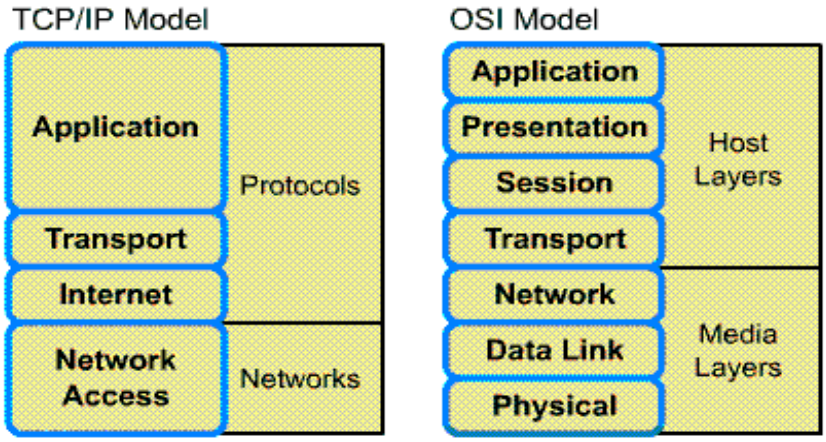
43

Mô hình TCP/IP



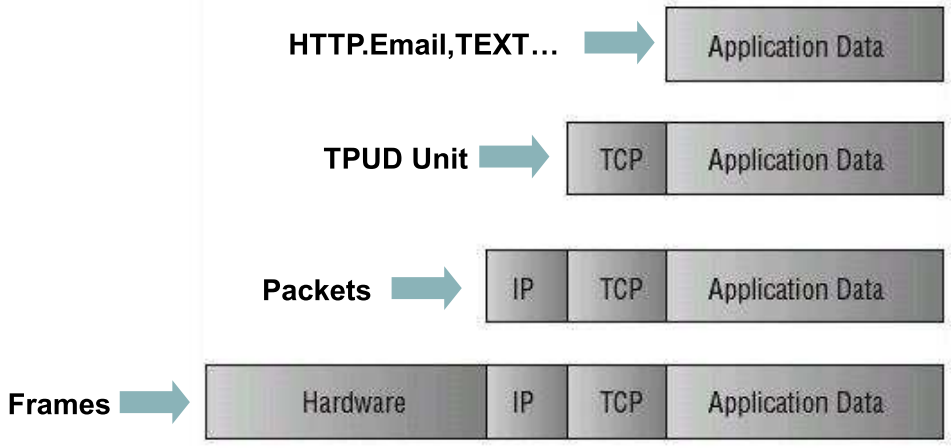
44

Mô hình OSI và TCP/IP



45

Đóng gói trong TCP/IP



46

Các điểm yếu dễ bị khai thác trên mạng

- TCP/IP Attacks

Xảy ra trên lớp IP hay “host –to- host”

Router /Firewall có thể ngăn chặn một số giao thức phổ biến trên hệ thống thông tin, mạng Internet

- ARP không phải giao thức định tuyến nên không gây tổn thương do các tấn công từ bên ngoài

- Các điểm yếu : SMTP & ICMP, TCP, UDP và IP → có thể vượt qua các lớp mạng

47

2.2 Các hình thức attack TCP/IP attack

- Port Scans : Dò quét các cổng hệ thống

- TCP Attacks :

TCP SYN or TCP ACK Flood Attack,

TCP Sequence Number Attack,

TCP/IP Hijacking

Network Sniffers : Bắt giữ và hiển thị các thông tin mạng

48

UDP Attack

UDP attack sử dụng các giao thức bảo trì hệ thống hoặc dịch vụ UDP để làm quá tải các dịch vụ giống như DoS . UDP attack khai thác các giao thức UDP protocols.

UDP packet không phải là " connection-oriented" nên không cần "synchronization process – ACK"

UDP attack - *UDP flooding (Tràn ngập UDP)*

Tràn ngập UDP gây quá tải băng thông của mạng dẫn đến DoS .

49

ICMP attacks
Smurf và ICMP tunneling

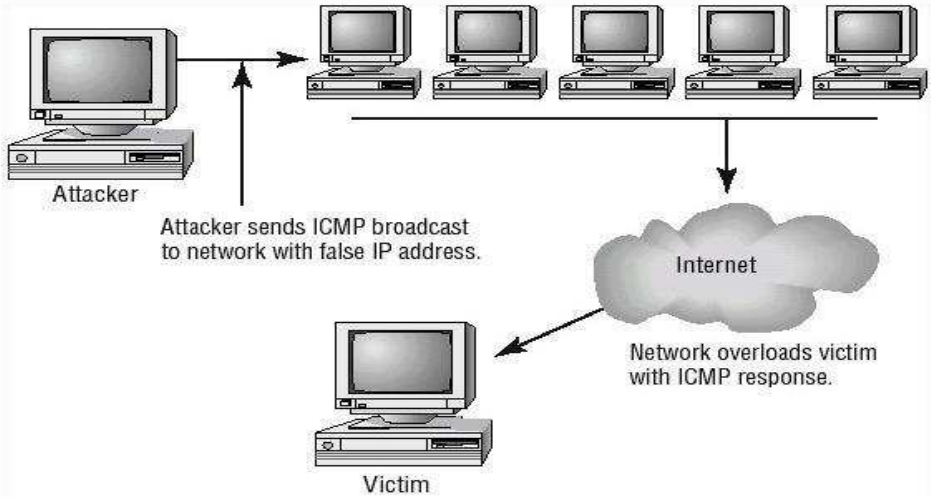
Cấu tạo gói tin ICMP

- Type (8 bits) [8 bít sử dụng để nhận diện loại ICMP]
- Code (8 bits) [Mỗi Type cụ thể có nhưng code cụ thể riêng để miêu tả cho dạng đó]
- Checksum (16 bits) [Checksum gồm 16bits]
- Message (Không cố định) [Phụ thuộc vào type và code]

- ICMP sử dụng PING program. Dùng lệnh PING đến IP của máy đích
- Gây ra do sự phản hồi các gói ICMP khi có các yêu cầu phát đi.

50

SMURF ATTACKS



51

SMURF ATTACKS

- Attacker gửi packet đến các Network Amplifier
- Thường là những packet ICMP ECHO REQUEST
- Amplifier sẽ gửi đến ICMP ECHO REQUEST đến tất cả các hệ thống thuộc địa chỉ broadcast
- Tất cả các hệ thống này sẽ REPLY packet về địa chỉ IP của mục tiêu tấn công Smurf Attack.

52

2.3 Tấn công DDOS

Các giai đoạn của một cuộc tấn công kiểu DDoS:

- Chuẩn bị :

  Bước quan trọng nhất của cuộc tấn công. Sử dụng các công cụ DDoS hoạt động theo mô hình client-server.

- Dùng các kỹ thuật hack khác để nắm trọn quyền một số host trên mạng, hệ thống thông tin.
- Cấu hình và thực nghiệm toàn bộ attack-network client

53

Một số Tool DDOS

1. Slowloris
2. HTTP POST 3.6
3. DDosim
4. Keep-alive attack
5. Low Orbit Ion Cannon Anonymous
6. r-u-dead
7. Slow Post Newver
8. Smurf 6.0
9. DNSDRDOS
10. Tools Slow dos PURIDDE Goobye ver3.0

54

Anti - DDOS

Có ba giai đoạn chính trong quá trình Anti-DDoS:

- Giai đoạn ngăn ngừa: tối thiểu hóa lượng Agent, tìm và vô hiệu hóa các Handler
- Giai đoạn đối đầu với cuộc tấn công: Phát hiện và ngăn chặn cuộc tấn công, làm suy giảm và dừng cuộc tấn công, chuyển hướng cuộc tấn công
- Giai đoạn sau khi cuộc tấn công xảy ra: thu thập chứng cứ, xử lý điểm yếu, vá lỗ hổng và rút kinh nghiệm

55

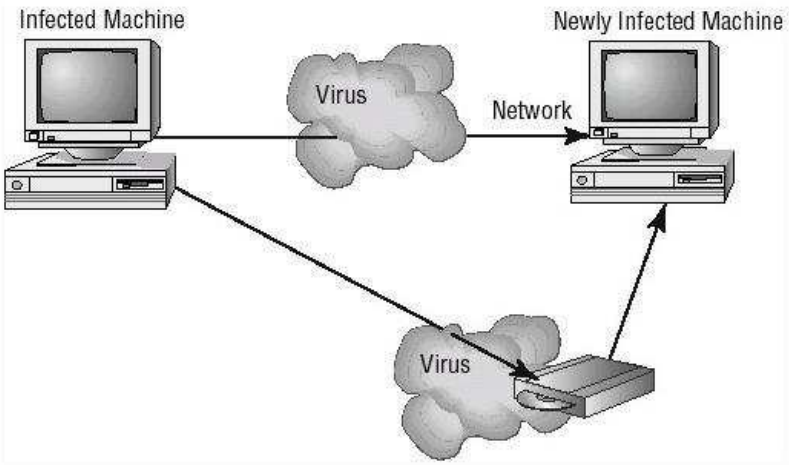
2.4 Malicious Code – Mã độc, Virus

Virus là một phần mềm được thiết kế để thâm nhập vào hệ thống máy tính. Virus làm hỏng dữ liệu trên hard disk, là sụp OS và lây lan sang các hệ thống khác.

Phương pháp lây lan : Từ floppy hoặc CD-ROM, USB, theo đường thư điện tử, mạng máy tính hoặc ký sinh làm một phần của một chương trình khác.

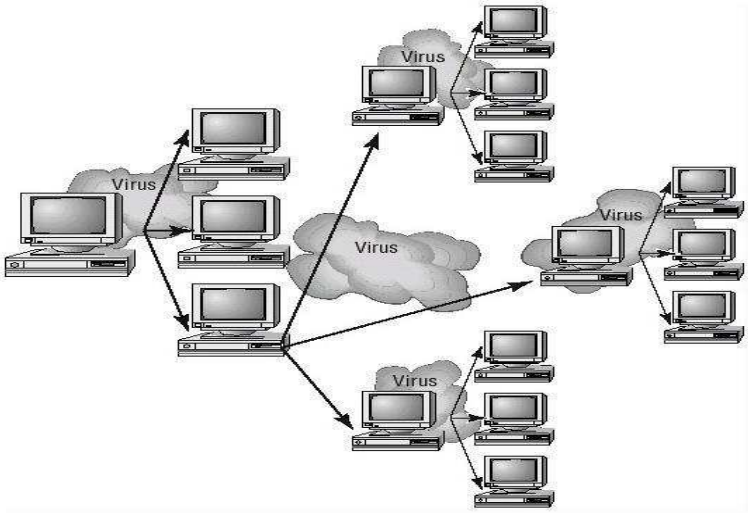
56

Hoạt động của virut



57

Virus - Lây nhiễm qua e-mail



58

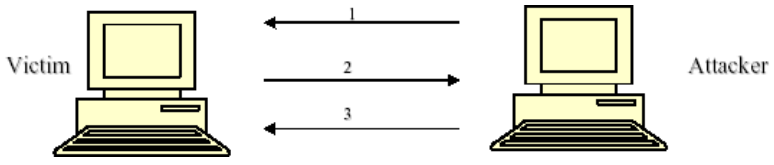
Trojan Horse

- Được gửi đính kèm một file nào đó
- "Trojan horse" còn là một phần của e-mail , free game, software hoặc một loại file nào đó. Khi nhiễm ,"trojan horse" sẽ kích hoạt các tác vụ như xử lý văn bản hoặc các file template. Hậu quả là nhiều file mới không cần thiết được sinh ra trong máy.
- "Trojan Horse" còn kích hoạt ứng dụng chạy ẩn hoặc nhiều tác vụ theo kịch bản của hacker .
- "Trojan horse" rất khó phát hiện vì chúng thường được che giấu bởi các chương trình hợp lệ .

59

Logic Bomb

- Là một đoạn mã được nhúng vào một chương trình có thể là hợp lệ trong hệ thống và được kích hoạt trong một điều kiện cho trước nào đó
- Khi kích hoạt logic bomb có thể làm thay đổi hoặc phá hủy một hoặc nhiều file dữ liệu



60

TRƯỜNG ĐẠI HỌC MỞ TP. HCM
Cơ hội học tập cho mọi người

Spyware

- Là những chương trình được bí mật cài lên máy tính
- Mục đích: theo dõi hoạt động web của người dùng, hướng trình duyệt đến các trang không mong muốn, thu thập và gửi các thông tin cá nhân,…
- Không tự lây lan mà thường lừa người dùng kích hoạt chương trình
- Khi bị nhiễm Spy, mức security của máy tính thường bị đặt xuống mức thấp nhất, tạo điều kiện cho các spyware khác lây nhiễm vào máy
- Khác với Adware, là những chương trình quảng cáo, hiện các popup (có thể chấp nhận Adware)

61

TRƯỜNG ĐẠI HỌC MỞ TP. HCM
Cơ hội học tập cho mọi người

2.5 Social Engineering

- *Social engineering* là quá trình attacker thu thập thông tin về mạng , hệ thống thông tin qua những người dùng trong một đơn vị, tổ chức
- ”Social engineering” có thể xảy ra trên điện thoại , website, e-mail, mạng xã hội hoặc qua các khách truy cập hệ thống. Giải pháp : Đào tạo , nâng cao nhận thức , ý thức của người dùng về An toàn hệ thống thông tin

62

2.6 Các giao thức bảo mật trên mạng Internet

- Bảo mật giao thức PPP (Layer 2).
- Tunneling Protocols.
- IPsec (Layer 3).
- Secure Shell (SSH) (Layer 4).
- HTTP/S – on top of SSH (Layer 4,5).
- Bảo mật E-Mail (Layer 5).
- Bảo mật Wireless network.

63

Chương 3

HẠ TẦNG KIẾN TRÚC KHÓA CÔNG KHAI (PKI)

64