CHƯƠNG 2

LỖ HỔNG BẢO MẬT VÀ CÁC KỸ THUẬT TẤN CÔNG HỆ THỐNG MÁY TÍNH

Bộ môn: Tin học quản lý
Khoa Thống kê – Tin học
Đại học Kinh Tế - Đại học Đà Nẵng

NỘI DUNG CHƯƠNG 2

1. Khái quát về lỗ hổng bảo mật và kỹ thuật tấn công hệ thống máy tính
2. Một số kỹ thuật tấn công phổ biến

1. Khái quát về lỗ hổng bảo mật và kỹ thuật tấn công hệ thống máy tính

1.1. Khái quát về lỗ hổng bảo mật và điểm yếu của hệ thống thông tin

1.2. Các phương pháp tấn công hệ thống thông tin

1.3. Quy trình, kỹ thuật tấn công vào hệ thống thông tin

1.1. Khái quát về lỗ hổng bảo mật và điểm yếu của hệ thống thông tin

❑ Các thách thức về an ninh thông tin

- ❖ Sự phát triển của công nghệ tập trung vào giao diện thân thiện với người sử dụng
- ❖ Số lượng các ứng dụng trên mạng tăng rất nhanh
- ❖ Quản trị và quản lý hạ tầng thông tin ngày càng phức tạp
- ❖ Việc bảo mật cho một hệ thống máy tính lớn là rất khó
- ❖ Vi phạm an ninh tác động trực tiếp đến uy tín và tài sản của công ty
- ❖ Sự tuân thủ pháp luật và các quy định của chính phủ

1.1. Khái quát về lỗ hổng bảo mật và điểm yếu của hệ thống thông tin

❑ Các thách thức về an ninh thông tin

- ❖ Phần mềm độc hại (blackmarket, Trojan/keylogger,..)
- ❖ Lỗi thiết bị (lỗi khi copy dữ liệu với USB, thẻ nhớ,..)
- ❖ Lỗi ứng dụng (các lỗ hổng công nghệ mới, mạng xã hội, Công nghệ ảo hóa và điện toán đám mây)
- ❖ Thảm họa tự nhiên
- ❖ Hacker xâm nhập (đường link xấu, web ảo…)

1.1. Khái quát về lỗ hổng bảo mật và điểm yếu của hệ thống thông tin

❑ Ảnh hưởng của các cuộc tấn công

- ❖ Các cuộc tấn công hàng năm gây hại trung bình 2,2 triệu USD cho các công ty lớn (theo Symantec)
- ❖ Trộm cắp thông tin khách hàng/hack trang chủ làm giảm uy tín của công ty
- ❖ Tấn công DoS/DDoS và các cuộc tấn công khác làm gián đoạn thời gian hoạt động dịch vụ của doanh nghiệp, gây mất mát về doanh thu
- ❖ Các thông tin quan trong trong các hợp đồng bị ăn cắp, tiết lộ cho đối thủ cạnh tranh

1.1. Khái quát về lỗ hổng bảo mật và điểm yếu của hệ thống thông tin

❑ Các thành phần của hệ thống máy tính:

- **Hệ thống phần cứng**
  - CPU, ROM, RAM, Bus,...
  - Các giao diện ghép nối và các thiết bị ngoại vi.
- **Hệ thống phần mềm**
  - Hệ điều hành
    - Nhân hệ điều hành, các trình điều khiển thiết bị
    - Các trình cung cấp dịch vụ, tiện ích,…
  - Các phần mềm ứng dụng
    - Các dịch vụ (máy chủ web, CSDL, DNS,...)
    - Trình duyệt web, các ứng dụng giao tiếp,…
    - Các bộ ứng dụng văn phòng, lập trình

1.1. Khái quát về lỗ hổng bảo mật và điểm yếu của hệ thống thông tin

- **Các điểm yếu hệ thống (system weaknesses)** là các lỗi hay các khiếm khuyết (thiết kế, cài đặt, phần cứng hoặc phần mềm) tồn tại trong hệ thống.
  - Có điểm yếu đã biết và đã được khắc phục;
  - Có điểm yếu đã biết và chưa được khắc phục;
  - Có điểm yếu chưa biết/chưa được phát hiện.
- **Lỗ hổng bảo mật (Security vulnerability)** là một điểm yếu trong một hệ thống cho phép kẻ tấn công khai thác gây tổn hại đến các thuộc tính an ninh, an toàn của hệ thống đó:
  - Toàn vẹn (integrity)
  - Bí mật (confidentiality)
  - Sẵn dùng (availability)

1.1. Khái quát về lỗ hổng bảo mật và điểm yếu của hệ thống thông tin

❑ **Toàn vẹn (integrity):**

• Mọi sửa đổi đến thông tin/hệ thống chỉ được thực hiện bởi các bên có đủ thẩm quyền;

• Kẻ tấn công có thể lợi dụng điểm yếu an ninh để lặng lẽ sửa đổi thông tin/hệ thống →phá vỡ tính toàn vẹn;

• **Ví dụ:**

– Thông thường trong hệ thống kiểm soát truy nhập, chỉ người quản trị có quyền thay đổi quyền truy nhập đến mọi file;

– Một điểm yếu trong hệ thống có thể cho phép một người dùng bình thường thay đổi quyền truy nhập đến mọi file tương tự người quản trị

1.1. Khái quát về lỗ hổng bảo mật và điểm yếu của hệ thống thông tin

❑ **Bí mật (confidentiality):**

- Chỉ những người có thẩm được phép truy nhập đến thông tin/hệ thống;
- Kẻ tấn công có thể lợi dụng điểm yếu an ninh để truy nhập trái phép → phá vỡ tính bí mật;
- Ví dụ:

– Một điểm yếu an ninh cho phép người dùng web thông thường đọc được nội dung một file mà lẽ ra người đó không được quyền đọc;

– Một điểm yếu trong hệ thống kiểm soát truy nhập cho phép một nhân viên bình thường đọc được các báo cáo “mật” của công ty mà chỉ Ban Giám đốc được phép đọc.

1.1. Khái quát về lỗ hổng bảo mật và điểm yếu của hệ thống thông tin

❑ **Sẵn dùng (availability):**

- Đảm bảo khả năng truy nhập đến thông tin/hệ thống cho người dụng hợp pháp;
- Kẻ tấn công có thể lợi dụng điểm yếu an ninh để ngăn chặn hoặc gây khó khăn cho người dụng hợp pháp truy nhập vào thông tin/hệ thông;
- Ví dụ:

– Một điểm yếu an ninh có thể cho phép kẻ tấn công làm máy chủ ngừng hoạt động → không thể cung cấp dịch vụ cho người dùng hợp pháp → phá vỡ tính sẵn dùng;

– Kẻ tấn công cũng có thể gửi một lượng lớn yêu cầu giả mạo đến máy chủ gây cạn kiệt tài nguyên hoặc tắc ngẽn đường truyền → người dùng hợp pháp không thể truy cập → phá vỡ tính sẵn dùng.

1.1. Khái quát về lỗ hổng bảo mật và điểm yếu của hệ thống thông tin

❑ Mức độ nghiêm trọng của lỗ hổng bảo mật:

- 4 mức độ nghiêm trọng theo Microsoft:

– Nguy hiểm (Critical)

– Quan trọng (Important)

– Trung bình (Moderate)

– Thấp (Low).

- 3 mức độ nghiêm trọng theo một số tổ chức khác:

– Cao (High)

– Trung bình (Medium)

– Thấp (Low).

1.1. Khái quát về lỗ hổng bảo mật và điểm yếu của hệ thống thông tin

- **Các dạng lỗ hổng bảo mật thường gặp trong hệ điều hành và các phần mềm ứng dụng:**
  - Lỗi tràn bộ đệm (buffer overflows)
  - Không kiểm tra đầu vào (unvalidated input)
  - Các vấn đề với điều khiển truy cập (access-control problems)
  - Các điểm yếu trong xác thực, trao quyền hoặc các hệ mật mã (weaknesses in authentication, authorization, or cryptographic practices)
  - Các lỗ hổng bảo mật khác

1.2. Các phương pháp tấn công HTTT

1. Nhận dạng tội phạm
2. Các công cụ tấn công
3. Các tấn công gây hại
4. Phần mềm mã độc

1.2.1. Nhận dạng tội phạm

❑ Hồ sơ tội phạm số 1

❖ Gửi những tin qua email khẩn cầu giúp đỡ bằng cách quyên tiền tới nạn nhân

❖ Không dựa vào xâm nhập để thực hiện hành vị phạm tội

❖ Có động cơ là lợi ích kinh tế

1.2.1 Nhận dạng tội phạm

❑ Hồ sơ tội phạm số 2

- ❖ Tham gia các giao dịch chợ đen bất hợp pháp trên Internet
- ❖ Thuốc phiện, vũ khí, hàng cấm
- ❖ Có động cơ là lợi ích kinh tế

1.2.1 Nhận dạng tội phạm

❑ Hồ sơ tội phạm số 3

- ❖ Xâm nhập hệ thống trái phép và cảnh báo về tính an toàn bảo mật của hệ thống
- ❖ Không làm việc cho công ty hoặc các khách hàng của công ty
- ❖ Không định gây hại, chỉ tỏ ra là “có ích”
- ❖ Động cơ chỉ là bốc đồng

1.2.1 Nhận dạng tội phạm

- **Hồ sơ tội phạm số 4**
  - Xâm nhập hệ thống trái phép lợi dụng các vấn đề bảo mật
  - Không làm việc cho công ty hoặc các khách hàng của công ty
  - Không muốn giúp đỡ mà chỉ gây hại
  - Động cơ là do từ cộng đồng tội phạm này tham gia

1.2.1 Nhận dạng tội phạm

❑ Hồ sơ tội phạm số 5

- ❖ Xâm nhập hệ thống để kiểm tra, xác nhận vấn đề về an toàn bảo mật hệ thống
- ❖ Làm việc cho công ty hoặc các khách hàng của công ty
- ❖ Không định gây hại, là “có ích”

1.2.2 Các công cụ tấn công

- Vulnerability Scanner - Quét lỗ hổng
- Port Scaner - Quét cổng
- Sniffer - Nghe trộm
- Wardialer – phần mềm quét số điện thoại
- Keylogger – nghe trộm bàn phím

1.2.2 Các công cụ tấn công

❑ Một số công cụ rà quét lỗ hổng bảo mật

- ❖ Công cụ quét cổng dịch vụ:
  - Nmap
  - Angry IP Scanner
  - SuperScan
- ❖ Công cụ rà quét lỗ hổng bảo mật hệ thống
  - Microsoft Baseline Security Analyser
  - Nessus Vulnerability Scanner
- ❖ Công cụ rà quét lỗ hổng ứng dụng web
  - Acunetix Web Vulnerability Scanner
  - IBM AppScan
  - Beyond Security AVDS
  - SQLMap

1.2.2 Các công cụ tấn công

❑ Công cụ quét cổng dịch vụ

- ❖ Port scanning là quá trình gửi các gói tin tới cổng TCP và UDP trên hệ thống đích để xác định dịch vụ nào đang chạy hoặc trong tình trạng đang lắng nghe.
- ❖ Các cổng TCP/IP, UDP năm trong khoảng từ 0 – 65535
  - Các cổng 0-1024 là các cổng chuẩn
  - Cổng lớn hơn 1024 là các cổng tùy gán.
- ❖ Kẻ tấn công thường sử dụng công cụ quét cổng để nhận dạng các điểm yếu trong hệ thống;
  - Các công cụ: Netcat, Nmap, BackTrack: Autoscan, Umit, NmapFE, ...

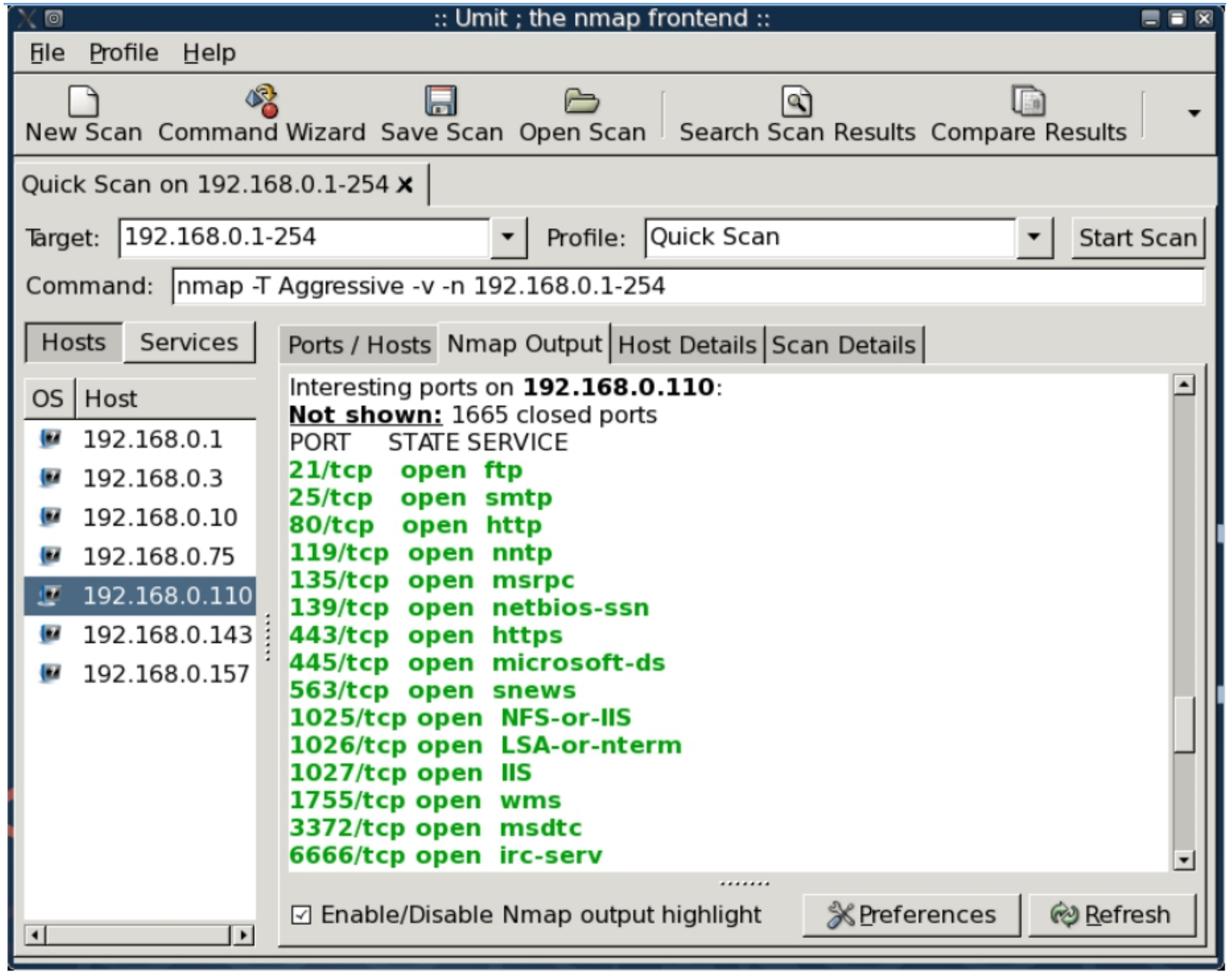
1.2.2 Các công cụ tấn công

❑ Công cụ quét cổng dịch vụ

❖ Công cụ quét cổng kết nối đến máy tính để xác định cổng nào được mở và có thể truy nhập vào máy tính. Từ đó xác định được dịch vụ/ứng dụng nào đang chạy trên hệ thống:

- Cổng 80/443 mở → dịch vụ web đang chạy
- Cổng 25 mở → dịch vụ email SMTP đang chạy
- Cổng 1433 mở → Máy chủ CSDL MS SQL Server đang chạy
- Cổng 53 mở → dịch vụ DNS đang chạy,...

1.2.2 Các công cụ tấn công



1.2.2 Các công cụ tấn công

❑ Công cụ nghe trộm

- Wireshark
- Ettercap
- Tcpdump
- Pcap / Wincap (packet capture)
- IP Tools (http://www.softpedia.com)

❑ Keylogger

❖ Phần mềm hoặc phần cứng

- Phần cứng yêu cầu truy cập
- Có thể truyền hoặc lưu trữ

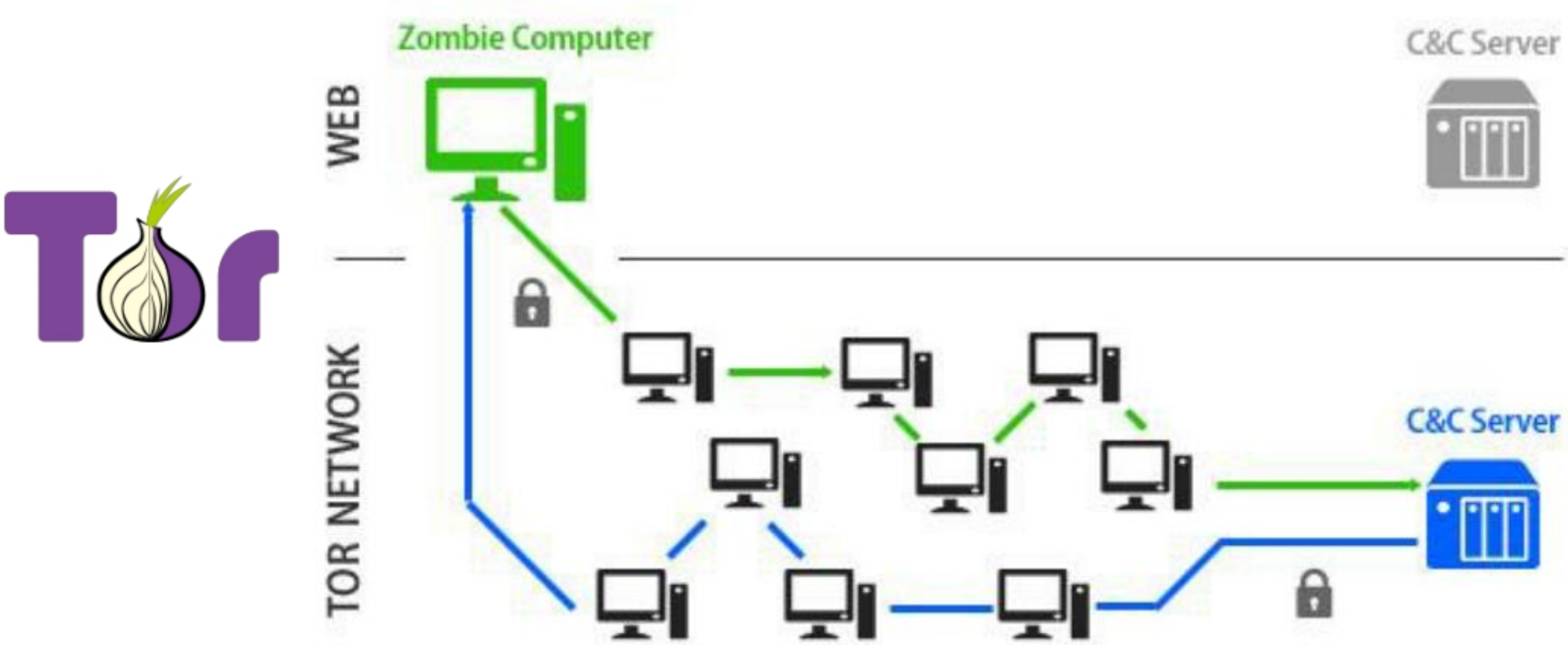
❖ Phần mềm có thể lưu và truyền đi

1.3 Quy trình, kỹ thuật tấn công vào HTTT

- ❖ Đảm bảo môi trường ẩn danh
  - Sử dụng các công cụ như Tor, VPN, Proxy chaining …
- ❖ Thực hiện tấn công theo từng giai đoạn

1.3 Quy trình, kỹ thuật tấn công vào HTTT

❑ Đảm bảo môi trường ẩn danh: Tor



1.3 Quy trình, kỹ thuật tấn công vào HTTT

❑ Đảm bảo môi trường ẩn danh: Tor

- ❖ Tor là viết tắt của “The Onion Router”, nó đề cập đến nhiều lớp mã hoá được sử dụng để bảo vệ sự riêng tư của người sử dụng.

- ❖ Chức năng cơ bản của Tor là giấu dấu vết của người sử dụng khi ở trên mạng, cho phép người sử dụng duyệt web và tải xuống một cách ẩn danh.

1.3 Quy trình, kỹ thuật tấn công vào HTTT

❑ Đảm bảo môi trường ẩn danh: Tor

❖ Ưu điểm của Tor:

- Trình duyệt Tor che giấu danh tính của người dùng bằng cách di chuyển hoạt động trên mạng của người dùng thông qua các máy chủ Tor khác nhau.
- Nó cho phép ẩn danh hoàn toàn và bảo mật khỏi những người muốn theo dõi hoạt động của người dùng, như các chính phủ, tin tặc và các nhà quảng cáo.
- Tor cũng là một cổng vào “Deep Web” hoặc “Dark Web”

1.3 Quy trình, kỹ thuật tấn công vào HTTT

❑ Đảm bảo môi trường ẩn danh: Tor

❖ Nhược điểm của Tor:

- Hạn chế lớn nhất của Tor là hiệu năng hoặc thiếu sót của nó.
- Bởi vì dữ liệu đi qua rất nhiều lớp, nên Tor xử lý rất chậm, đặc biệt là đối với các file âm thanh và video.
- Người dùng không thể không bị tấn công 100% khi sử dụng trình duyệt Tor.
- Các cơ quan của chính phủ có thể thấy người dùng đang sử dụng trình duyệt Tor

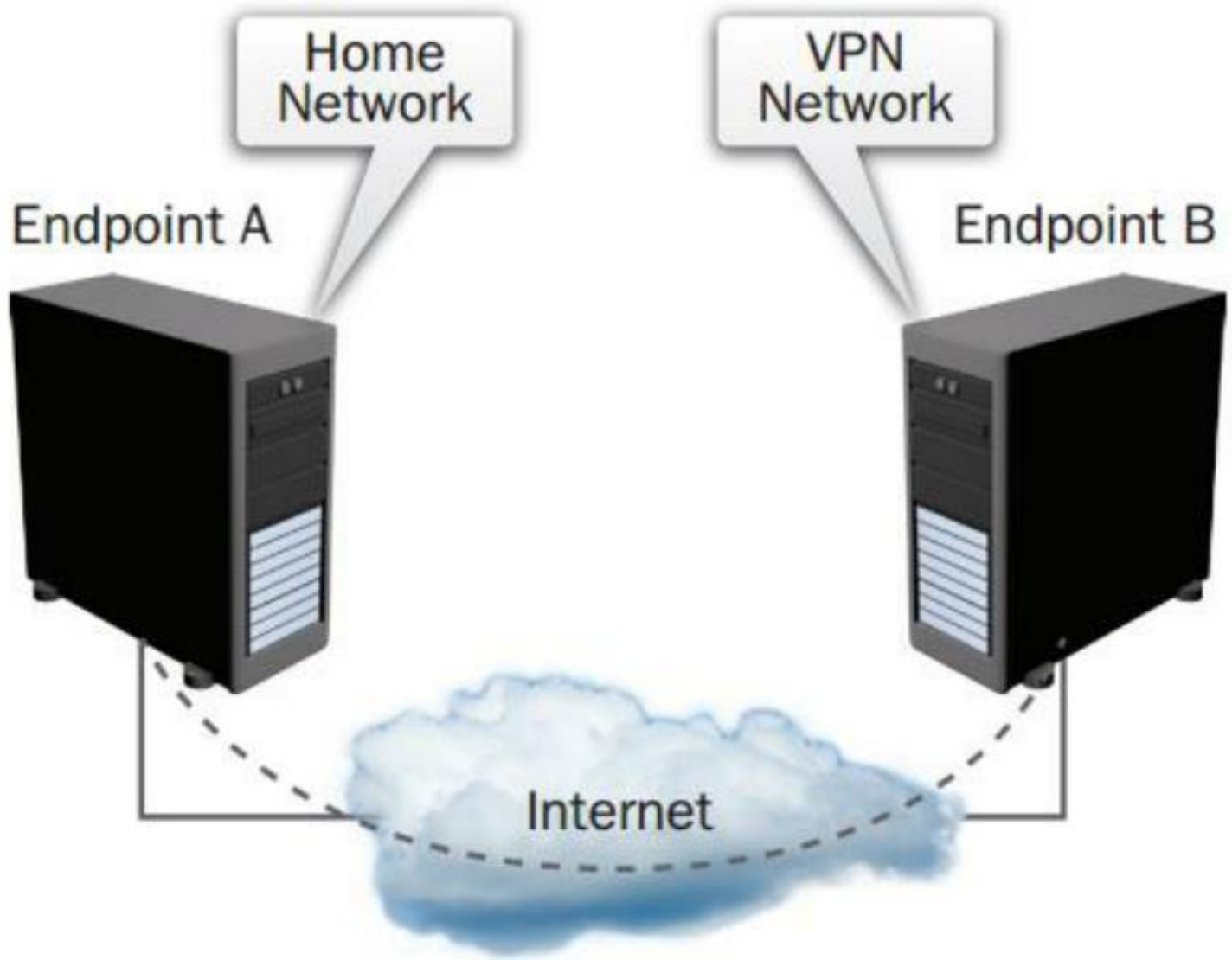
1.3 Quy trình, kỹ thuật tấn công vào HTTT

❑ Đảm bảo môi trường ẩn danh: VPN tunnel

- ❖ VPN là mạng riêng ảo, **Virtual Private Network**, là một công nghệ mạng giúp tạo kết nối mạng an toàn khi tham gia vào mạng công cộng như Internet hoặc mạng riêng do một nhà cung cấp dịch vụ sở hữu
- ❖ Muốn kết nối vào hệ thống VPN, thì mỗi 1 tài khoản đều phải được xác thực (phải có **Username** và **Password**). Những thông tin xác thực tài khoản này được dùng để cấp quyền truy cập thông qua 1 dữ liệu - **Personal Identification Number** (PIN), các mã PIN này thường chỉ có tác dụng trong 1 khoảng thời gian nhất định

1.3 Quy trình, kỹ thuật tấn công vào HTTT

❑ Đảm bảo môi trường ẩn danh: VPN tunnel



1.3 Quy trình, kỹ thuật tấn công vào HTTT

❑ Đảm bảo môi trường ẩn danh: VPN tunnel

❖ **VPN lại được ứng dụng để làm rất nhiều thứ:**

- Truy cập vào mạng doanh nghiệp khi ở xa
- Truy cập mạng gia đình, dù không ở nhà
- Duyệt web ẩn danh
- Truy cập đến những website bị chặn giới hạn địa lý, bỏ qua kiểm duyệt Internet, vượt tường lửa,...
- Tải tập tin

1.3 Quy trình, kỹ thuật tấn công vào HTTT

❑ Đảm bảo môi trường ẩn danh: VPN tunnel

Bản chất của giao thức VPN là một tập hợp các giao thức. Có một số chức năng mà mọi VPN phải giải quyết được:

- **Tunnelling** (kỹ thuật truyền dữ liệu qua nhiều mạng có giao thức khác nhau) - Chức năng cơ bản của VPN là phân phối các gói (packet) từ điểm này đến điểm khác mà không để lộ chúng cho bất kỳ ai trên đường truyền. Để làm điều này, VPN đóng gói tất cả dữ liệu theo định dạng mà cả máy khách và máy chủ đều hiểu được. Bên gửi dữ liệu đặt nó vào định dạng tunnelling và bên nhận trích xuất để có được thông tin.

1.3 Quy trình, kỹ thuật tấn công vào HTTT

❑ Đảm bảo môi trường ẩn danh: VPN tunnel

- **Mã hóa**: Tunnelling không cung cấp tính năng bảo vệ. Bất cứ ai cũng có thể trích xuất dữ liệu. Dữ liệu cũng cần phải được mã hóa trên đường truyền. Bên nhận sẽ biết cách giải mã dữ liệu từ một người gửi nhất định.
- **Xác thực**. Để bảo mật, VPN phải xác nhận danh tính của bất kỳ client nào cố gắng "giao tiếp" với nó. Client cần xác nhận rằng nó đã đến đúng máy chủ dự định.
- **Quản lý phiên**: Một khi người dùng được xác thực, VPN cần duy trì phiên để client có thể tiếp tục "giao tiếp" với nó trong một khoảng thời gian.

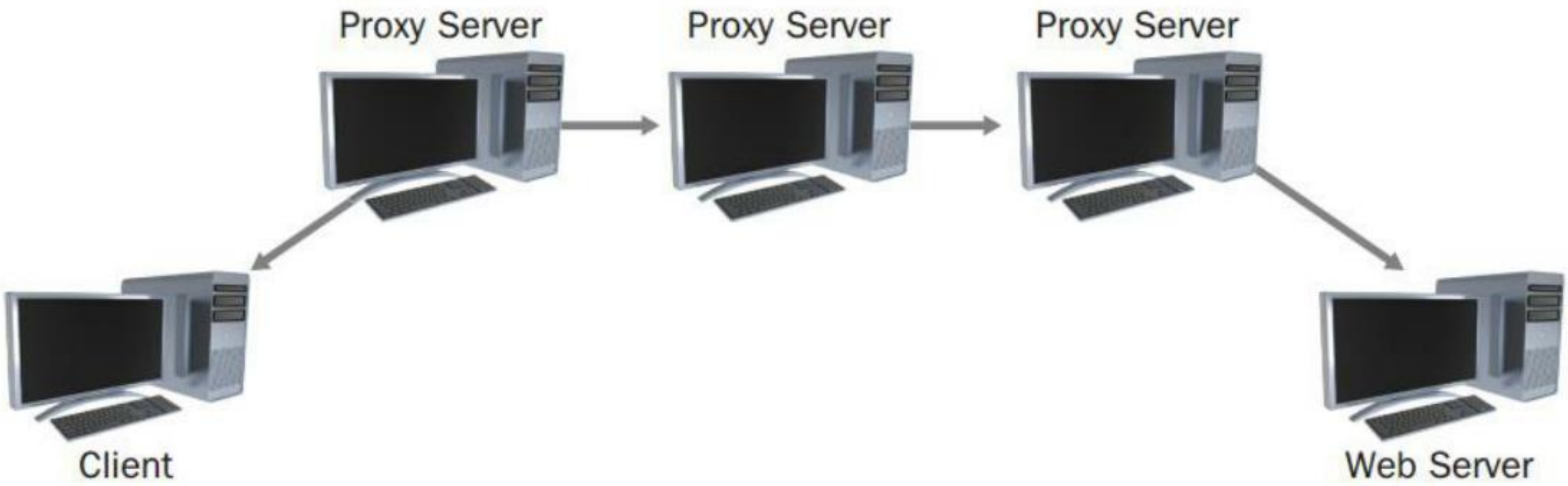
1.3 Quy trình, kỹ thuật tấn công vào HTTT

❑ Đảm bảo môi trường ẩn danh: Proxy chaining

- ❖ Một proxy ẩn danh được thiết kế để tăng sự riêng tư của người dùng trên web bằng cách giấu địa chỉ IP công cộng do nhà cung cấp dịch vụ Internet cung cấp và định tuyến tất cả lưu lượng truy cập thông qua các máy chủ và địa chỉ công cộng khác nhau.
- ❖ Những máy chủ proxy này có thể giúp người dùng tránh khóa nội dung mà một số trang web đặt trên địa chỉ IP từ một số quốc gia nhất định. Khi trang web cho rằng yêu cầu đến từ một quốc gia được hỗ trợ, nó sẽ không chặn. Ví dụ: nếu trang web muốn sử dụng chỉ hoạt động cho người Canada, bạn có thể sử dụng máy chủ proxy của Canada để tải trang

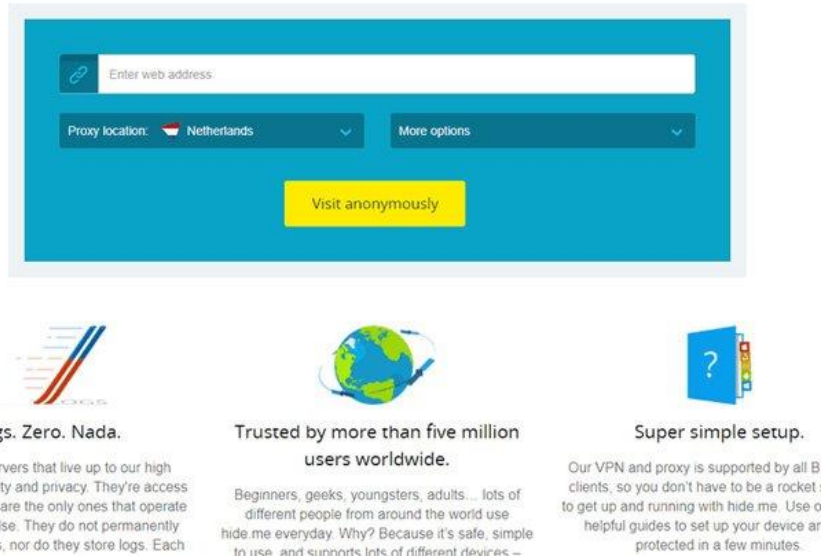
1.3 Quy trình, kỹ thuật tấn công vào HTTT

❑ Đảm bảo môi trường ẩn danh: Proxy chaining



1.3 Quy trình, kỹ thuật tấn công vào HTTT

❑ Đảm bảo môi trường ẩn danh: Proxy chaining



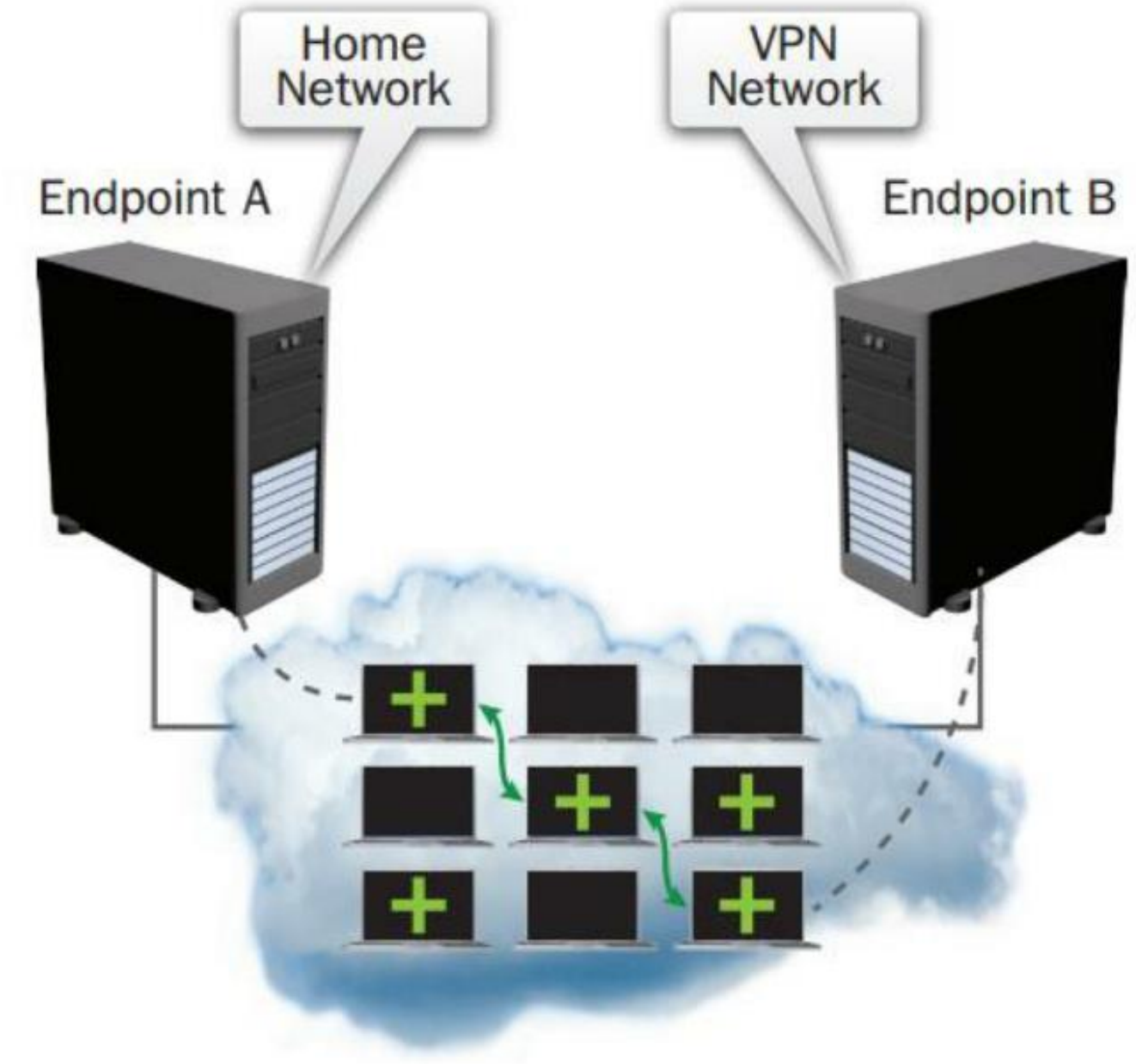
1.3 Quy trình, kỹ thuật tấn công vào HTTT

❑ Đảm bảo môi trường ẩn danh: Tor to VPN

- Truy cập **Tor thông qua VPN** được thực hiện thông qua quy trình: **máy tính của người dùng → VPN→ Tor→ Internet.**
- Lợi ích của việc này là **nhà cung cấp dịch vụ mạng của người dùng sẽ không biết rằng người dùng đang sử dụng trình duyệt Tor,** mặc dù họ vẫn có thể biết rằng người dùng đang sử dụng VPN. Ngoài ra, **nút mạng truy cập của trình duyệt Tor sẽ không thấy được địa chỉ IP của người dùng, đây là lớp bảo mật được thêm vào.**
- Nhược điểm của thiết lập này là **VPN của người dùng sẽ biết địa chỉ IP thật của người dùng** và người dùng sẽ không được bảo vệ khỏi các nút mạng thoát độc hại của trình duyệt Tor.

1.3 Quy trình, kỹ thuật tấn công vào HTTT

❑ Đảm bảo môi trường ẩn danh: Tor to VPN



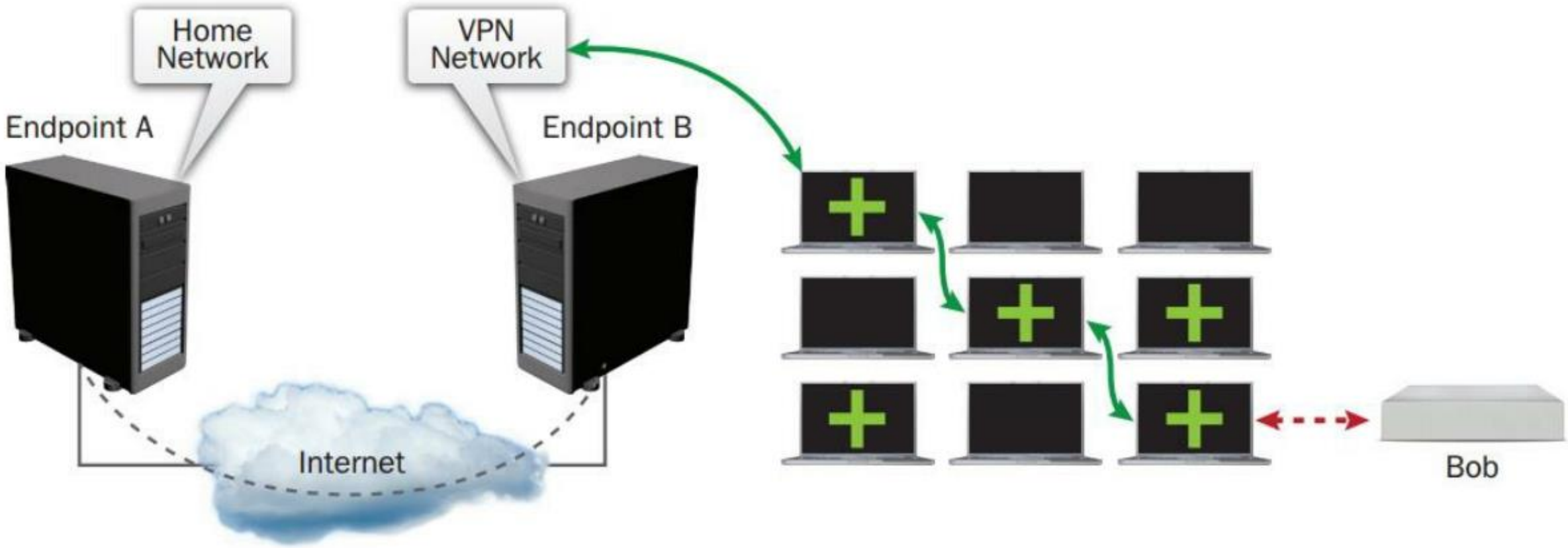
1.3 Quy trình, kỹ thuật tấn công vào HTTT

❑ Đảm bảo môi trường ẩn danh: VPN to Tor

- ❖ **Truy cập VPN thông qua Tor** được thực hiện thông qua quy trình: **máy tính của người dùng→ Tor→ VPN→ Internet.**
- ❖ **Truy cập VPN thông qua Tor an toàn hơn một cách đáng kể, cho phép người dùng ẩn danh gần như hoàn toàn.**
- ❖ Điều đó cho thấy rằng, nó đòi hỏi người dùng phải cấu hình VPN để làm việc với trình duyệt TOR
- ❖ 2 dịch vụ mà cho phép người dùng thực hiện nó: AirVPN và BolehVPN.

1.3 Quy trình, kỹ thuật tấn công vào HTTT

❑ Đảm bảo môi trường ẩn danh: VPN to Tor



1.3 Quy trình, kỹ thuật tấn công vào HTTT

❑ Các giai đoạn tấn công một hệ thống thông tin

- ❖ Trinh sát
- ❖ Dò quét hệ thống
- ❖ Truy cập hệ thống
- ❖ Duy trì truy cập
- ❖ Xóa dấu vết

1.3 Quy trình, kỹ thuật tấn công vào HTTT

❑ Giai đoạn 1: Trinh sát

- ❖ Kẻ tấn công tìm kiếm, thu thập các thông tin về mục tiêu cần tấn công
- ❖ Bao gồm cả các hoạt động của công ty, khách hàng, các nhân viên, hệ thống thông tin …
- ❖ Gồm 2 loại:
  - Trinh sát thụ động: thu thập thông tin mà không cần tiếp xúc với mục tiêu
  - Trinh sát chủ động: hoạt động tương tác với mục tiêu. Ví dụ: gọi điện thoại

1.3 Quy trình, kỹ thuật tấn công vào HTTT

❑ Giai đoạn 2: Dò quét hệ thống

- ❖ Dựa trên thông tin đã thu thập trong giai đoạn trước đó, kẻ tấn công tiến hành dò quét mạng của hệ thống thông tin
- ❖ Việc dò quét bao gồm quét các cổng, quét số điện thoại, lập bản đồ mạng, quét các lỗ hổng, …
- ❖ Khai thác các thông tin như tên máy tính, địa chỉ IP, và các tài khoản người dùng sẽ tấn công

1.3 Quy trình, kỹ thuật tấn công vào HTTT

❑ Giai đoạn 3: Truy cập

- ❖ Kẻ tấn công truy cập vào hệ điều hành hay phần mềm qua các lỗ hổng an ninh
- ❖ Kẻ tấn công có thể truy cập ở mức hệ điều hành, mức ứng dụng hay mức mạng
- ❖ Tiến hành nâng quyền hệ thống và tiến tới kiểm soát toàn bộ hệ thống
- ❖ Ví dụ: tấn công bẻ mật khẩu, tràn bộ đệm hoặc đánh cắp tài khoản nhờ cài Trojan

1.3 Quy trình, kỹ thuật tấn công vào HTTT

❑ Giai đoạn 4: Duy trì truy cập

- ❖ Kẻ tấn công sau khi có quyền truy cập hệ thống muốn duy trì quyền kiểm soát hệ thống
- ❖ Sử dụng các công cụ như backdoor, rootkit hoặc Trojan
- ❖ Khai thác dữ liệu trên hệ thống đã kiểm soát
- ❖ Sử dụng các hệ thống đã kiểm soát để làm bàn đạp tấn công các hệ thống khác

1.3 Quy trình, kỹ thuật tấn công vào HTTT

❑ Giai đoạn 5: Xóa dấu vết

- ❖ Kẻ tấn công thực hiện che dấu hành vi tấn công của mình
- ❖ Việc xóa dấu vết nhằm xóa các bằng chứng liên quan tới bản thân để bị phát hiện hay chú ý, từ đó có thể tiếp tục truy cập vào hệ thống đã kiểm soát
- ❖ Xóa dấu vết bằng cách:
  - Xóa các bản ghi log trên hệ thống, trong các ứng dụng
  - Ẩn dấu các phần mềm độc hại dùng để duy trì truy cập

CHƯƠNG 2 (TT)

LỖ HỔNG BẢO MẬT VÀ CÁC KỸ THUẬT TẤN CÔNG HỆ THỐNG MÁY TÍNH

Bộ môn: Tin học quản lý
Khoa Thống kê – Tin học
Đại học Kinh Tế - Đại học Đà Nẵng

2. Một số kỹ thuật tấn công phổ biến

1. Tấn công mật khẩu
2. Tấn công Spoofing
3. Tấn công Packet Sniffing
4. Tấn công MitM (Man-in-the-Middle)
5. Tấn công Chiếm quyền điều khiển phiên (Session Hijacking)
6. Tấn công từ chối dịch vụ
7. Tấn công lặp lại (Replay)
8. Tấn công DNS
9. Tấn công Social Engineering

2.1 Tấn công mật khẩu

❑ Tấn công mật khẩu

❖ Tấn công vào mật khẩu là kiểu tấn công cổ điển chiếm quyền truy cập máy tính nạn nhân, bằng cách tìm ra mật khẩu và đăng nhập.

❖ Có nhiều kiểu tấn công:

- Vét cạn
- Sử dụng từ điển
- Nghe trộm

2.1 Tấn công mật khẩu

❑ Kiểu tấn công – Vét cạn mật khẩu (Brute force attacks)

❖ Sử dụng tổ hợp các ký tự và thử tự động.

• Phương pháp này thường sử dụng với các mật khẩu đã được mã hóa;

• Kẻ tấn công sử dụng tổ hợp ký tự, sau đó mã hóa với cùng thuật toán hệ thống sử dụng, và so sánh chuỗi mã hóa với chuỗi mà mật khẩu thu thập được. Nếu hai bản mã trùng nhau → tổ hợp ký tự là mật khẩu.

2.1 Tấn công mật khẩu

❑ Kiểu tấn công – Từ điển

- ❖ Kẻ tấn công sẽ sử dụng file từ điển có sẵn chứa các hash để so sánh với hash của password để tìm ra dạng plaint text của password nếu hash trùng nhau.
- ❖ Chúng ta có thể thêm hoặc đảo các từ có trong từ điển (Hybird Attacks).
- ❖ Dạng này ứng dụng tốt khi password là những ký tự thông thường, tốc độ nhanh, mức độ thành công tùy thuộc vào từ điển.

2.1 Tấn công mật khẩu

❑ Các kiểu tấn công – Kết hợp

❖ Kết hợp hai cách trên bằng cách tạo sẵn các bản hash của tất cả tổ hợp các ký tự và chỉ so sánh trong quá trình hash.

❖ Tốc độ crack chỉ mất vài phút nếu có sẵn các bản hash

2.1 Tấn công mật khẩu

❑ Phòng chống

❖ Chọn mật khẩu đủ mạnh: độ dài >= 8 ký tự gồm chữ cái hoa, thường, chữ số và ký tự đặc biệt (?#$...).

- VD: Mật khẩu ‘Abc123$5’ an toàn hơn ‘abc12345’ về mặt tính toán
- Định kỳ thay đổi mật khẩu.

❑ Một số công cụ khôi phục mật khẩu:

- Password Cracker (http://www.softpedia.com)
- Ophcrack
- Offline NT Password & Registry Editor
- PC Login Now
- L0phtCrack
- John the Ripper

2.2 Tấn công giả mạo

- **Tấn công giả mạo** (Spoofing) là tình huống một người/một chương trình giả mạo thành công là một người khác/một chương trình khác bằng cách làm sai lệch dữ liệu và do đó đạt được một lợi thế không chính đáng.

- Có nhiều loại *tấn công giả mạo* như:
  - Giả mạo IP
  - Giả mạo MAC
  - Giả mạo URL
  - Giả mạo ARP
  - Giả mạo DNS
  - Giả mạo địa chỉ Email

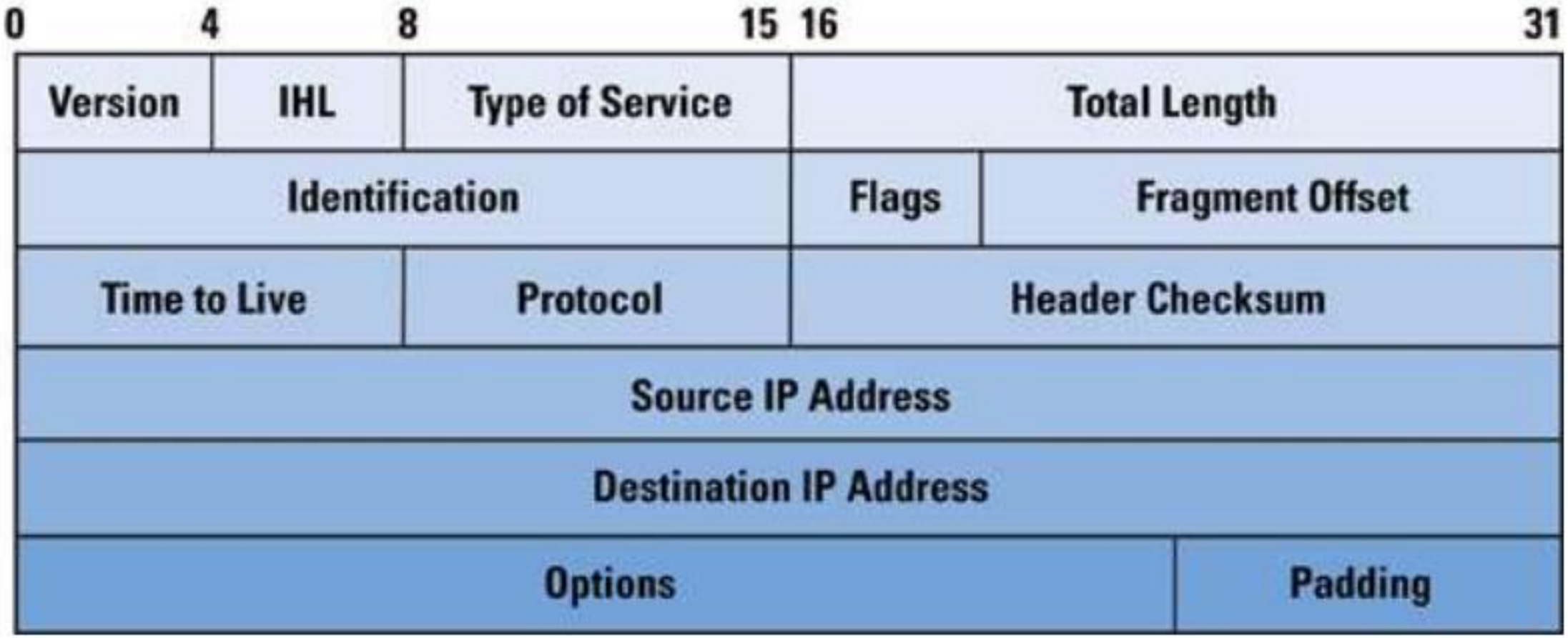
2.2 Tấn công giả mạo

❑ Giả mạo địa chỉ IP (IP Spoofing)

- ❖ Là dạng tấn công trong đó kẻ tấn công sử dụng địa chỉ IP giả, thường để đánh lừa máy nạn nhân để vượt qua các hàng rào kiểm soát an ninh;
- ❖ Nếu kẻ tấn công giả địa chỉ IP là địa chỉ cục bộ của mạng LAN, hắn có thể có nhiều cơ hội đột nhập vào các máy khác trong LAN do chính sách kiểm soát an ninh với các máy trong mạng LAN thường được giảm nhẹ.
- ❖ Nếu router hoặc firewall của mạng không được cấu hình để nhận ra IP giả mạo của mạng LAN nội bộ → kẻ tấn công có thể thực hiện.

2.2 Tấn công giả mạo

❑ Giả mạo địa chỉ IP (IP Spoofing)



Định dạng gói tin IPv4

2.2 Tấn công giả mạo

❑ Giả mạo địa chỉ IP

A

10.10.10.1

http://www.abc.com

www.abc.com

124.111.1.10

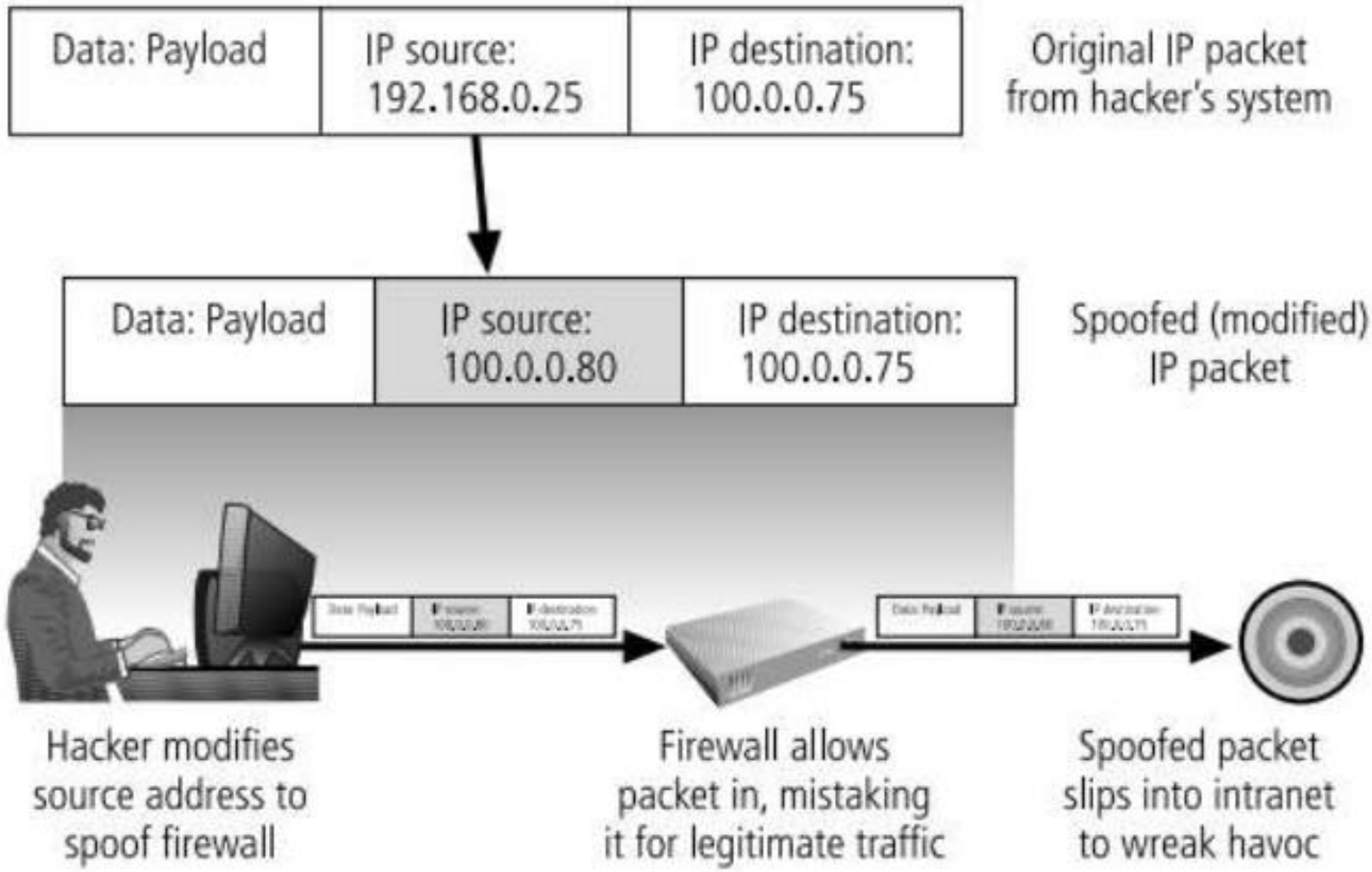
10.10.10.1	124.111.1.10	Any (>1024)	80
Src_IP	dst_IP	Src_port	dst_port

Giả mạo

11.11.11.1	134.117.1.60	Any (>1024)	80
Src_IP	dst_IP	Src_port	dst_port

2.2 Tấn công giả mạo

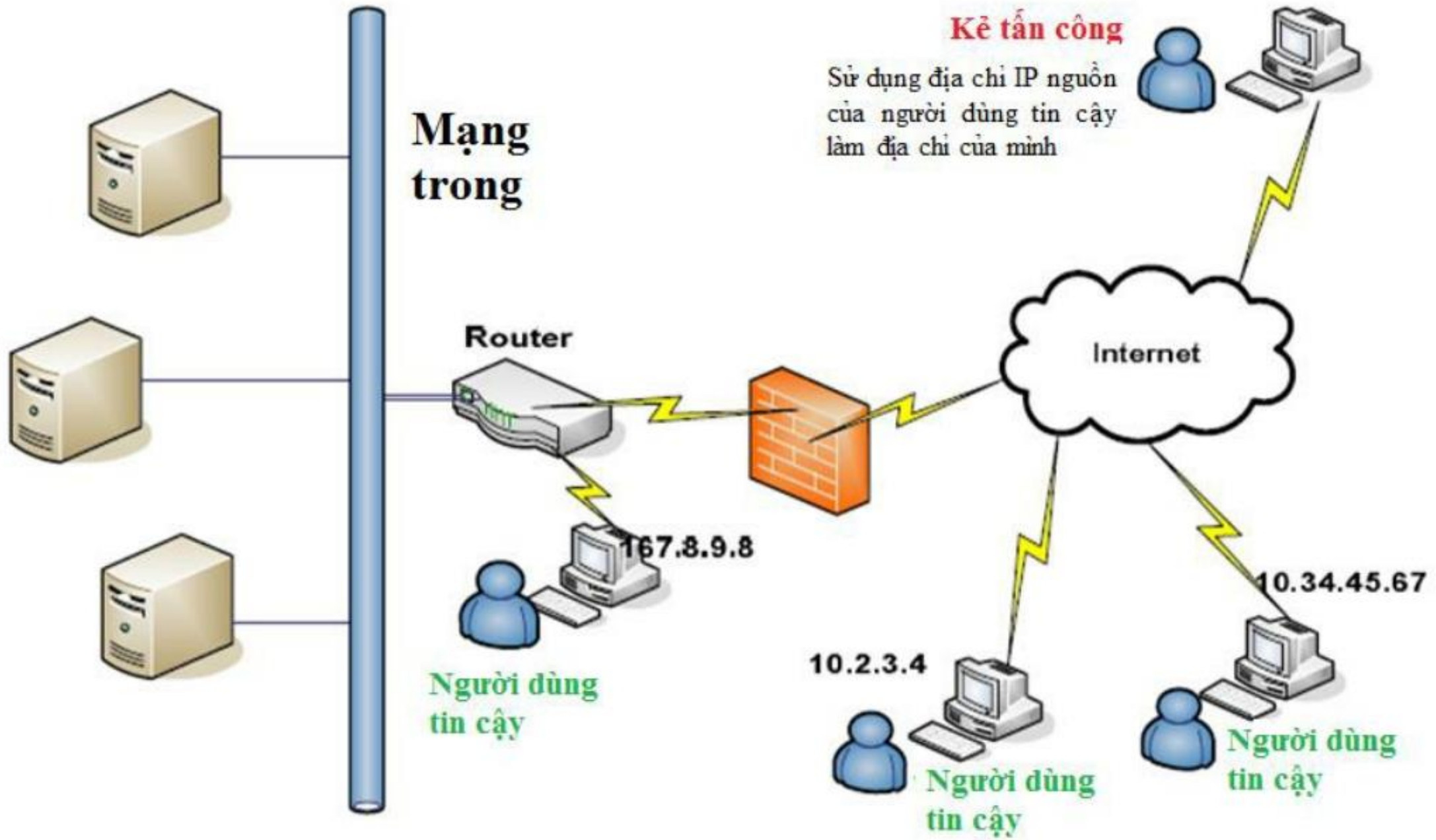
❑ Giả mạo địa chỉ IP



Tấn công giả mạo địa chỉ IP

2.2 Tấn công giả mạo

❑ Giả mạo địa chỉ IP



2.2 Tấn công giả mạo

❑ **Giả mạo địa chỉ IP**

→ **Câu hỏi:** Tại sao dễ dàng thực hiện tấn công giả mạo IP?

→ **Trả lời: Là do**

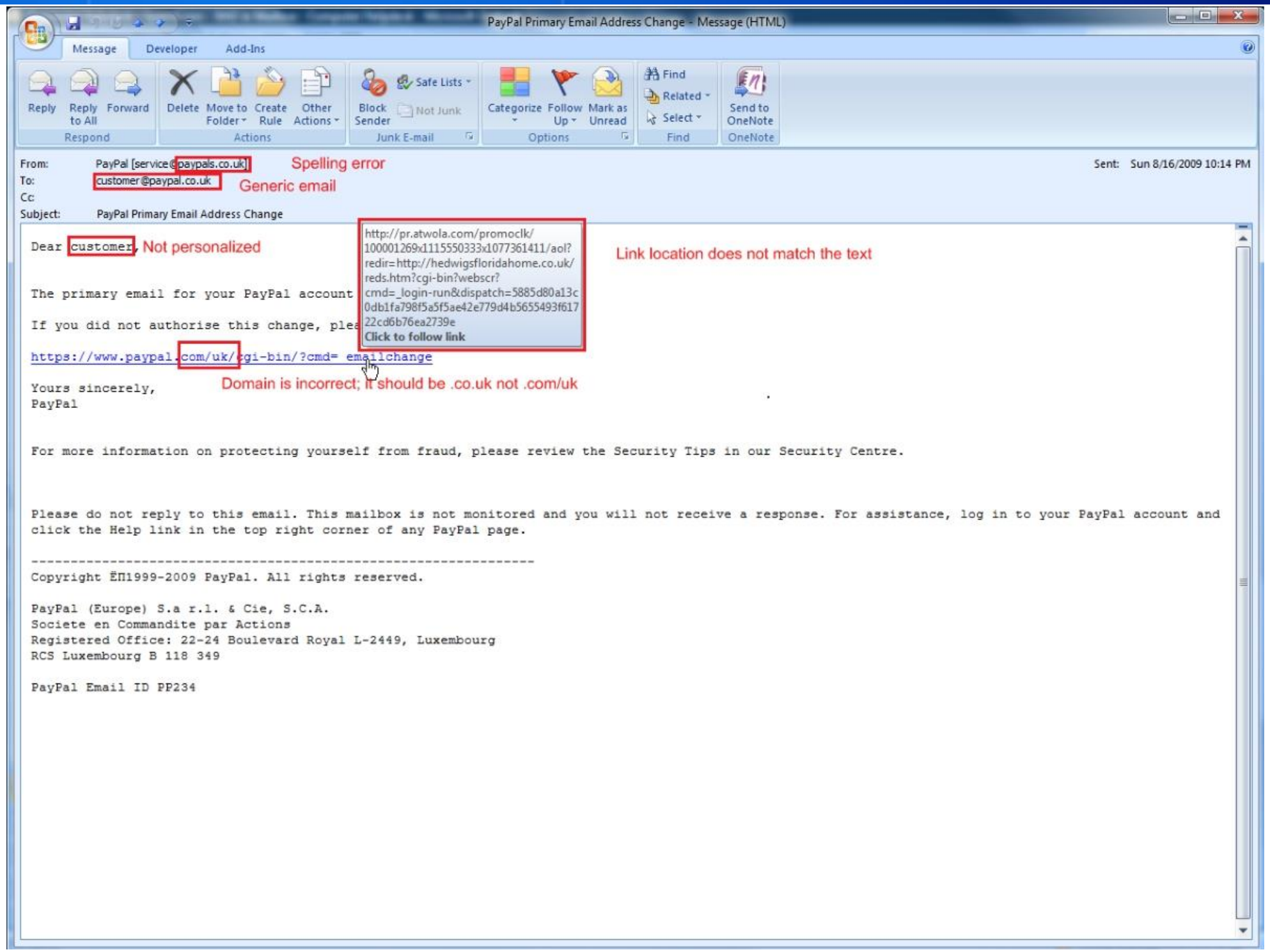
- Các lỗi trong cấu hình router
- Router chỉ quan tâm các địa chỉ đích
- Việc xác thực chỉ dựa trên các địa chỉ nguồn
- Thay đổi các trường trong gói tin IP rất dễ dàng

2.2 Tấn công giả mạo

❑ Giả mạo địa chỉ MAC

- ❖ Kẻ tấn công nghe lén địa chỉ MAC của máy trạm hợp pháp trong mạng, sau đó dùng địa chỉ MAC đó để truy cập mạng.
- ❖ Bằng cách dùng địa chỉ MAC ăn cắp được của nạn nhân, kẻ tấn công có thể nhận được tất cả các lưu lượng đi từ máy nạn nhân tới đích.
- ❖ Nếu địa chỉ MAC được quyền thực thi trong mạng, kẻ tấn công có thể có quyền thực thi trong mạng đó.
- ❖ Kẻ tấn công có thể tiến hành nhận dạng một ai đó trên mạng
- ❖ Công cụ giả mạo MAC trên MS Windows: SMAC 2.0

2.2 Tấn công giả mạo



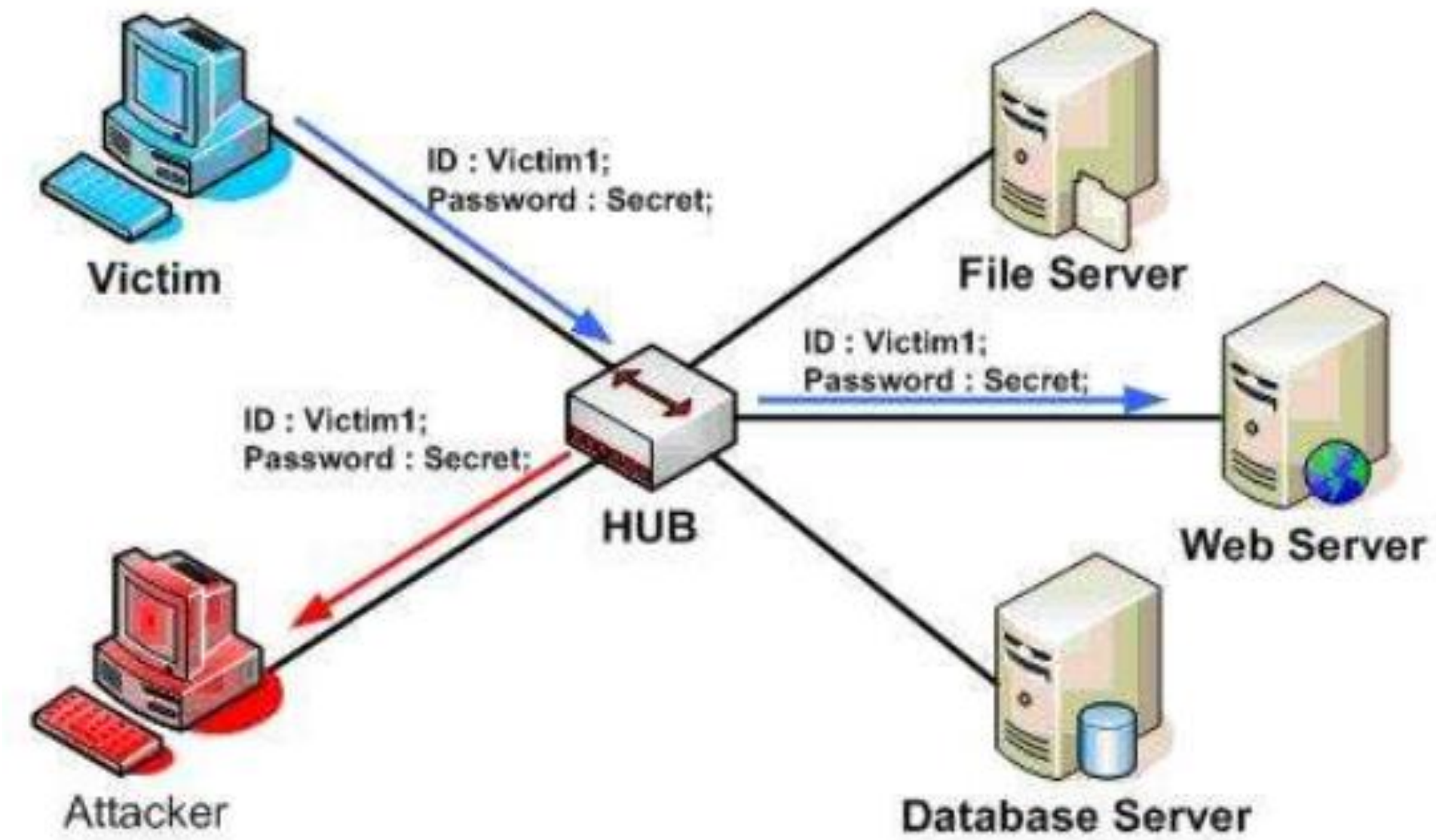
2.3 Tấn công Packet Sniffing

❑ Công cụ Sniffer

- ❖ Sniffer là công cụ (phần cứng hoặc phần mềm) "bắt" các thông tin lưu chuyển trên mạng.
- ❖ Có thể bắt được các thông tin trao đổi giữa nhiều trạm làm việc với nhau.
- ❖ Từ các thông tin "bắt" được có thể xử lý để trích ra những nội dung có giá trị → phân tích gói tin
- ❖ Các chương trình sniffer bắt các gói tin ở tầng Network trở xuống (gồm IP datagram và Ethernet Packet).
- ❖ Gói tin chứa các giao thức khác nhau ở các tầng như: TCP, UDP, IPX, …

2.3 Tấn công Packet Sniffing

❑ Công cụ Sniffer



2.3 Tấn công Packet Sniffing

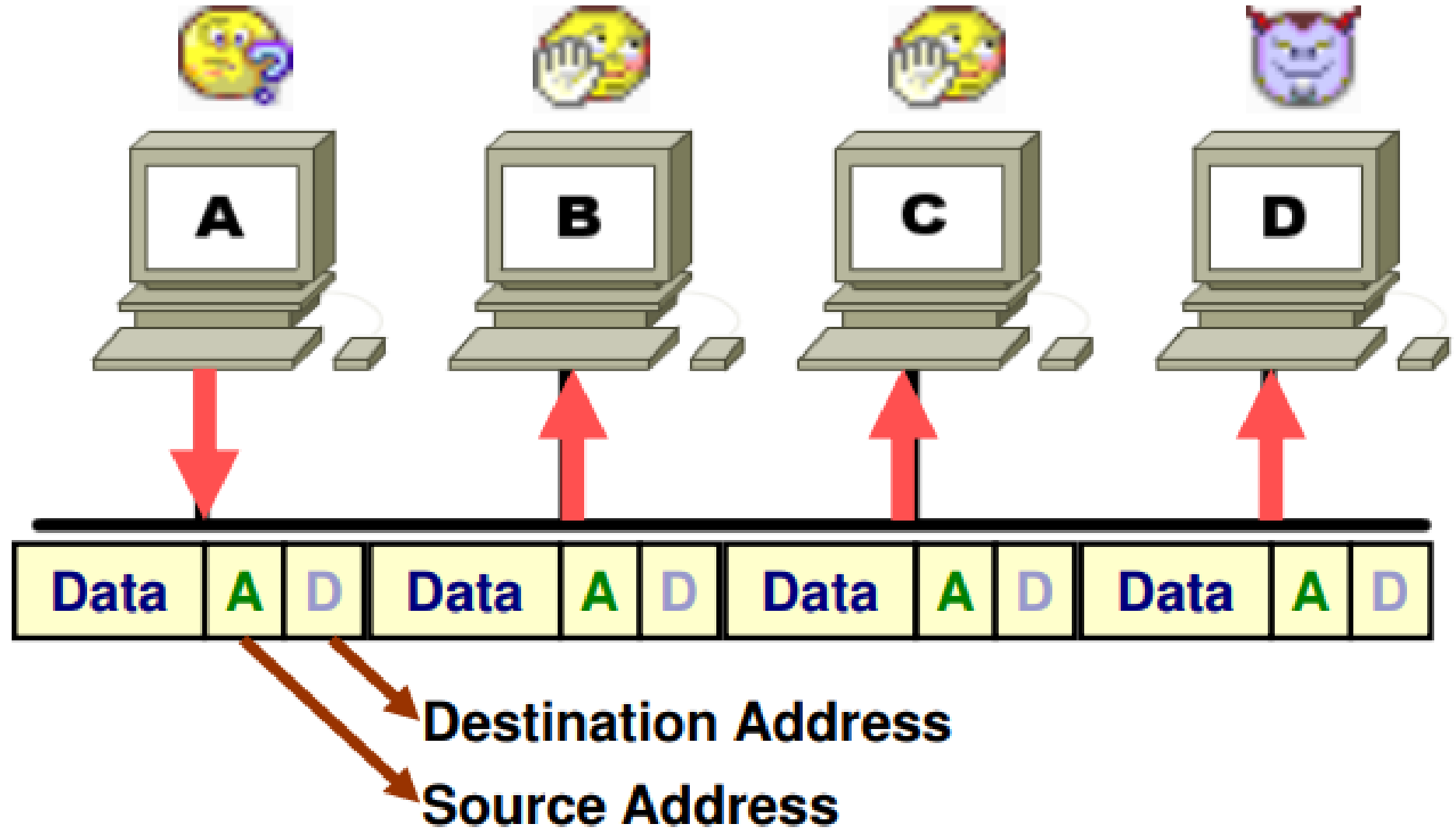
❑ Công cụ Sniffer

❖ Sniffer hoạt động theo cơ chế:

- Trên hệ thống mạng dạng quảng bá (bus, ring …) dữ liệu được truyền theo mọi hướng
- Các trạm khác trên mạng sẽ bỏ qua các thông tin trao đổi giữa hai trạm nguồn và trạm đích
- Các thiết bị/chương trình sniffer có thể bắt được toàn bộ thông tin trao đổi trên mạng là dựa vào nguyên tắc roadcast (quảng bá) các gói tin trong mạng Ethernet.

2.3 Tấn công Packet Sniffing

❑ Công cụ Sniffer



2.3 Tấn công Packet Sniffing

❑ Công cụ Sniffer

- ❖ Các trạm khác có thể "nghe" được bằng cách thiết lập chế độ hỗn tạp (promiscuous mode) trên các card mạng của trạm đó. Các chương trình Sniffer sẽ thực hiện công việc này.
- ❖ Cần phải xâm nhập được vào hệ thống mạng đó và cài đặt các phần mềm sniffer.
- ❖ Chương trình sniffer cũng yêu cầu người sử dụng phải hiểu sâu về kiến trúc, các giao thức mạng.
- ❖ Số lượng các thông tin trên mạng rất lớn nên các dữ liệu do các chương trình sniffer sinh ra khá lớn.

2.3 Tấn công Packet Sniffing

❑ Sniffing

- ❖ Lấy và chuyển đi
  - Các user ID và password
  - Số thẻ tín dụng
  - Các cuộc hội thoại email bí mật
- ❖ Tấn công Island hopping:
  - Đi qua các máy tính đơn (ví dụ, vir)
  - Cài đặt sniffer, quan sát password, đi qua nhiều máy, cài đặt các sniffer

2.3 Tấn công Packet Sniffing

❑ Mức độ nguy hại của Sniffer

❖ Tấn công sniffer rất nguy hiểm, vì được thực hiện ở các tầng rất thấp trong hệ thống mạng.

❖ Hệ thống sniffer cho phép lấy được toàn bộ các thông tin trao đổi trên mạng:

- Các tài khoản và mật khẩu truy nhập
- Các thông tin nội bộ hoặc có giá trị cao
- ....

2.3 Tấn công Packet Sniffing

❑ Sniffing thụ động

❖ Thực hiện lắng nghe và bắt tất cả các gói tin lưu thông trên mạng. Cách này khó bị phát hiện.

❑ Sniffing chủ động

❖ Thực hiện đánh lừa giao thức phân giải địa chỉ (ARP), hay tấn công làm tràn lưu lượng trong thiết bị chuyển mạch nhằm bắt các gói tin trong mạng. Các này dễ bị phát hiện.

2.3 Tấn công Packet Sniffing

- **Các công cụ sniffer thông dụng**
  - Wireshark, tcpdump (for unix), Snort (sniffing và kiểm tra xâm nhập)
- **Các công cụ sniffing mạnh**:
  - Dsniff và ettercap
    - Làm tràn bộ nhớ switch
    - Phá hoại bảng ARP

2.3 Tấn công Packet Sniffing

❑ Phòng thủ tấn công từ Sniffer

- ❖ Gắn các địa chỉ MAC vào cổng switch
  - Có sẵn trên các switch cao cấp
  - Cấu hình phức tạp
- ❖ Ưu tiên cho ánh xạ hiện có
  - Chỉ thay thế chúng khi timeout đã hết

2.3 Tấn công Packet Sniffing

❑ Các biện pháp hạn chế Sniffer

- ❖ Mã hóa dữ liệu trên đường truyền
  - SSL (Secure Sockets Layer),
  - Mạng riêng ảo VPN (Virtual Private Network)
  - Dùng SSH (Secure Shell Host) thay cho Telnet
  - Truyền tập tin SFTP (secure FTP) thay cho FTP
  - Giao thức HTTPS thay cho HTTP v.v…
- ❖ Không sử dụng hub: chuyển hoàn toàn sang mạng chuyển mạch
- ❖ Sử dụng mã hóa cho cả không dây và các kênh cáp.
- ❖ Xây dựng chính sách bảo vệ mạng (Network security policy)

2.3 Tấn công Packet Sniffing

❑ Các biện pháp hạn chế Sniffer

❖ Quản lý hệ thống mạng với những quy định:

- Đối tượng được phép sử dụng máy
- Đối tượng được phép gắn thêm thiết bị/cài chương trình
- Không cho người dùng tự ý cài đặt chương trình, v.v…

nhằm hạn chế tối đa khả năng xâm nhập về mặt vật lý để cài đặt các chương trình nghe lén trong mạng.

❖ Kiểm tra các tiến trình trên hệ thống: tài nguyên sử dụng, thời gian khởi tạo tiến trình... để phát hiện các chương trình sniffer.

2.4 Tấn công MitM (Man-in-the-Middle)

❑ Tấn công người đứng giữa (Man in the middle)

- ❖ Lợi dụng quá trình chuyển gói tin đi qua nhiều trạm (hop) thuộc các mạng khác nhau;
- ❖ Kẻ tấn công chặn bắt các thông điệp giữa 2 bên tham gia truyền thông, có thể xem, sửa đổi và chuyển thông điệp lại cho bên kia.
- ❖ Thường được sử dụng để đánh cắp thông tin

2.4 Tấn công MitM (Man-in-the-Middle)

❑ Các kịch bản tấn công MitM

❖Cách tấn công khác nhau trong các tình huống khác nhau

- **LOCAL AREA NETWORK:**

- Phá hoại ARP - Giả mạo DNS - STP mangling - Đánh cắp cổng

- **TỪ LOCAL TỚI REMOTE (qua gateway):**

- Phá hoại ARP - Giả mạo DNS - Giả mạo DHCP

- ICMP redirection - Giả mạo IRDP - route mangling

- **REMOTE:**

- Phá hoại DNS - traffic tunneling - route mangling

2.4 Tấn công MitM (Man-in-the-Middle)

❑ Ví dụ local MitM: giả mạo DNS

❖ Nếu kẻ tấn công nghe trộm được ID của bản tin DNS request, họ có thể gửi trả lời trước server DNS thật

❑ Các công cụ dùng trong giả mạo DNS

❖ ettercap (http://ettercap.sf.net)
- Phantom plugin

❖ dsniff (http://www.monkey.org/~dugsong/dsniff)
- Dnsspoof

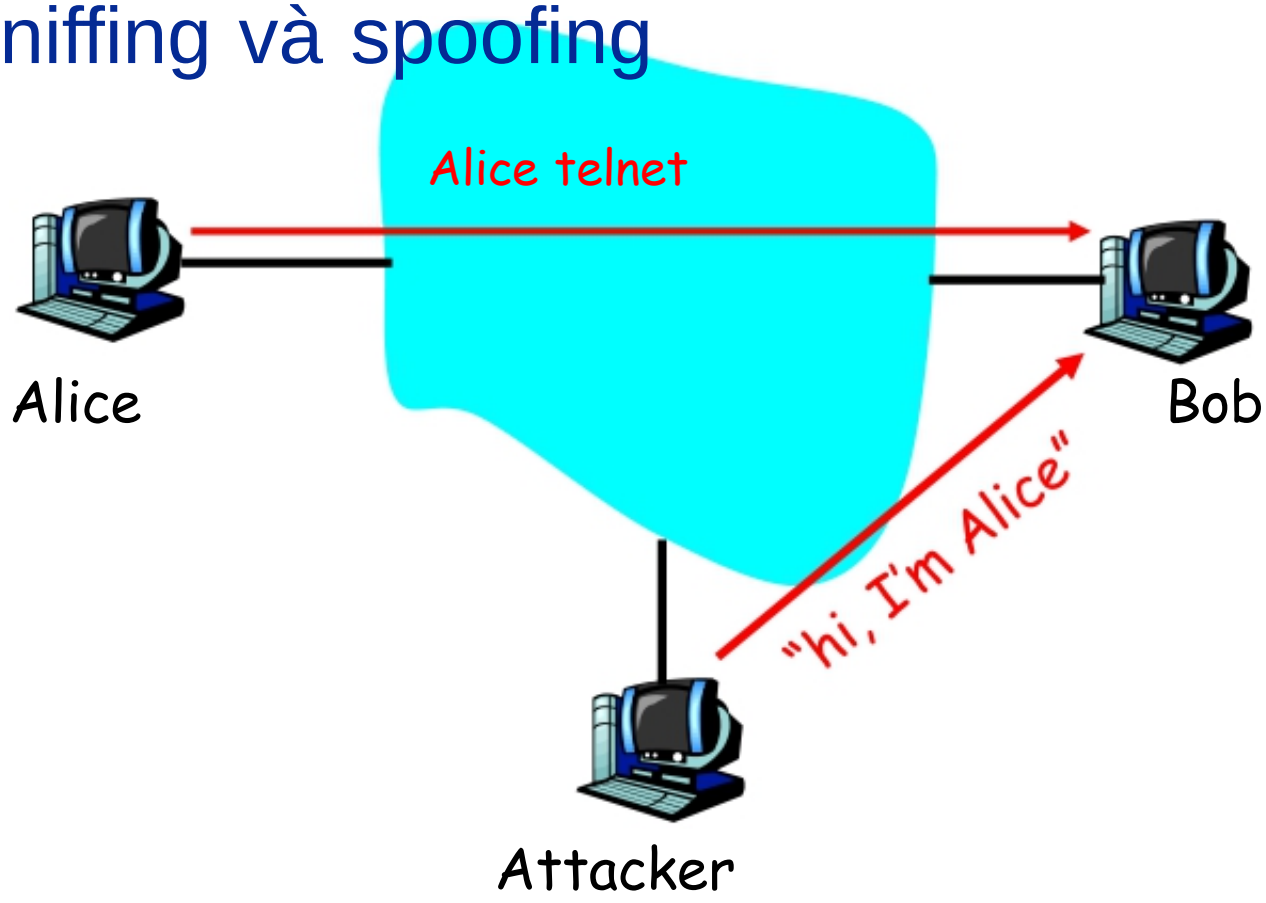
❖ zodiac (http://www.packetfactory.com/Projects/zodiac)

2.4 Tấn công MitM (Man-in-the-Middle)

- **Ví dụ local tới remote MitT: chuyển hướng ICMP**
  - Nếu kẻ tấn công có thể bắt chuyển hướng gói ICMP nhằm chuyển lưu lượng tới chúng
- **Các công cụ dùng trong chuyển hướng ICMP**
  - IRPAS icmp_redirect (Phenoelit) (http://www.phenoelit.de/irpas/)
  - icmp_redir (Yuri Volobuev)
- **Các công cụ dùng trong tấn công MitT từ xa**
  - ettercap (http://ettercap.sf.net)
    - Zaratan plugin
  - tunnelX (http://www.phrack.com)

2.5 Session hijacking

- Kẻ tấn công sẽ tiếp cuộc liên lạc, trong khi đó ngắt kết nối ban đầu
- Lấy quyền điều khiển của một phía trong kết nối TCP
  - Kết hợp sniffing và spoofing



2.5 Session hijacking

❑ Chi tiết tấn công session hijacking

- ❖ Kẻ tấn công trên đoạn lưu lượng giữa Alice và Bob
  - Kẻ tấn công sniff các gói tin, và thấy được các gói tin TCP giữa Bob và Alice và các số thứ tự (sequence number) của chúng.
- ❖ Kẻ tấn công nhảy vào, gửi các gói TCP tới Bob; địa chỉ IP nguồn = Địa chỉ IP của Alice
  - Lúc này Bob sẽ nghe lệnh được gửi từ kẻ tấn công, vì nghĩ là nó được gửi từ Alice.
- ❖ Nguyên lý phòng thủ: mã hóa
  - Kẻ tấn công không có khóa để mã hóa và chèn lưu lượng có ý nghĩa.

2.5 Session hijacking

❑ Hạn chế của session hijacking

Bob nhận được segments từ kẻ tấn công và Alice. Địa chỉ IP nguồn là như nhau, nhưng số thứ tự (seq#) khác nhau.
Bob sẽ ngắt kết nối.

Cách thức của kẻ tấn công:

- Gửi các đáp ứng ARP không được yêu cầu tới Alice và Bob với địa chỉ MAC không tồn tại.
- Ghi đè lên bảng ARP IP-to-MAC
- Segments của Alice sẽ không tới được Bob và ngược lại.
- Nhưng kẻ tấn công sẽ tiếp tục nghe ngóng các segments từ phía Bob, liên lạc với Bob.

2.5 Session hijacking

❑ Các công cụ session Hijacking

- ❖ Hunt
  - http://ihackers.co/hunt-session-hijacking-tool/
  - Hỗ trợ phá hoại ARP
- ❖ Netcat
  - Rất thông dụng

2.6 Tấn công Từ chối dịch vụ

- Tấn công từ chối dịch vụ (DoS - Denial of Service Attacks) là dạng tấn công cản trở người dùng hợp pháp truy nhập các tài nguyên hệ thống

- Hai loại tấn công DoS:
  - Tấn công logic (Logic attacks): tấn công dựa vào các lỗi phần mềm làm dịch vụ ngừng hoạt động hoặc làm giảm hiệu năng hệ thống.
    - Cần cài đặt các bản cập nhật thường xuyên để phòng chống.
  - Tấn công gây ngập lụt (Flooding attacks): Kẻ tấn công gửi một lượng lớn yêu cầu gây cạn kiệt tài nguyên hệ thống hoặc băng thông đường truyền mạng.

2.6 Tấn công Từ chối dịch vụ

❑ Các dạng tấn công DoS – SYN Floods

- ❖ SYN floods là kỹ thuật gây ngập lụt các gói tin mở kết nối TCP.
  - SYN là bít điều khiển của TCP dùng để đồng bộ số trình tự gói.
- ❖ SYN floods khai thác điểm yếu trong thủ tục bắt tay 3 bước khi thiết lập kết nối cho phiên truyền thông TCP/IP.
- ❖ SYN floods gây cạn kiệt tài nguyên máy chủ:
  - Có thể làm máy chủ ngừng hoạt động;
  - Hoặc không chấp nhận yêu cầu mở kết nối mới

2.6 Tấn công Từ chối dịch vụ

❑ Các dạng tấn công DoS – SYN Floods

❖ Kịch bản tấn công SYN floods:

- Kẻ tấn công gửi 1 lượng lớn gói tin yêu cầu mở kết nối (SYN-REQ) đến máy tính nạn nhân;
- Máy tính nạn nhân ghi nhận yêu cầu kết nối và dành 1 chỗ trong bảng lưu kết nối trong bộ nhớ cho mỗi yêu cầu kết nối;
- Máy tính nạn nhân sau đó gửi gói tin xác nhận kết nối (SYN-ACK) đến kẻ tấn công;
- Do kẻ tấn công không bao giờ trả lời xác nhận kết nối, nên máy tính nạn nhân vẫn phải lưu tất cả các yêu cầu kết nối chưa được xác nhận trong bảng kết nối→ bảng kết nối đầy và người dùng hợp pháp không thể truy nhập;
- Máy tính nạn nhân chỉ có thể xóa yêu cầu kết nối chưa được xác nhận khi nó quá hạn (timed-out)

2.6 Tấn công Từ chối dịch vụ

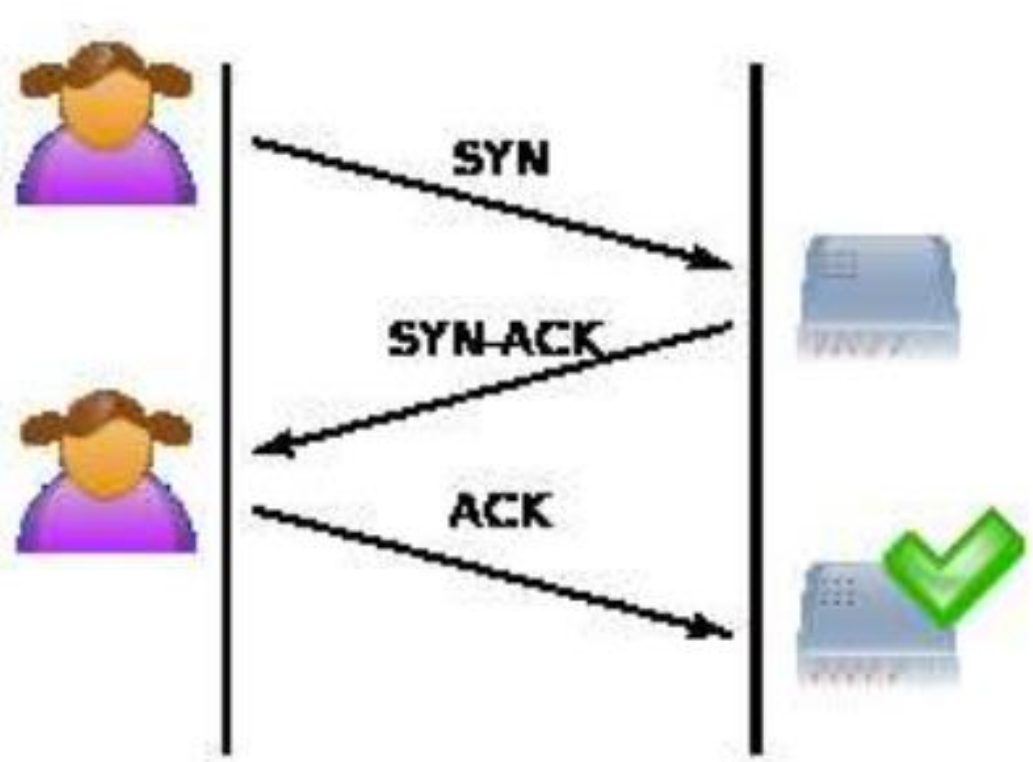
❑ Các dạng tấn công DoS – SYN Floods

❖ Phân tích tấn công SYN floods:

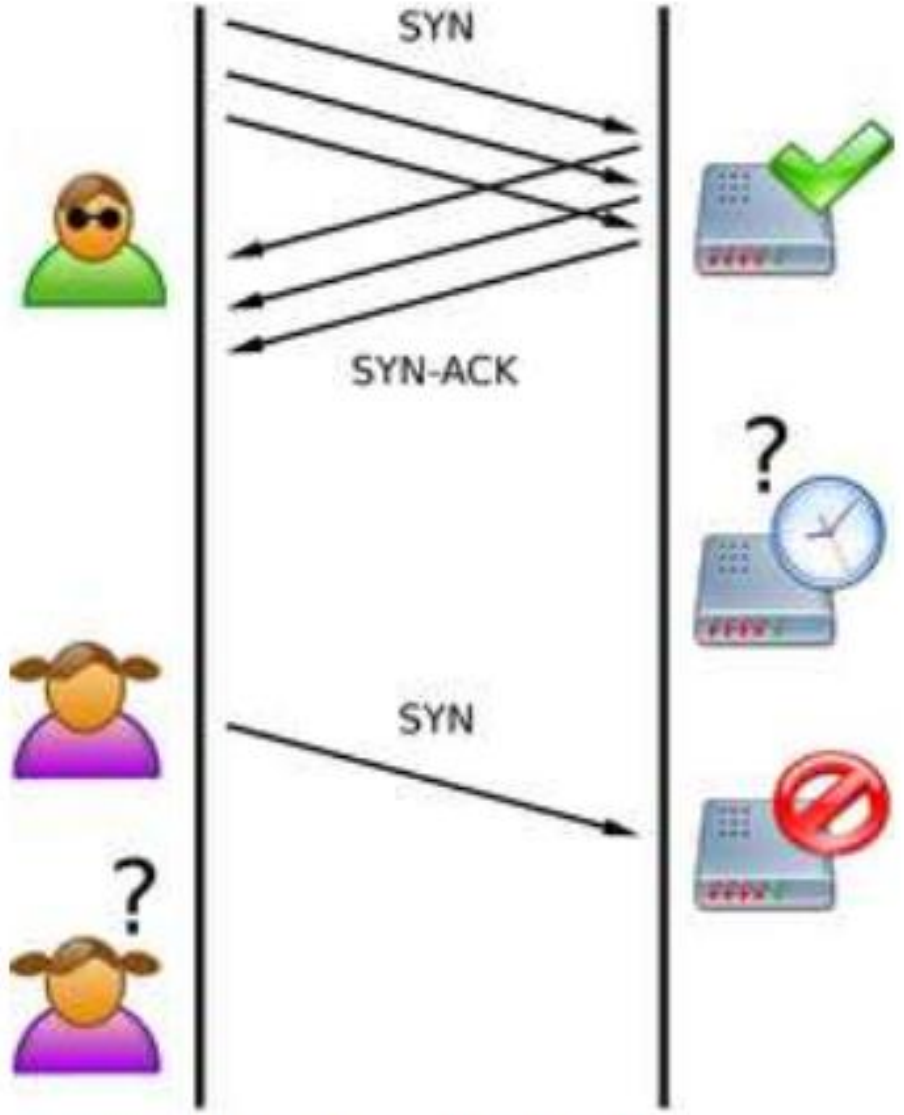
- Kẻ tấn công thường dùng địa chỉ IP giả mạo hoặc địa chỉ không có thực làm Source IP trong gói tin IP, nên thông điệp SYN-ACK của máy tính nạn nhân không bao giờ đến đích;
- Kẻ tấn công cố tình tạo một lượng rất lớn yêu cầu kết nối dở dang để:
  - Các yêu cầu kết nối SYN-REQ điền đầy bảng kết nối → máy nạn nhân không thể chấp nhận yêu cầu của những người dùng khác;
  - Làm cạn kiệt tài nguyên bộ nhớ của máy nạn nhân→ có thể làm máy nạn nhân ngừng hoạt động;
  - Gây nghẽn đường truyền mạng.

2.6 Tấn công Từ chối dịch vụ

❑ Các dạng tấn công DoS – SYN Floods



Normal TCP
three-way handshake



SYN Floods Attack

2.6 Tấn công Từ chối dịch vụ

❑ Các dạng tấn công DoS – SYN Floods

❖ Phòng chống:

- Sử dụng kỹ thuật lọc (Filtering): cần sửa đổi giao thức TCP không cho phép kẻ tấn công giả mạo địa chỉ;
- Tăng kích thước bảng kết nối (Backlog): tăng kích thước Backlog lưu các yêu cầu kết nối→tăng khả năng chấp nhận các yêu cầu;
- Giảm thời gian chờ (SYN-RECEIVED Timer): các kết nối chưa được xác nhận sẽ bị xóa khi hết thời gian chờ;
- SYN cache: yêu cầu kết nối chỉ được cấp phát không gian nhớ đầy đủ khi nó được xác nhận;
- Sử dụng Firewalls và Proxies
  - Có khả năng nhận dạng các địa chỉ IP nguồn là địa chỉ không có thực;
  - Có khả năng tiếp nhận kết nối, chờ đến khi có xác nhận mới chuyển lại cho máy chủ đích.

2.6 Tấn công Từ chối dịch vụ

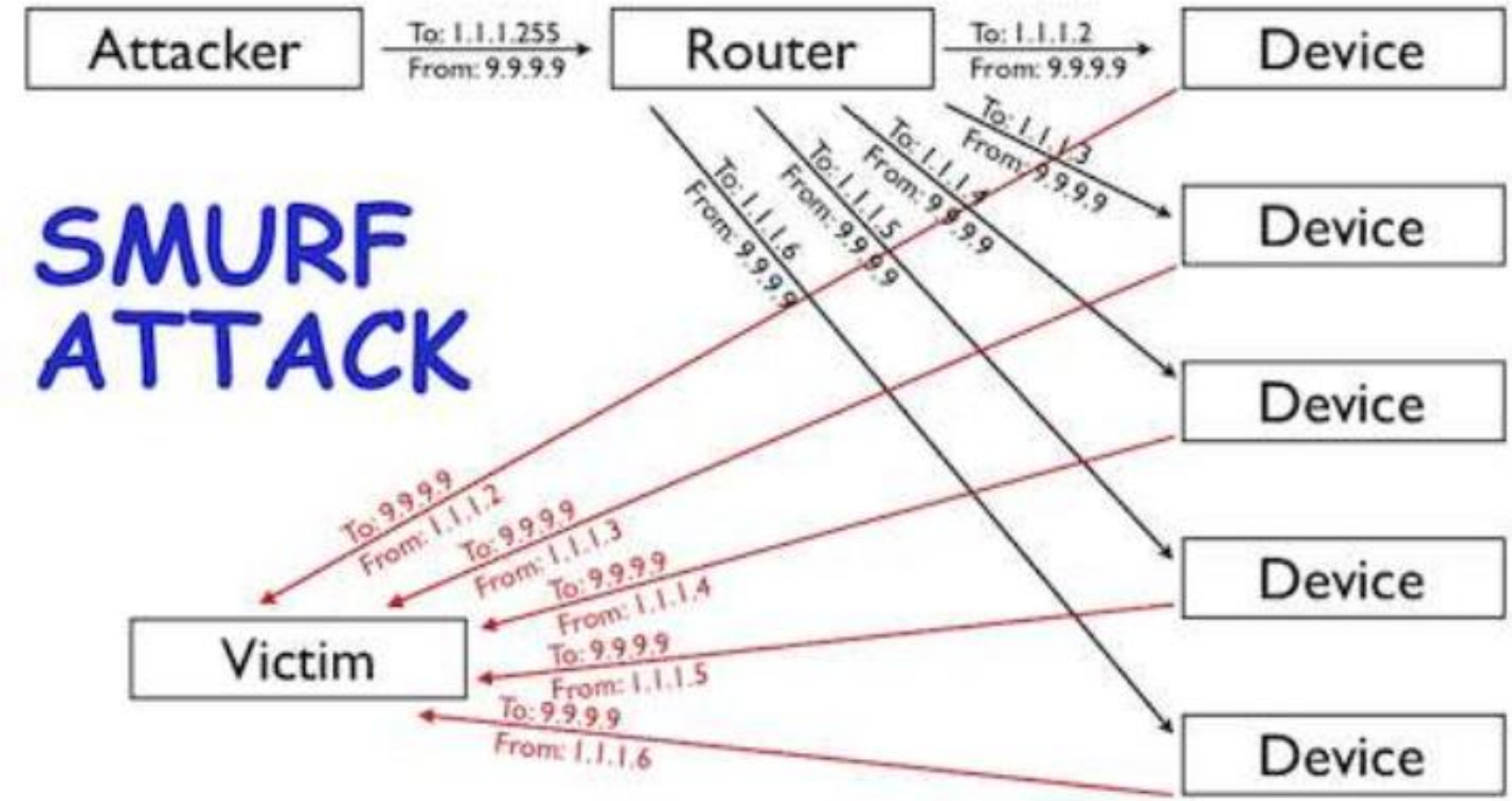
❑ Các dạng tấn công DoS – Smurf

- ❖ Tấn công Smurf sử dụng kiểu phát quảng bá có định hướng để gây ngập lụt đường truyền mạng của máy nạn nhân.
- ❖ Kịch bản tấn công Smurf:
  - ▪ Kẻ tấn công gửi một lượng lớn gói tin ICMP (Ping) với địa chỉ IP nguồn là địa chỉ của máy nạn nhân đến một mạng sử dụng một địa chỉ quảng bá (IP Broadcast address);
  - ▪ Các máy trong mạng nhận được thông điệp ICMP sẽ gửi trả lời đến máy có địa chỉ IP là địa nguồn trong thông điệp ICMP (là máy nạn nhân);

• Nếu lượng máy trong mạng rất lớn → máy nạn nhân sẽ bị ngập lụt đường truyền

2.6 Tấn công Từ chối dịch vụ

❑ Các dạng tấn công DoS – Smurf



2.6 Tấn công Từ chối dịch vụ

❑ Các dạng tấn công DoS – Smurf

❖ Phòng chống:

- Cấu hình các máy và router không trả lời các yêu cầu ICMP hoặc các yêu cầu phát quảng bá;
- Cấu hình các router không chuyển tiếp yêu cầu gửi đến các địa chỉ quảng bá;
- Sử dụng tường lửa để lọc các gói tin với địa chỉ giả mạo địa chỉ trong mạng

2.6 Tấn công Từ chối dịch vụ

❑ Các kỹ thuật tấn công DoS

- ❖ **Land:** gửi gói tin giả mạo với địa chỉ/cổng nguồn và đích giống nhau.
- ❖ **Ping of death:** gửi gói tin ping quá kích cỡ
- ❖ **Jolt2:** gửi một luồng các mảnh, không mảnh nào có offset là 0. Tập hợp lai sử dụng tất cả nguồn lực xử lý.
- ❖ **Teardrop, Newtear, Bonk, Syndrop:** các công cụ gửi các segment chồng nhau, nghĩa là, offset của các mảnh không đúng.

2.6 Tấn công Từ chối dịch vụ

❑ Tấn công DDoS

❖ Tấn công DDoS (Distributed Denial of Service Attacks) là một loại tấn công DoS:

- Liên quan đến gây ngập lụt các máy nạn nhân với một lượng rất lớn các yêu cầu kết nối giả mạo;
- DDoS khác DoS ở phạm vi tấn công:
  - Số lượng máy tham gia tấn công DoS thường tương đối nhỏ, chỉ gồm một số ít máy tại một, hoặc một số ít địa điểm;
  - Số lượng máy tham gia tấn công DDoS thường rất lớn, có thể lên đến hàng ngàn, hoặc trăm ngàn máy, và đến từ rất nhiều vị trí địa lý khác nhau trên toàn cầu.

2.6 Tấn công Từ chối dịch vụ

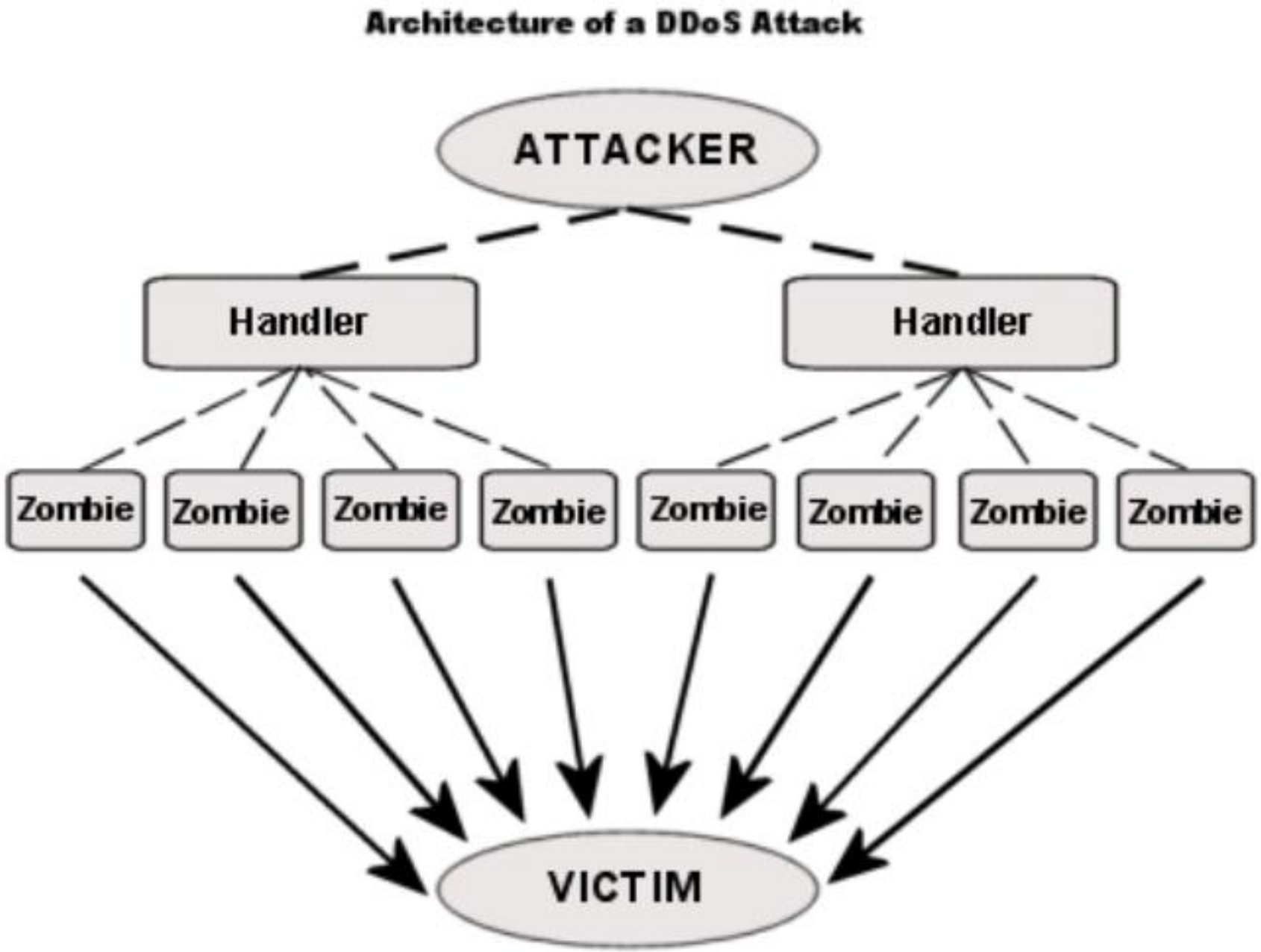
❑ Tấn công DDoS

❖ Kịch bản tấn công DDoS:

- Kẻ tấn công chiếm quyền điều khiển hàng trăm thậm chí hàng ngàn máy tính trên mạng Internet, sau đó cài các chương trình tấn công tự động (Automated agents) lên các máy này;
  - Automated agents còn được gọi là các Bots hoặc Zombies;
  - Các máy bị chiếm quyền điều khiển hình thành mạng máy tính ma, gọi là botnet hay zombie network.
- Tiếp theo, kẻ tấn công ra lệnh cho các automated agents đồng loạt tạo các yêu cầu giả mạo gửi đến các máy nạn nhân;
- Lượng yêu cầu giả mạo có thể rất lớn và đến từ rất nhiều nguồn khác nhau nên rất khó đối phó và lần vết để tìm ra kẻ tấn công thực sự

2.6 Tấn công Từ chối dịch vụ

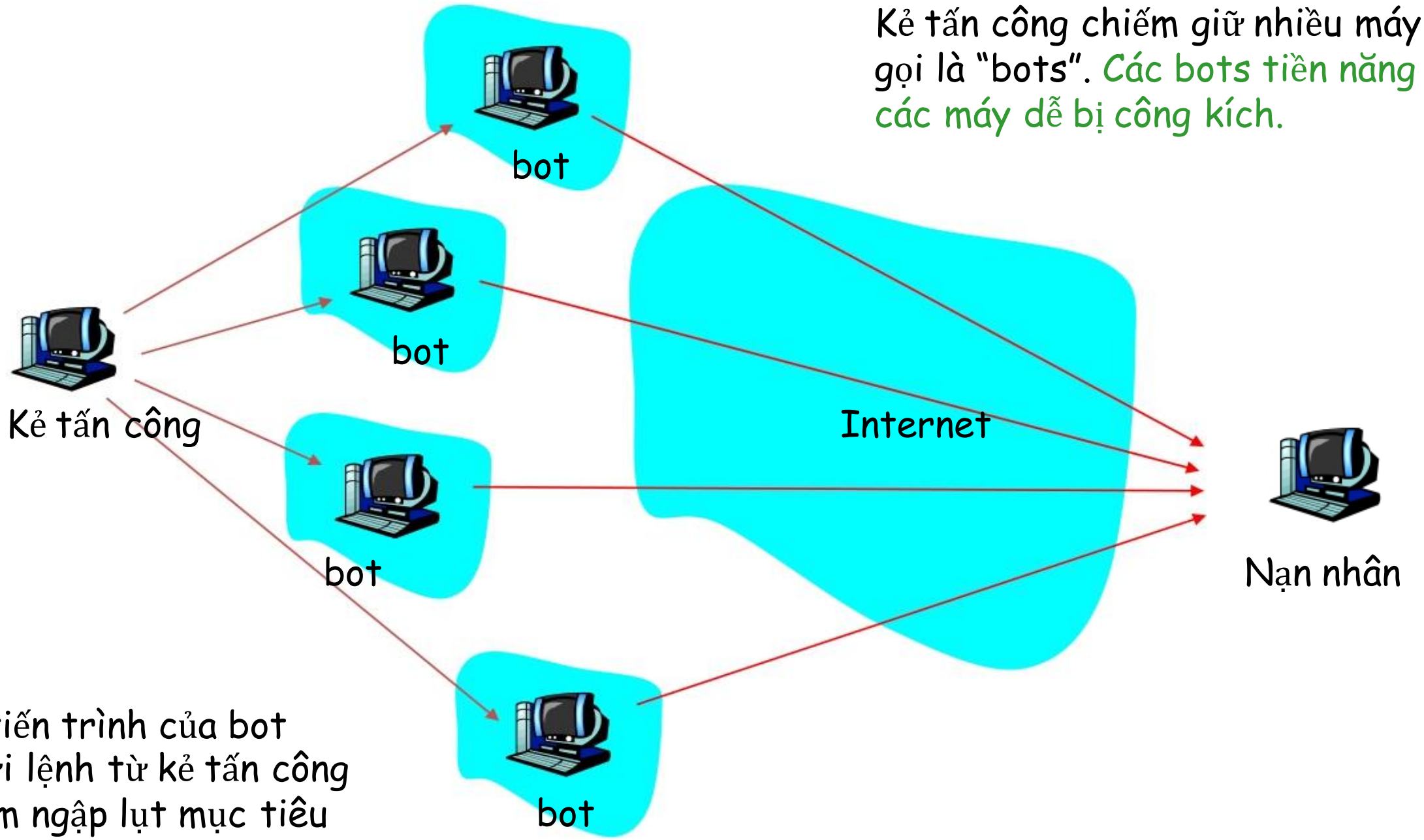
❑ Tấn công DDoS



2.6 Tấn công Từ chối dịch vụ

❑ DoS phân tán: DDos

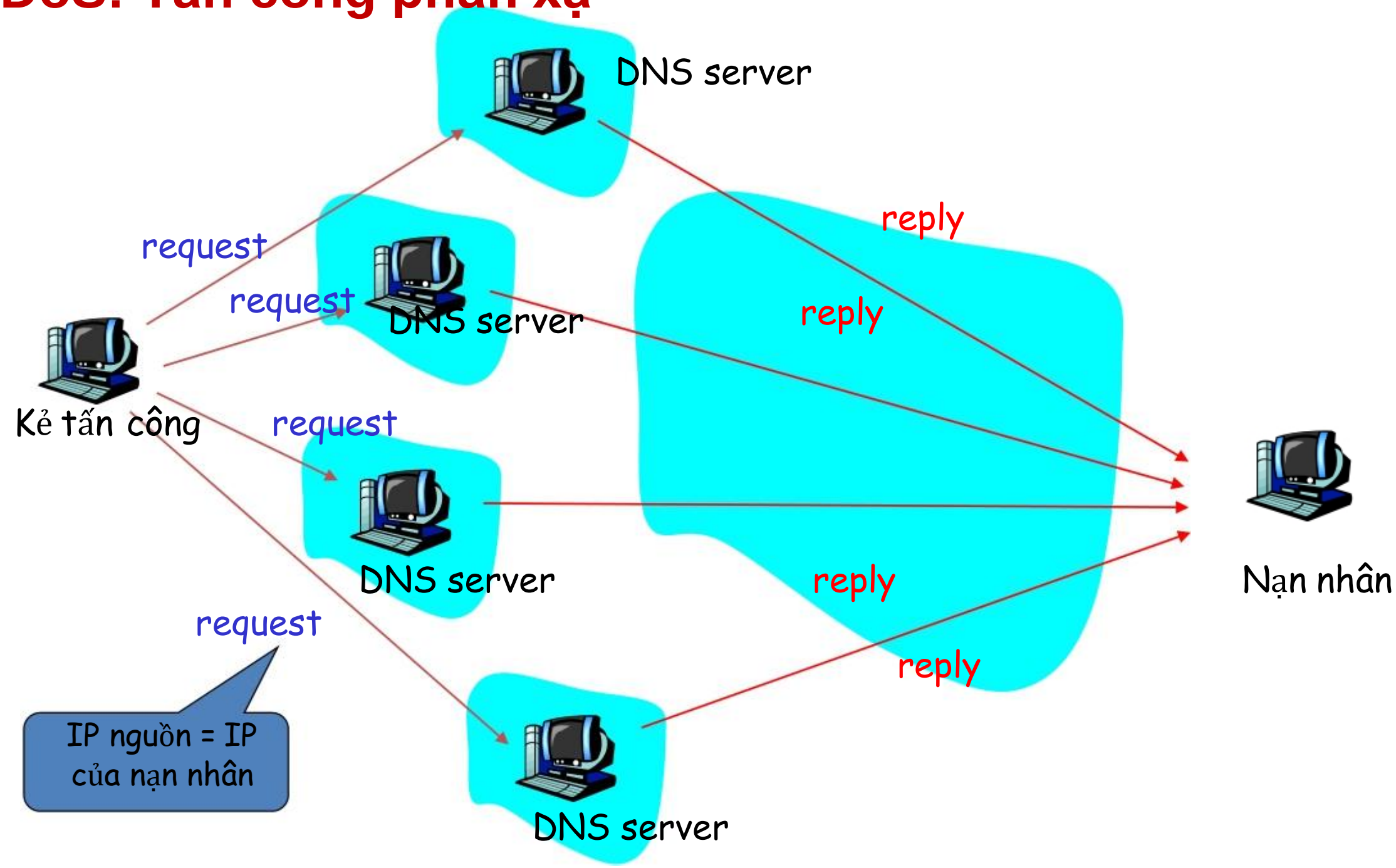
Kẻ tấn công chiếm giữ nhiều máy, gọi là "bots". Các bots tiền năng là các máy dễ bị công kích.



Các tiến trình của bot sẽ đợi lệnh từ kẻ tấn công để làm ngập lụt mục tiêu

2.6 Tấn công Từ chối dịch vụ

❑ DDoS: Tấn công phản xạ



2.6 Tấn công Từ chối dịch vụ

❑ DDoS: Tấn công phản xạ (tiếp)

❖Địa chỉ IP nguồn giả mạo = IP của nạn nhân

❖*Mục tiêu:* tạo ra câu trả lời dài dòng hoặc nhiều cho các yêu cầu ngắn: *khuếch đại*

- *Nếu không có khuêch đại: nên làm gì?*

❖Tấn công tháng 1 năm 2001:

- Yêu cầu bản ghi DNS lớn
- Tạo ra lưu lượng 60-90 Mbps

❖Tấn công phản xạ có thể cũng được thực hiện với Web hoặc các dịch vụ khác.

2.6 Tấn công Từ chối dịch vụ

❑ Phòng thủ tấn công DDoS

❖ Không để cho hệ thống của người dùng trở thành bot

- Giữ hệ thống cập nhật bản vá
- Cung cấp lọc chống giả mạo đi ra trên router ngoài.

❖ Lọc các gói tin nguy hiểm

- Các tấn công lỗ hổng
- Hệ thống ngăn chặn xâm nhập

2.6 Tấn công Từ chối dịch vụ

❑ Phòng thủ tấn công DDoS

- ❖ Dự phòng tài nguyên lớn
  - Băng thông dồi dào
  - Tài nguyên server lớn
  - ISP cũng cần băng thông dồi dào
  - Nhiều ISPs
- ❖ Chữ ký, phát hiện bất thường và lọc
- ❖ Giới hạn tốc độ
  - Giới hạn số lượng gói tin từ nguồn đến đích

2.6 Tấn công Từ chối dịch vụ

❑ Tấn công DoS: Ping of Death

- ❖ **Ping of death:** gửi gói tin ping có kích thước quá khổ
- ❖ ICMP Ping Of Death
  - Flag=last fragment
  - Offset*8 + Length > 65535

Là một kiểu tấn công DoS !

2.6 Tấn công Từ chối dịch vụ

❑ Tấn công DoS: Ping of Death

❖ICMP Echo Request (Ping) là 56 bytes

❖Nếu một thông điệp ping lớn hơn 65536 bytes (là kích thước lớn nhất của một gói tin IP), thì có thể làm cho một số máy bị sập khi tập hợp lại gói tin.

❖Các hệ thống windows cũ

2.6 Tấn công Từ chối dịch vụ

❑ Tấn công DoS: LAND

❖Local Area Network Denial

❖Gói tin giả mạo với tập cờ SYN

❖Gửi tới cổng mở

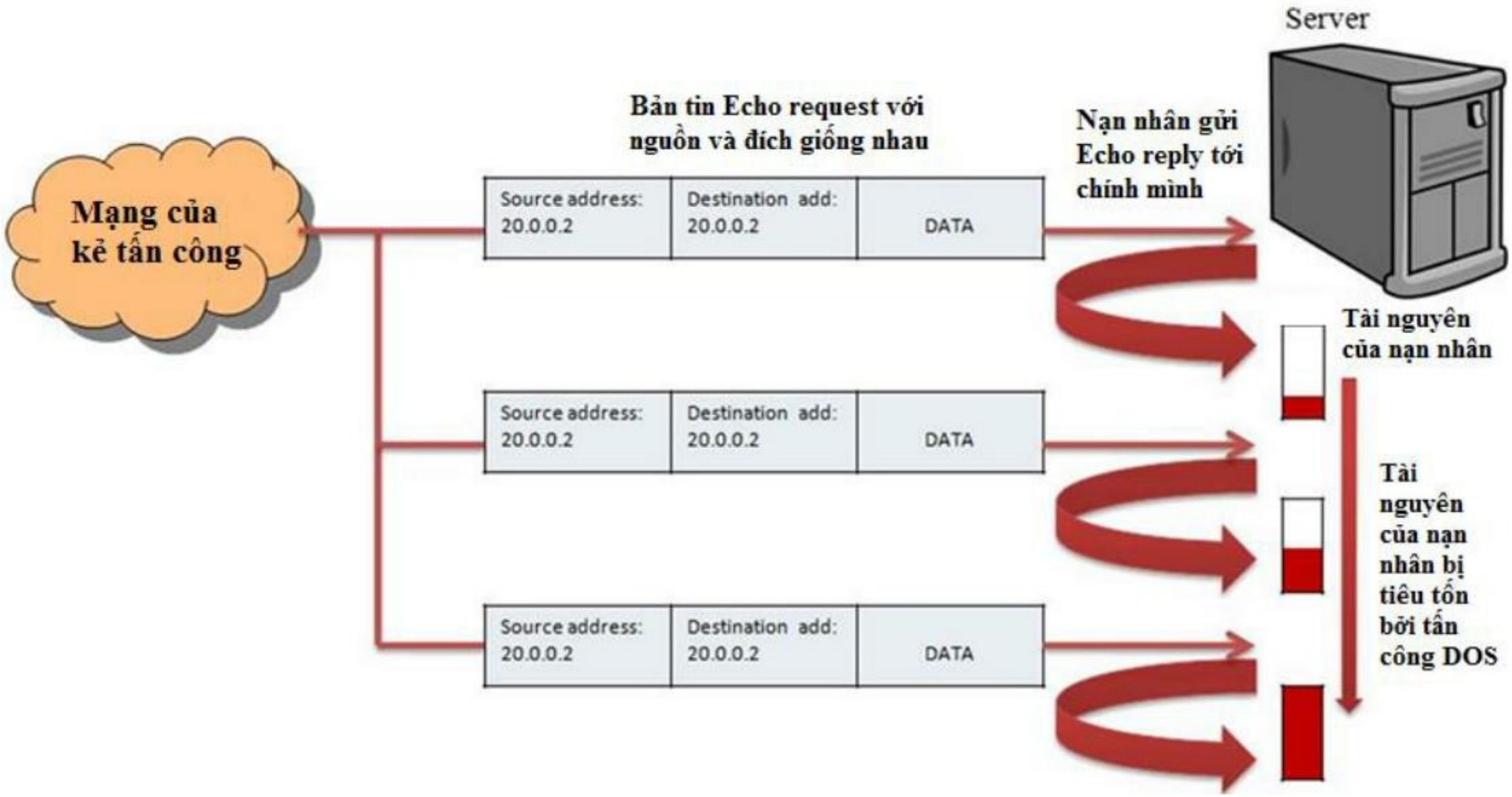
❖Địa chỉ/Cổng nguồn giống địa chỉ/cổng đích

❖Nhiều hệ điều hành bị khóa

Là một loại tấn công DoS lớp 4

2.6 Tấn công Từ chối dịch vụ

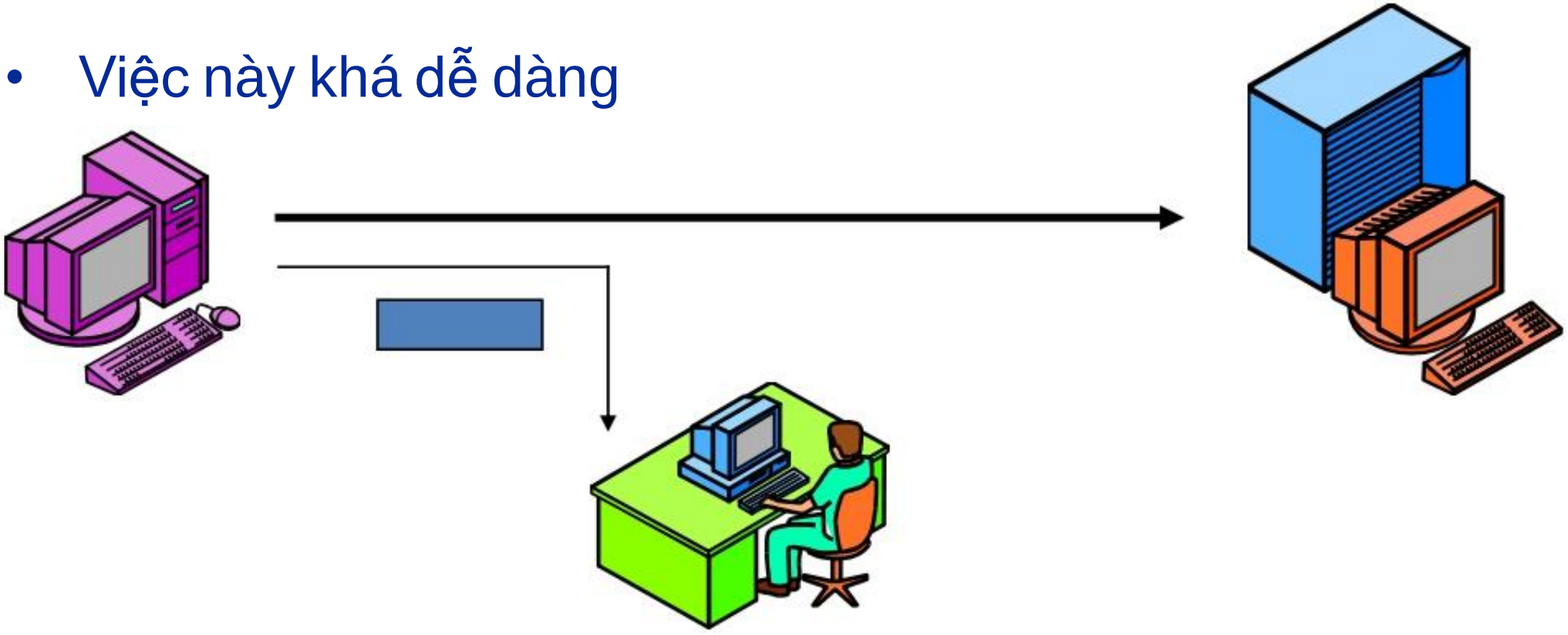
❑ Tấn công ICMP LAND



2.7 Tấn công lặp lại

❑ Tấn công lặp lại

- ❖ Tấn công lặp lại (Replay) là tấn công mà kẻ tấn công tái sử dụng các cuộc liên lạc trước.
- ❖ Các bước tấn công:
  - Trước tiên, kẻ tấn công chặn thông điệp
    - Việc này khá dễ dàng

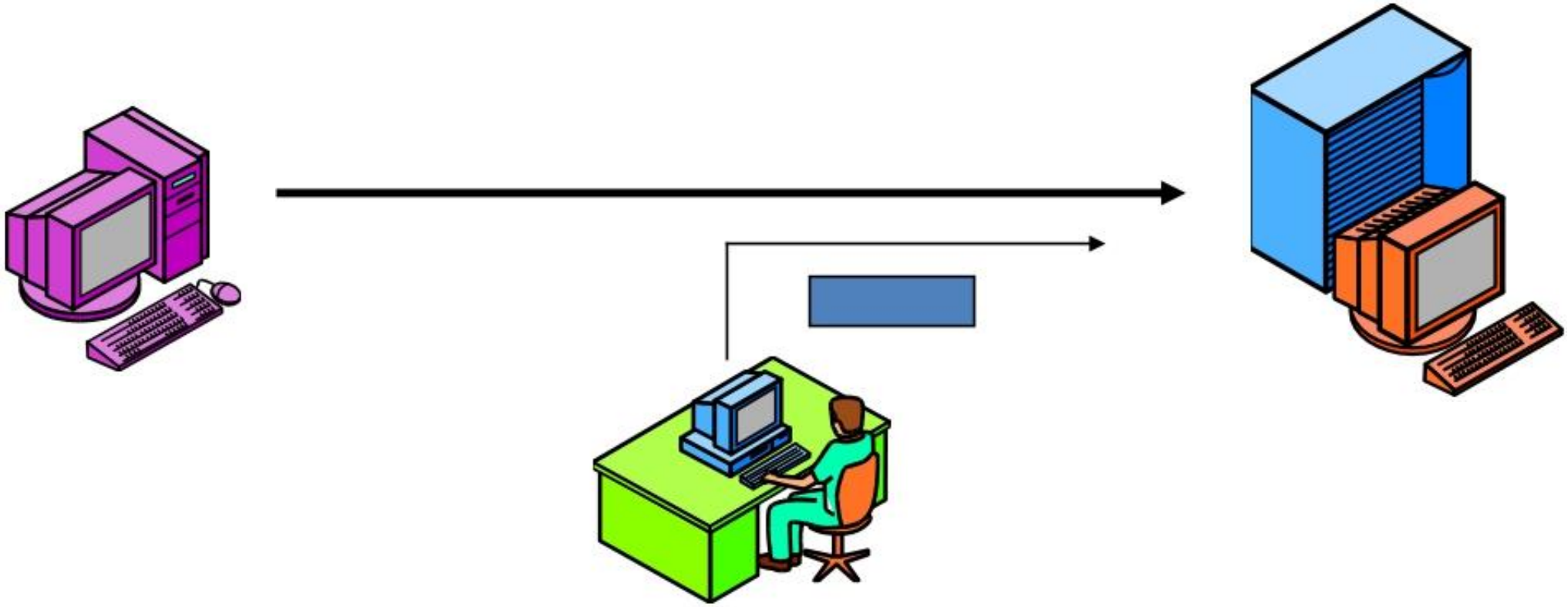


2.7 Tấn công lặp lại

❑ Tấn công lặp lại

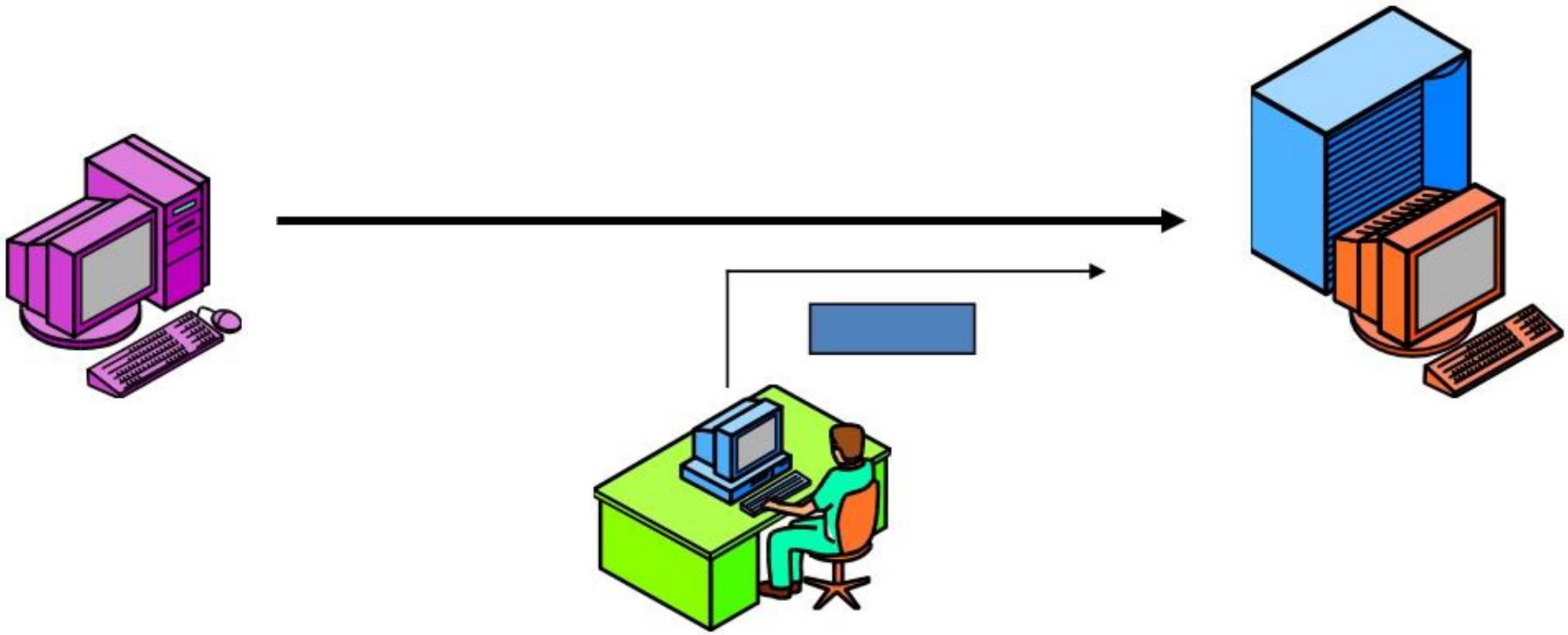
❖ Sau đó, kẻ tấn công truyền lại (lặp lại) thông điệp tới host đích ban đầu

- Không cần thiết phải đọc được thông điệp để truyền lại



2.7 Tấn công lặp lại

- Tại sao lại thực hiện tấn công lặp lại?
  - Để chiếm quyền truy cập tới tài nguyên bằng cách lặp lại thông điệp xác thực
  - Trong tấn công DoS, được dùng để gây nhiễu host đích

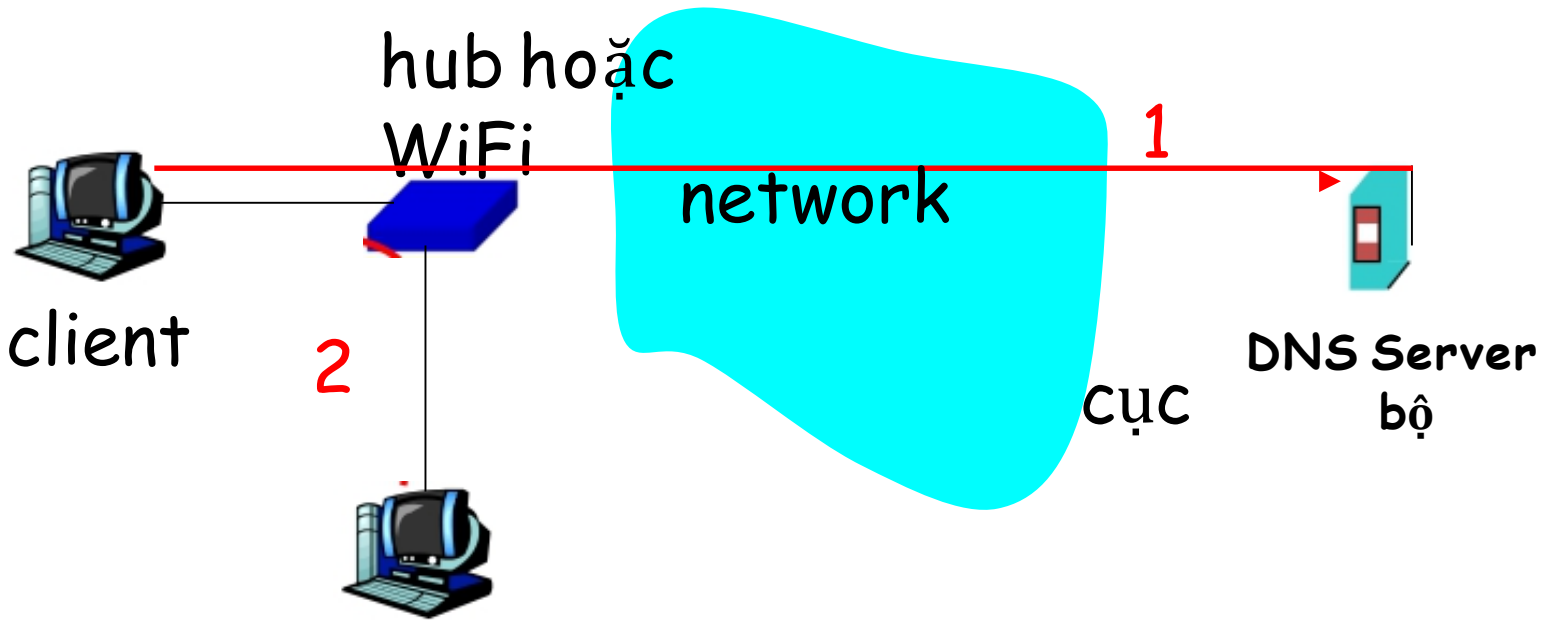


2.8 Tấn công DNS

- Tấn công phản xạ
  - Tận dụng DNS cho các cuộc tấn công vào mục tiêu tùy ý
- Từ chối dịch vụ DNS
  - Dừng DNS server gốc
  - Dừng top-level-domain servers (ví dụ, tênmiền.com)
  - Dừng server cục bộ (servers tên mặc định)
- Sử dụng giả mạo DNS để trả lời nhằm chuyển hướng người dùng
- Phá hoại DNS (poisoning):
  - Chèn bản ghi tài nguyên lỗi vào các vùng đệm DNS khác nhau.
  - Các bản ghi lỗi chứa địa chỉ IP được điều hành bởi kẻ tấn công.

2.8 Tấn công DNS

❑ Tấn công DNS: chuyển hướng



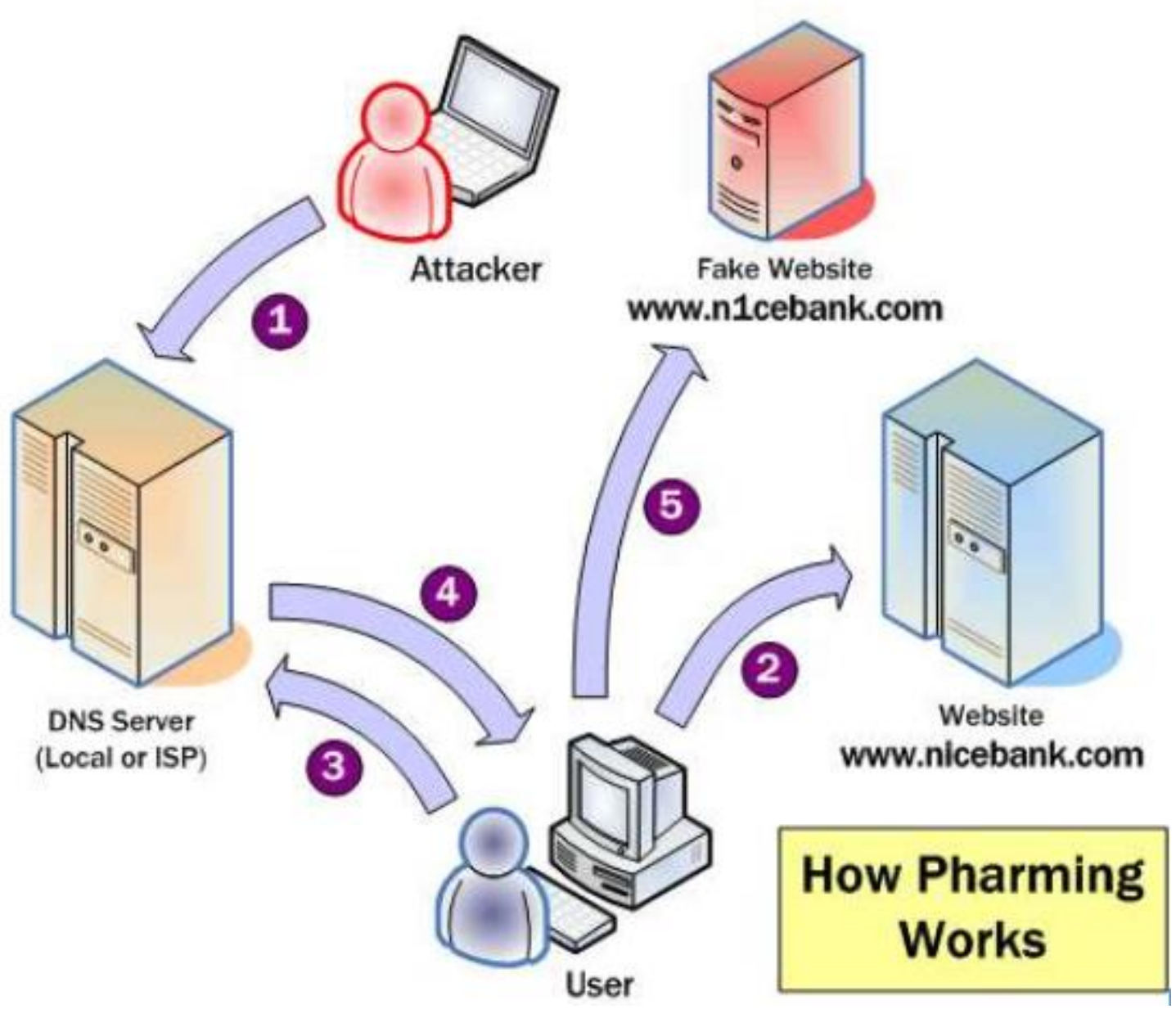
1. Client gửi truy vấn DNS query tới DNS server cục bộ của nó; sniffing bởi kẻ tấn công.
2. Kẻ tấn công trả lời bằng đáp ứng DNS không có thật.

Vấn đề:

- Phải spoof địa chỉ IP: thiết lập DNS server cục bộ *(dễ dàng)*
- Phải so khớp ID trả lời với ID yêu cầu (dễ dàng)
- Có thể cần dừng đáp ứng từ DNS server cục bộ *(khó khăn hơn)*

2.8 Tấn công DNS

❑ Tấn công DNS: chuyển hướng



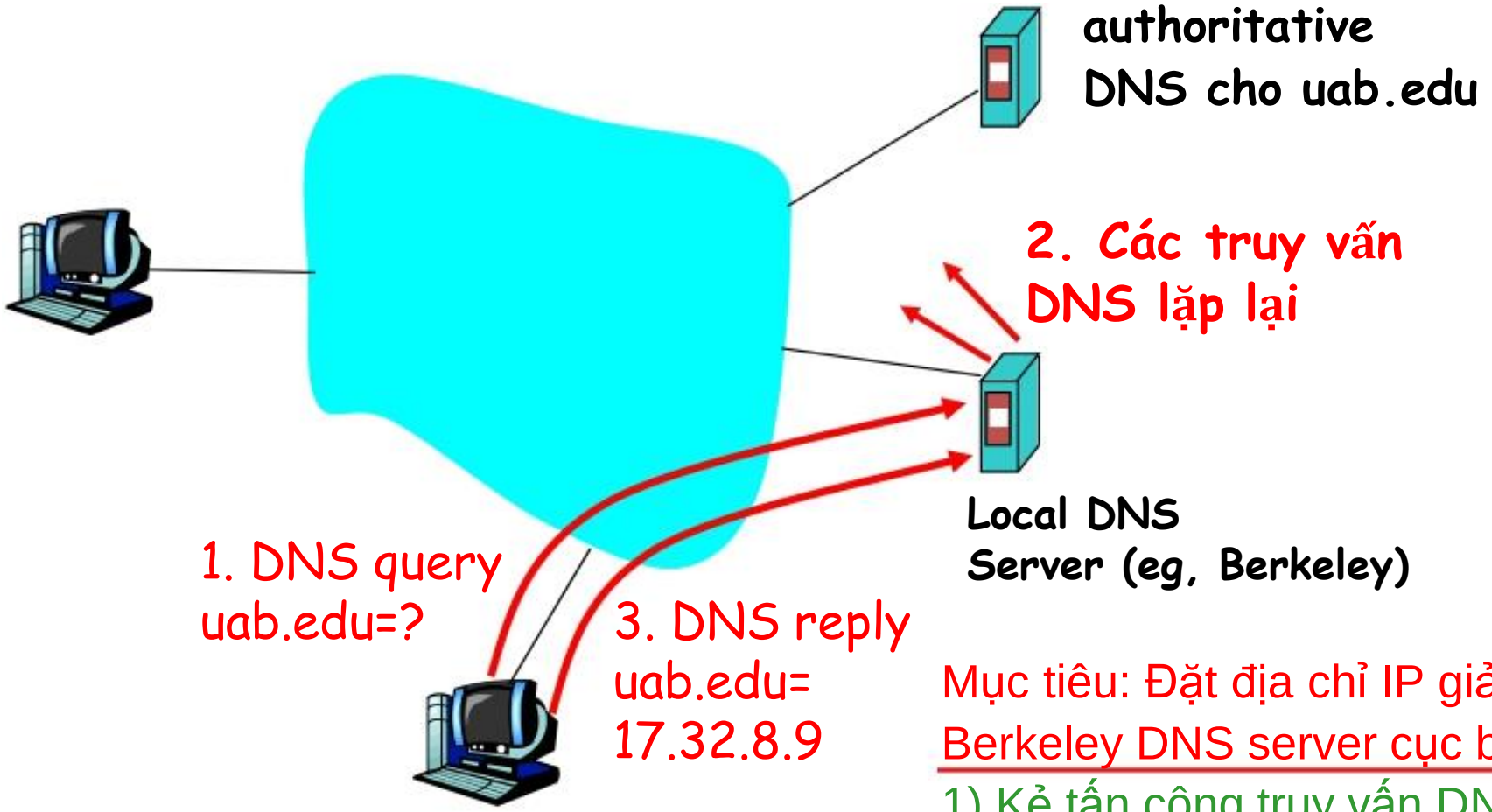
2.8 Tấn công DNS

❑ Phá hoại bộ đệm DNS

- ❖ Phá hoại (Poisoning): Cố gắng đưa các bản ghi giả vào trong vùng đệm của DNS name server.
  - Các bản ghi giả có thể trỏ đến các nút của kẻ tấn công
  - Các nút của kẻ tấn công có thể giả mạo.
- ❖ Những trả lời không được yêu cầu sẽ không được chấp nhận tại một name server.
  - Các name server sử dụng ID trong thông điệp DNS để so khớp đáp ứng với truy vấn.
  - Do vậy, không thể chỉ chèn một bản ghi vào trong một name server bằng cách gửi một thông điệp đáp ứng DNS.
- ❖ Có thể gửi trả lời cho một yêu cầu.

2.8 Tấn công DNS

❑ Phá hoại máy chủ DNS cục bộ



Mục tiêu: Đặt địa chỉ IP giả cho uab.edu trong Berkeley DNS server cục bộ

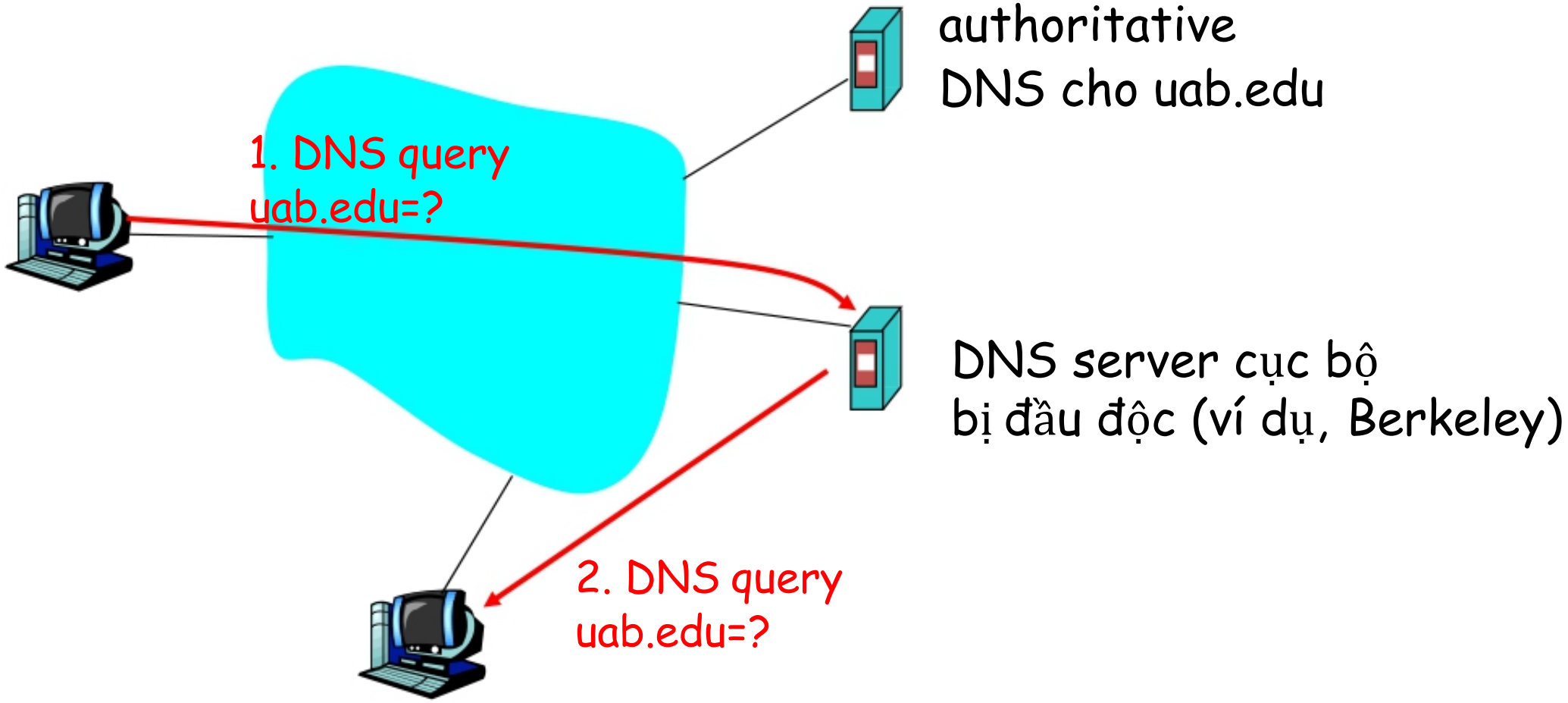
1) Kẻ tấn công truy vấn DNS server cục bộ

2) DNS cục bộ làm cho các truy vấn lặp lại

3) Kẻ tấn công đợi một thời gian; gửi một đáp ứng giả, lừa server thẩm quyền (authoritative server) cho uab.edu.

2.8 Tấn công DNS

❑ Phá hoại máy chủ DNS cục bộ



Đáp ứng DNS có thể cung cấp địa chỉ Ip của server độc hại !

2.8 Tấn công DNS

❑ Tóm tắt tấn công DNS

- ❖ DNS là một thành phần quan trọng của cơ sở hạ tầng Internet
- ❖ Nhưng rất đáng ngạc nhiên:
  - Các cuộc tấn công DDoS chống lại các servers gốc phần lớn là thành công.
  - Tấn công đầu độc và tấn công chuyển hướng là khó khăn trừ khi người dùng có thể sniff các yêu cầu DNS
    - Và thậm chí, có thể cần dừng DNS servers từ việc đáp ứng.
- ❖ DNS có thể được tận dụng cho các tấn công phản chiếu chống lại các nút không phải là DNS.

2.9 Tấn công Social Engineering

- Social engineering là kỹ thuật lợi dụng sự ảnh hưởng và niềm tin để lừa một người nào đó nhằm mục đích lấy cắp thông tin hoặc thuyết phục nạn nhân để thực hiện việc gì.
- Các kiểu tấn công
  - Dựa trên con người
    - Mạo danh qua các cuộc gọi hỗ trợ
    - Nghe trộm
    - Nhìn trộm
    - Tìm thông tin trong thùng rác
    - Ăn cắp các tài liệu
    - ....
  - Dựa trên máy tính
    - Cửa sổ pop-up
    - Giả mạo (Phishing)
    - Phần mềm giả danh
    - Trojan
    - SMS
    - Email
    - Chat

2.9 Tấn công Social Engineering

❑ Các kiểu tấn công

➢ Mạo danh

❖ Giả làm người sử dụng hợp pháp về nhân dạng và yêu cầu các thông tin nhạy cảm:

• Xin chào. Tôi là A, đang làm ở bộ phận X. Tôi đã quên mật khẩu email của tôi, nhờ anh đọc lại giúp tôi được không.

❖ Giả làm người sử dụng quan trọng: như thư ký giám đốc, khách hàng quan trọng

❖ Giả làm nhân viên hỗ trợ kỹ thuật và yêu cầu ID và mật khẩu để khôi phục dữ liệu

2.9 Tấn công Social Engineering

❑ Các kiểu tấn công

- **Nghe trộm**
  - ❖ Nghe trộm các cuộc điện thoại hoặc đọc tin nhắn trái phép
- **Nhìn trộm**
  - ❖ Nhìn trộm bàn phím khi người dùng đang nhập mật khẩu bằng cách nhìn sau lưng, hay thậm chí bằng ống nhòm, webcam
- **Tìm thông tin từ thùng rác**
  - ❖ Hóa đơn, thông tin liên lạc, thông tin tài chính, thông tin cá nhân

2.9 Tấn công Social Engineering

❑ Các kiểu tấn công

- **Piggybacking**
  - ❖ Giả vờ quên thẻ ở nhà để người khác rủ lòng thương được người có thẩm quyền cho phép được truy cập trái phép
- **Cửa sổ pop-up**
  - ❖ Lừa người dùng điền thông tin hoặc download phần mềm độc hại
- **Giả mạo (Phishing)**
  - ❖ Lừa đảo bằng cách giả mạo qua các phương tiện liên lạc như email, SMS

2.9 Tấn công Social Engineering

❑ Các kiểu tấn công

- **Phần mềm giả danh**
  - ❖ Giả dạng màn hình chờ hay phần mềm hợp lệ
- **Tấn công từ bên trong:**
  - ❖ Đối thủ cạnh tranh muốn gây thiệt hại bằng cách cài người của họ vào công ty
- **Nhân viên bất mãn**
  - ❖ Những nhân viên bất mãn với công ty có thể tự phá hoại hoặc bán thông tin cho công ty cạnh tranh
- **Nguy cơ từ mạng xã hội**

2.10 Tấn công Phishing, pharming

❑ Phishing và Pharming

❖ **Phishing** – giả mạo website

- Là một dạng của tấn công Social Engineering, lừa người dùng để lấy thông tin cá nhân, thông tin tài khoản, thẻ tín dụng,…
- Kẻ tấn công có thể giả mạo trang web của các tổ chức tài chính, ngân hàng (Có thể đơn giản thay .org thay vì .com)
- Chúng gửi email cho người dùng (địa chỉ email thu thập trên mạng), yêu cầu xác thực thông tin;
- Nếu người dùng làm theo hướng dẫn → cung cấp các thông tin cá nhân, thông tin tài khoản, thẻ tín dụng cho kẻ tấn công
- Do thiếu hiểu biết và tò mò

2.10 Tấn công Phishing, pharming

❑ Phishing và Pharming

❖ **Phishing** – giả mạo website

2.10 Tấn công Phishing, pharming

❑ Phishing và Pharming

❖ **Phishing** – giả mạo website

From: CustomerSecurity@royalbank.com[1]
Sent: Monday, July 20, 2009 7:54 PM
To: Rob.Smith@hotmail.com
Subject: Renew your Online Account with Royal Bank Immediately – Final reminder[2]

Royal Bank

Dear valued Royal Bank customer,[3]

It has come to our attention that you have not logged into your online banking account for some time[4] now and, as a security measure, we must to suspend your online account.[5] If you would like to continue to use the online banking facilty[6] offered by Royal Bank, please click the link below and renew your security details[7] immediately. Failure to do so will result in your online account being suspended.[8]

Renew your security details immediately and continue to use our online banking facilty:
https://customerbankingrenewal.royalbank.com/[9]

We are sorry for any convenience[10] caused and hope you continue to use our online banking facilty.

The Royal Bank Online Security Team[11]

Link: http://customerbankingrenewal.royalbank.com/

2.10 Tấn công Phishing, pharming

❑ Phishing và Pharming

❖ **Pharming** – là kiểu tấn công vào trình duyệt người dùng:

- Người dùng gõ địa chỉ 1 website, trình duyệt lại yêu cầu 1 website khác (độc hại);
- Kẻ tấn công thường sử dụng sâu, virus hoặc các phần mềm độc hại cài vào hệ thống để điều khiển trình duyệt của người dùng;
- Kẻ tấn công cũng có thể tấn công vào hệ thống DNS để thay đổi kết quả truy vấn: thay địa chỉ IP của website hợp pháp thành IP của website độc hại.

2.10 Tấn công Phishing, pharming

❑ Phishing và Pharming

❖ Pharming

Sửa đổi file hosts, hoặc điều khiển trình duyệt để chuyển hướng và giả mạo website