An toàn Mạng

Trần Đức Khánh
Bộ môn HTTT – Viện CNTT&TT
ĐH BKHN

Mạng máy tính

- Môi trường sử dụng
- Tôpô và kích thước
- Phương tiện truyền thông
  - Cáp, Cáp quang, Vi sóng, Hồng ngọa, Satellite
- Giao thức
  - 7 tầng OSI: Vật lý, Liên kết Dữ liệu, Mạng, Vận chuyển, Phiên, Trình diễn, Ứng dụng
- Địa chỉ
  - MAC, IP
- Định tuyến
- Loại mạng
  - LAN, WAN, Internets

An toàn Mạng

- Các mối đe dọa
  - Thăm dò
  - Nghe trộm
  - Mạo danh, lừa đảo
  - Từ chối dịch vụ
- Các biện pháp ngăn chặn
  - Mã hóa
  - Xác thực
  - Tường lửa
  - Phát hiện đột nhập

An toàn Mạng

- Các mối đe dọa
  - Thăm dò
  - Nghe trộm
  - Mạo danh, lừa đảo
  - Từ chối dịch vụ
- Các biện pháp ngăn chặn
  - Mã hóa
  - Xác thực
  - Tường lửa
  - Phát hiện đột nhập

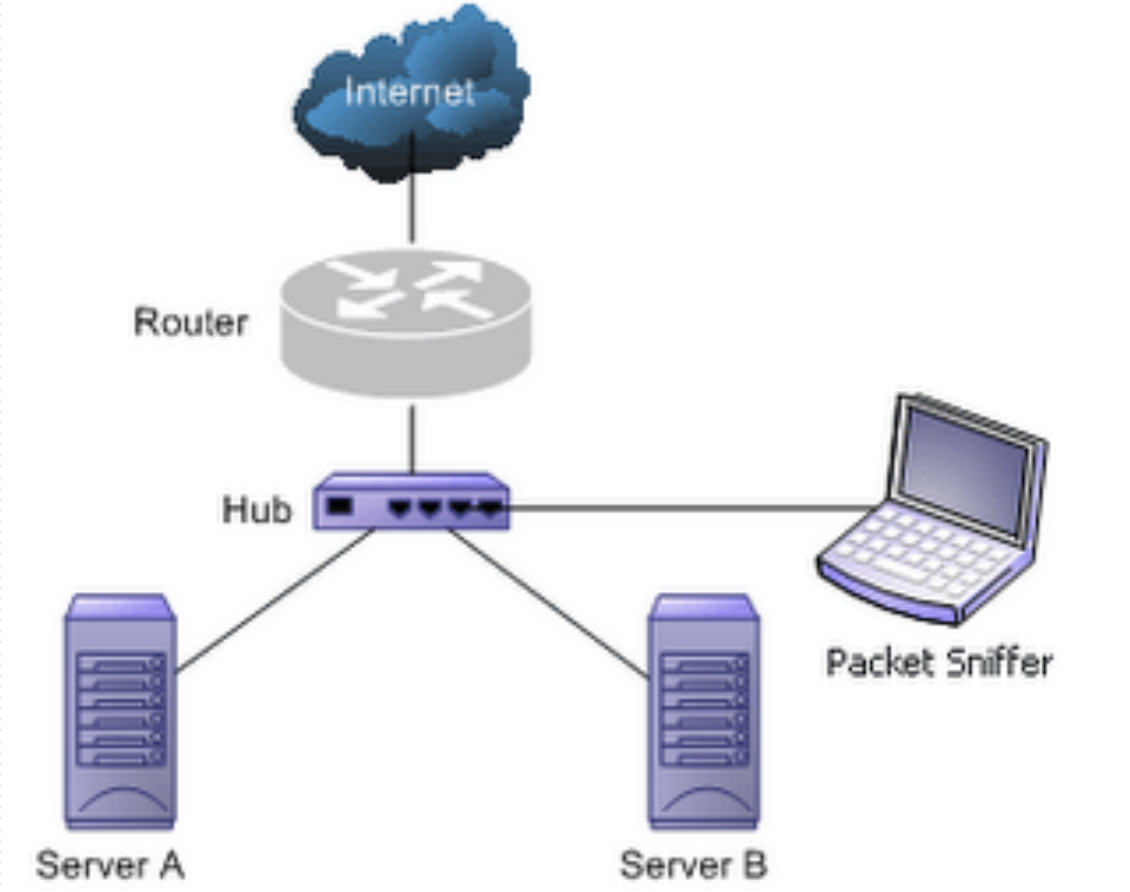
Thăm dò

- Quét cổng (Port Scan)
  - Thu thập thông tin đối tượng tấn công
    - dịch vụ, cổng đang hoạt động (HTTP:80, POP:110, SMTP:25, FTP:21)
    - phiên bản hệ điều hành
    - phiên bản ứng dụng
  - Tham khảo danh sách các lỗ hổng của các phiên bản
  - Thực hiện tấn công

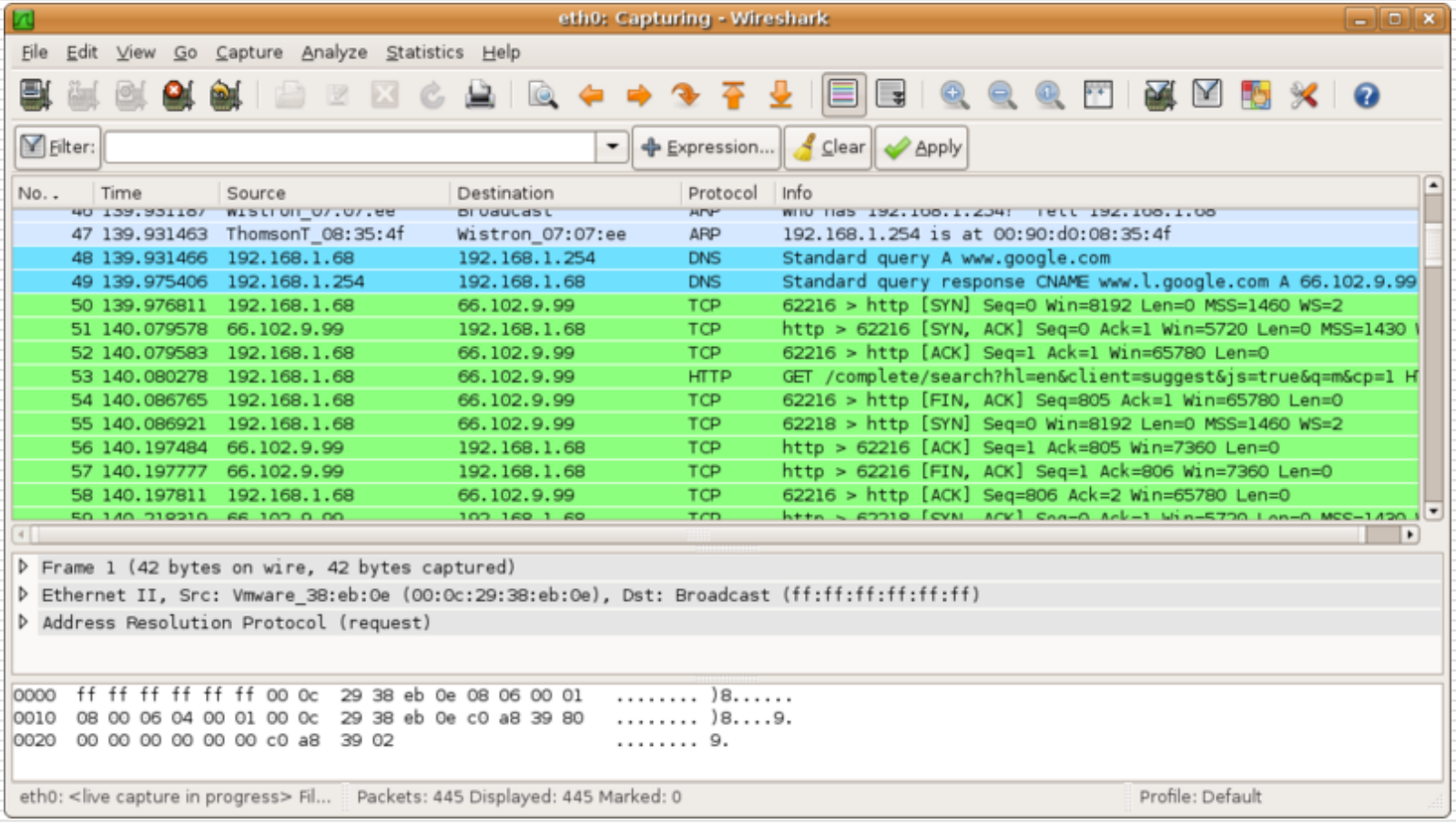
Nghe trộm

- Đường truyền cáp
  - Sử dụng “packet sniffer”
- Wireless
  - Tín hiệu rất dễ bị nghe trộm
    - Sử dụng ăng ten

Package sniffing



Wireshark


eth0: Capturing - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter:
Expression... Clear Apply
No. . Time Source Destination Protocol Info
47 139.931463 ThomsonT_08:35:4f Wistron_07:07:ee ARP 192.168.1.254 is at 00:90:d0:08:35:4f
48 139.931466 192.168.1.68 192.168.1.254 DNS Standard query A www.google.com
49 139.975406 192.168.1.254 192.168.1.68 DNS Standard query response CNAME www.l.google.com A 66.102.9.99
50 139.976811 192.168.1.68 66.102.9.99 TCP 62216 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=2
51 140.079578 66.102.9.99 192.168.1.68 TCP http > 62216 [SYN, ACK] Seq=0 Ack=1 Win=5720 Len=0 MSS=1430
52 140.079583 192.168.1.68 66.102.9.99 TCP 62216 > http [ACK] Seq=1 Ack=1 Win=65780 Len=0
53 140.080278 192.168.1.68 66.102.9.99 HTTP GET /complete/search?hl=en&client=suggest&js=true&q=m&cp=1 H
54 140.086765 192.168.1.68 66.102.9.99 TCP 62216 > http [FIN, ACK] Seq=805 Ack=1 Win=65780 Len=0
55 140.086921 192.168.1.68 66.102.9.99 TCP 62218 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=2
56 140.197484 66.102.9.99 192.168.1.68 TCP http > 62216 [ACK] Seq=1 Ack=805 Win=7360 Len=0
57 140.197777 66.102.9.99 192.168.1.68 TCP http > 62216 [FIN, ACK] Seq=1 Ack=806 Win=7360 Len=0
58 140.197811 192.168.1.68 66.102.9.99 TCP 62216 > http [ACK] Seq=806 Ack=2 Win=65780 Len=0
Frame 1 (42 bytes on wire, 42 bytes captured)
Ethernet II, Src: Vmware_38:eb:0e (00:0c:29:38:eb:0e), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Address Resolution Protocol (request)
0000 ff ff ff ff ff ff 00 0c 29 38 eb 0e 08 06 00 01 ....)8......
0010 08 00 06 04 00 01 00 0c 29 38 eb 0e c0 a8 39 80 ....)8....9.
0020 00 00 00 00 00 00 c0 a8 39 02 .... 9.
eth0: <live capture in progress> Fil... Packets: 445 Displayed: 445 Marked: 0 Profile: Default

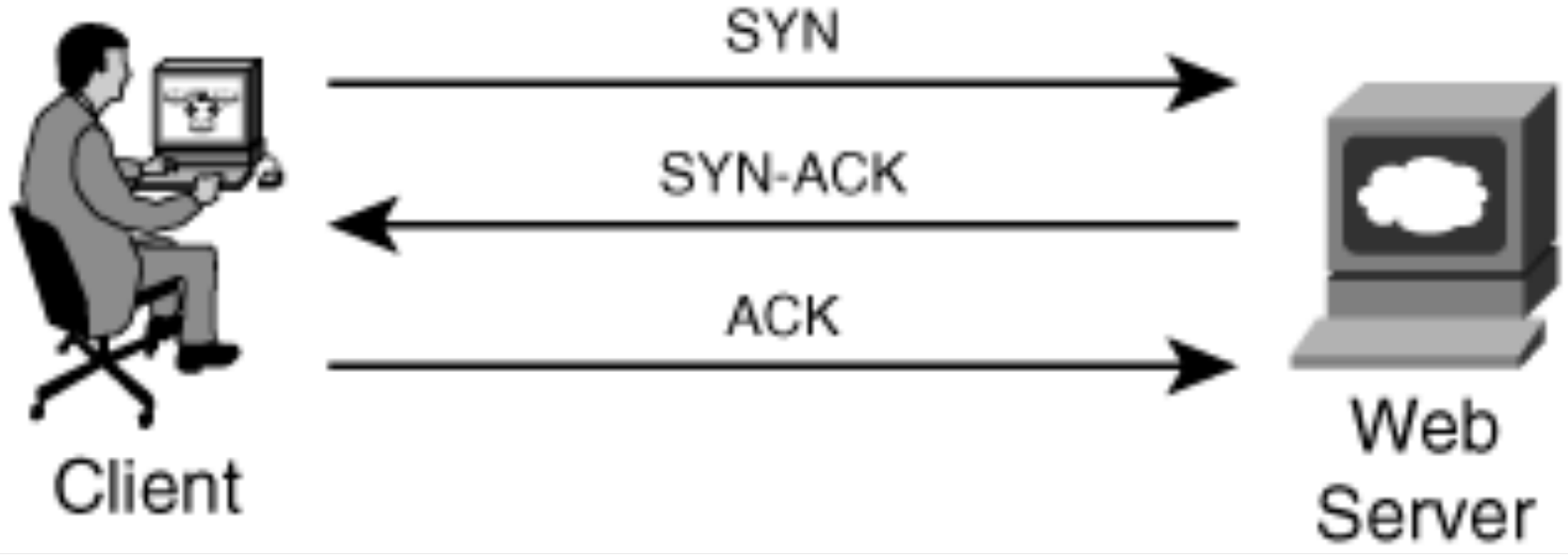
Mạo danh, lừa đảo

- 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
- Tận dụng lỗ hổng cơ chế xác thực
  - Tràn bộ đệm
- Thông tin xác thực công cộng
  - Thiết bị mạng quản lý bởi SNMP
- Man-in-the-middle
- Phishing

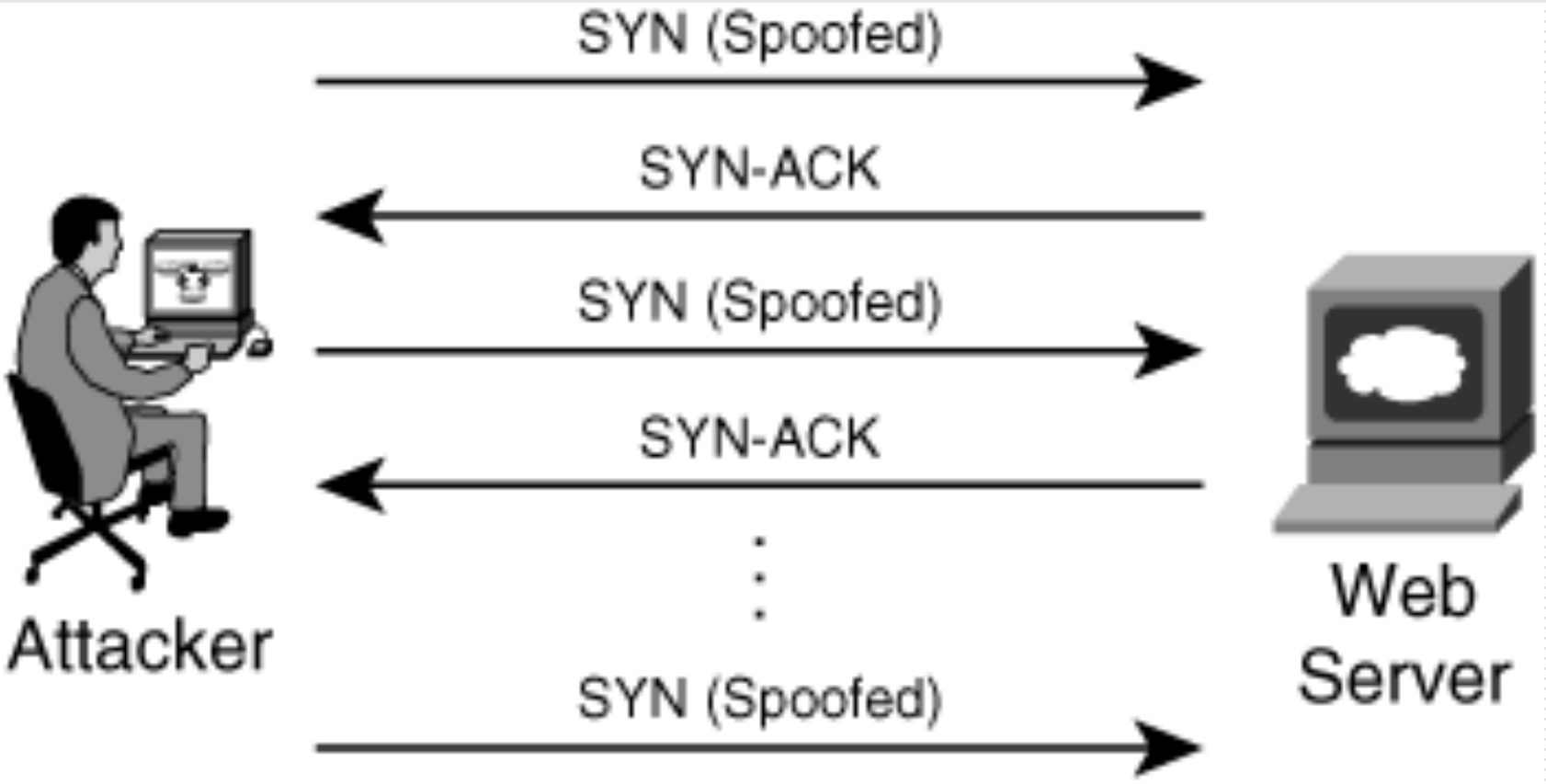
Từ chối dịch vụ

- Tràn kết nối (Connection Flooding)
  - Tấn công giao thức TCP, UDP, ICMP
    - Ping, Smurf, Syn Flood
- 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

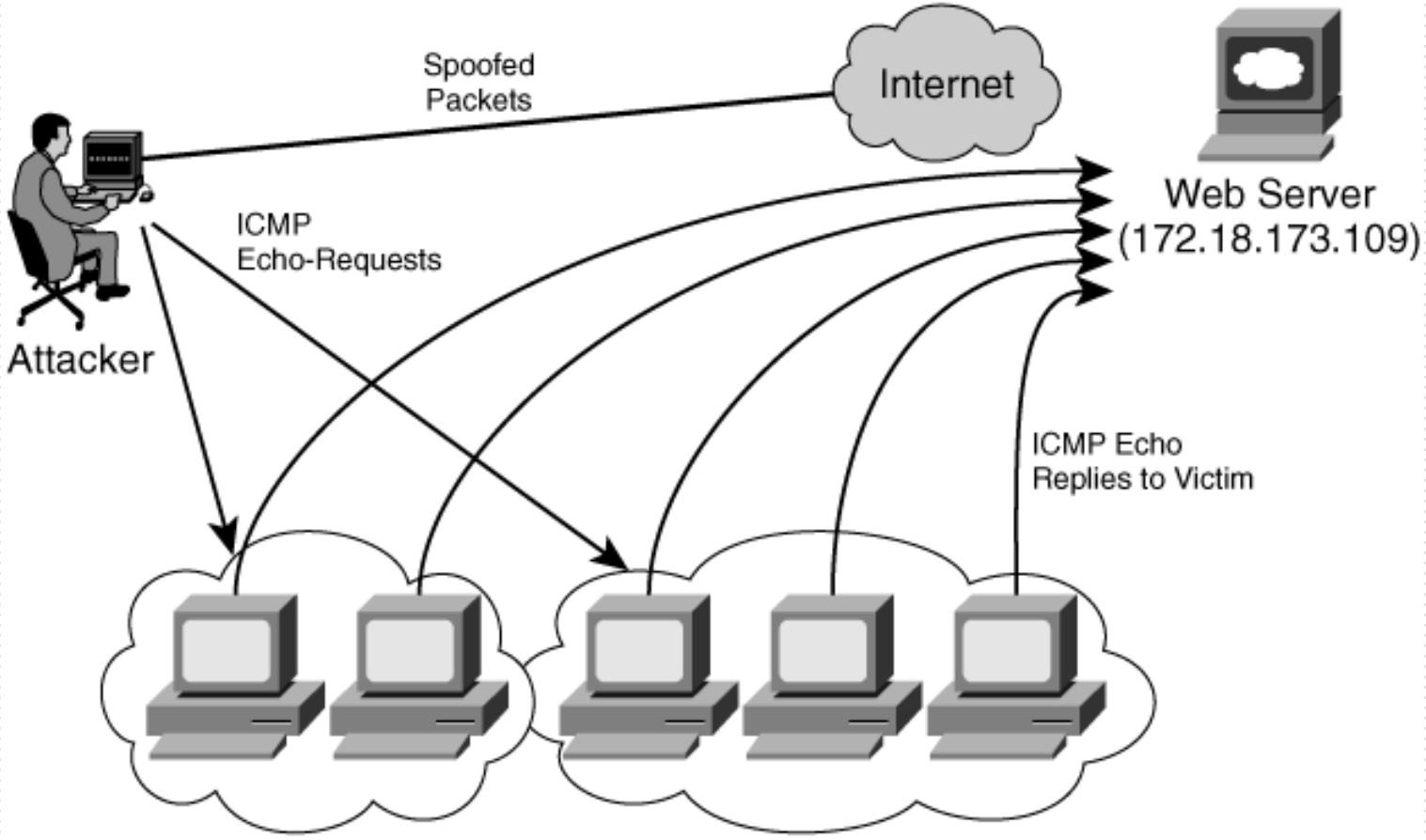
TCP handshake



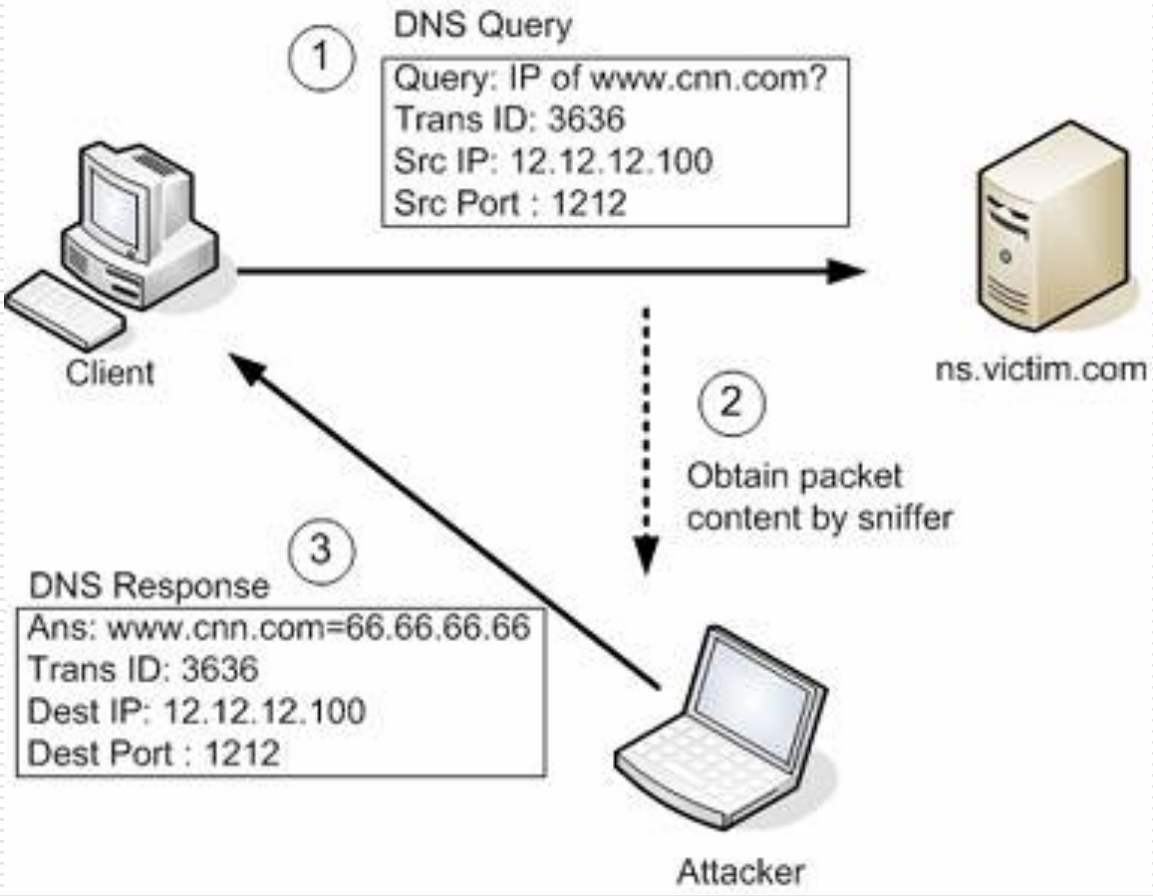
TCP SYN flooding



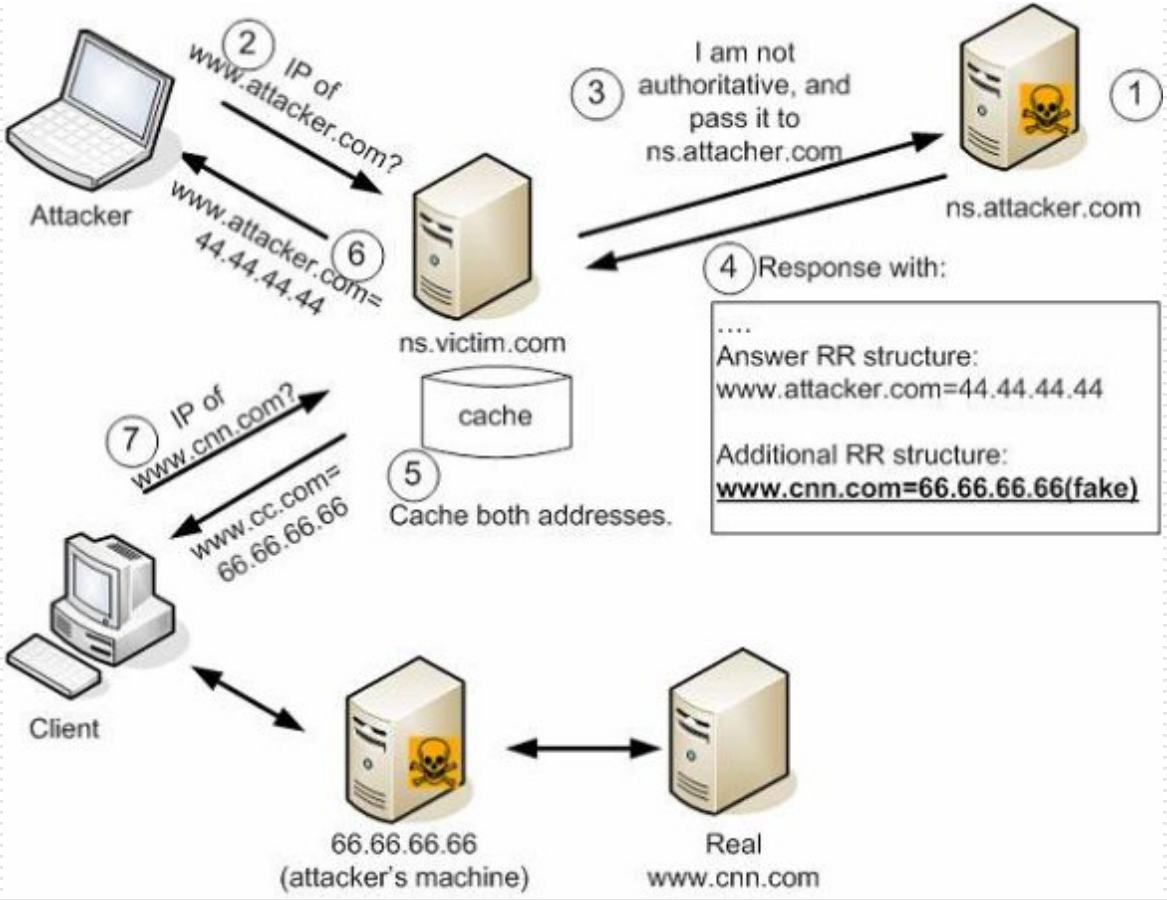
ICMP smurfing



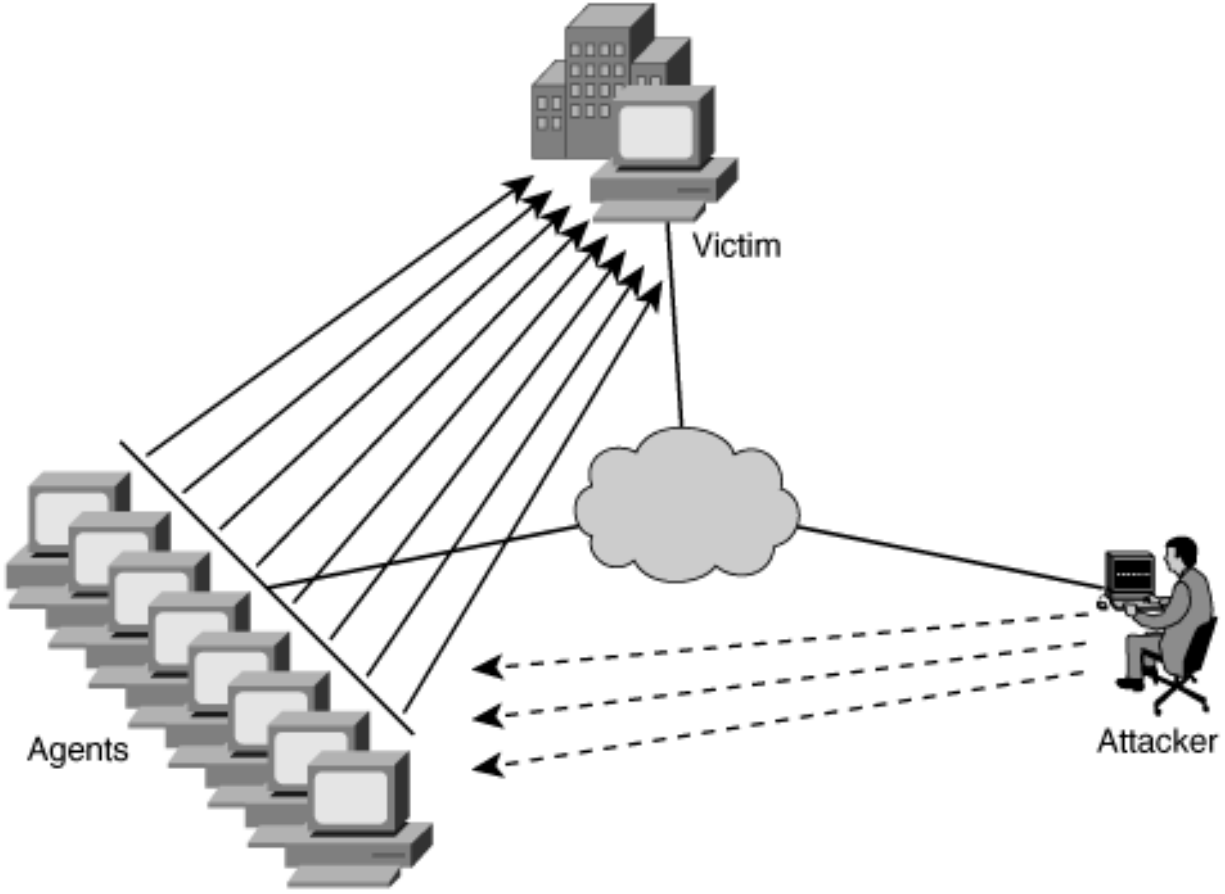
DNS cache poisoning



DNS cache poisoning



DDoS



An toàn Mạng

- Các mối đe dọa
  - Thăm dò
  - Nghe trộm
  - Mạo danh, lừa đảo
  - Từ chối dịch vụ
- Các biện pháp ngăn chặn
  - Mã hóa
  - Xác thực
  - Tường lửa
  - Phát hiện đột nhập

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)
  - Trao đổi thông tin giữa người dùng và Firewall thông qua kênh mã hóa
- PKI
  - Mật mã công khai và chứng nhận
- Giao thức mật mã
  - SSH, SSL, IPSec

Xác thực

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

Tường lửa

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

Tường lửa

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)

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

Phát hiện đột nhập

Các loại hệ thống phát hiện đột nhập

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