TẤN CÔNG MẠNG MÁY TÍNH

Giáo viên: PGS.TS. Nguyễn Hiếu Minh

Nội dung trình bày

1. Tổng quan về tấn công mạng
2. Các mô hình tấn công mạng
3. Một số kỹ thuật tấn công mạng

1. Tổng quan về tấn công mạng

A. ĐỊNH NGHĨA

- ✓ Hiện nay vẫn chưa có định nghĩa chính xác về thuật ngữ "tấn công" (xâm nhập, công kích). Mỗi chuyên gia trong lĩnh vực ATTT luận giải thuật ngữ này theo ý hiểu của mình. Ví dụ, "xâm nhập - là tác động bất kỳ đưa hệ thống từ trạng thái an toàn vào tình trạng nguy hiểm".
- ✓ Thuật ngữ này có thể giải thích như sau: "xâm nhập - đó là sự phá huỷ chính sách ATTT" hoặc "là tác động bất kỳ dẫn đến việc phá huỷ tính toàn vẹn, tính bí mật, tính sẵn sàng của hệ thống và thông tin xử lý trong hệ thống".

Định nghĩa

- ***Tấn công (attack) là hoạt động có chủ ý của kẻ phạm tội lợi dụng các thương tổn của hệ thống thông tin và tiến hành phá vỡ tính sẵn sàng, tính toàn vẹn và tính bí mật của hệ thống thông tin.***

Tổng quan

- Tấn công (*attack, intrustion*) mạng là các tác động hoặc là trình tự liên kết giữa các tác động với nhau để phá huỷ, dẫn đến việc hiện thực hoá các nguy cơ bằng cách lợi dụng đặc tính dễ bị tổn thương của các hệ thống thông tin này.
  - Có nghĩa là, nếu có thể bài trừ nguy cơ thương tổn của các hệ thông tin chính là trừ bỏ khả năng có thể thực hiện tấn công.

Một số phương thức tấn công

- Phân loại

1) Tấn công thăm dò.
2) Tấn công sử dụng mã độc.
3) Tấn công xâm nhập mạng.
4) Tấn công từ chối dịch vụ.

- Hoặc:

1) Tấn công chủ động.
2) Tấn công thụ động.

Một số khái niệm cơ bản

1. Người thực hiện tấn công

- Người thực hiện các tấn công mạng thường là những người có hiểu biết sâu sắc về giao thức TCP/IP, có hiểu biết về hệ điều hành, có thể sử dụng thành thạo một số ngôn ngữ lập trình.

  - Các hướng tấn công:

    ✓ Tấn công từ bên trong mạng.

    ✓ Tấn công từ bên ngoài mạng.

Tấn công bên trong mạng

- *Tấn công không chủ ý*: Nhiều hư hại của mạng do người dùng trong mạng vô ý gây nên. Những người này có thể vô ý để hacker bên ngoài hệ thống lấy được password hoặc làm hỏng các tài nguyên của mạng do thiếu hiểu biết.
- *Tấn công có chủ ý*: Kẻ tấn có chủ ý chống lại các qui tắc, các qui định do các chính sách an ninh mạng đưa ra.

Tấn công từ ngoài mạng

- *Kẻ tấn công nghiệp dư ("script-kiddy")*: Dùng các script đã tạo sẵn và có thể tạo nên các các thiệt hại đối với mạng.
- *Kẻ tấn công đích thực ("true- hacker")*: Mục đích chính của nhóm người này khi thực hiện các tấn công mạng là để mọi người thừa nhận khả năng của họ và để được nổi tiếng.
- *Kẻ tấn công chuyên nghiệp ("the elite")*: Thực hiện các tấn công mạng là để thu lợi bất chính.

Một số khái niêm cơ bản

2. Thời điểm thực hiện tấn công

- Bất kỳ.
- Thường thực hiện về đêm.

3. Hệ điều hành sử dụng để tấn công

- Bất kỳ.
- Thường sử dụng các HĐH mã nguồn mở.

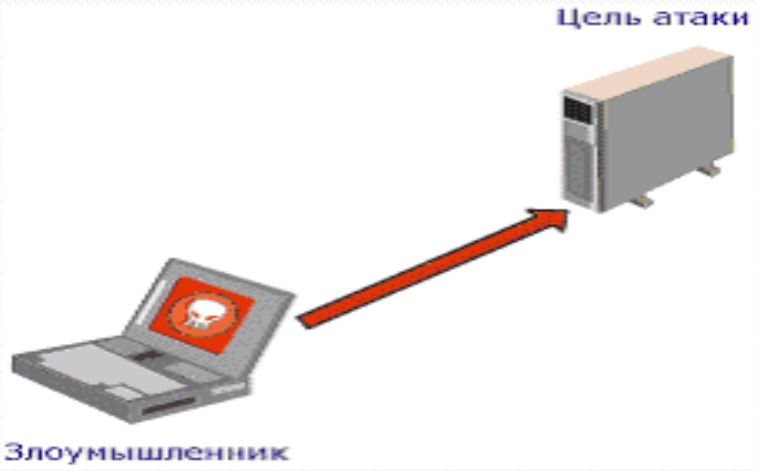
4. Các hệ thống mục tiêu

- Con người, phần cứng, phần mềm.

2. Các mô hình tấn công mạng

1. Mô hình tấn công truyền thống

- Mô hình tấn công truyền thống được tạo dựng theo nguyên tắc "một đến một" hoặc "một đến nhiều", có nghĩа là cuộc tấn công xảy ra từ một nguồn gốc.
- Mô tả: Tấn công "một đến một"

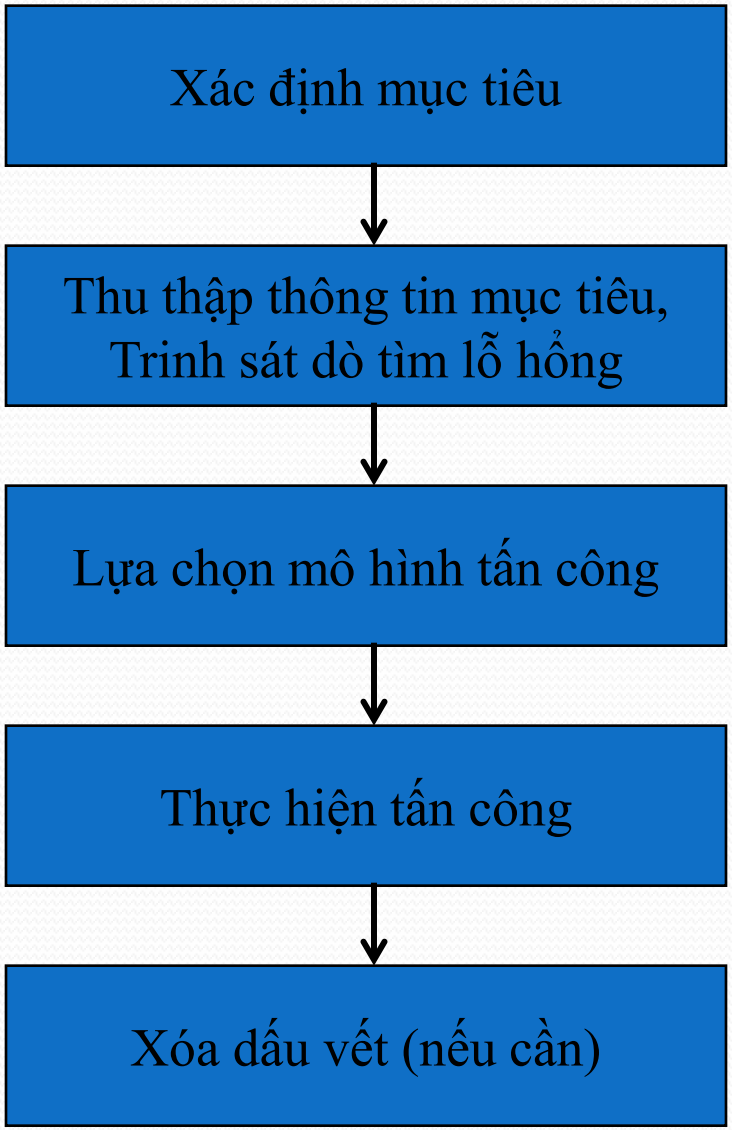


Mô hình tấn công phân tán

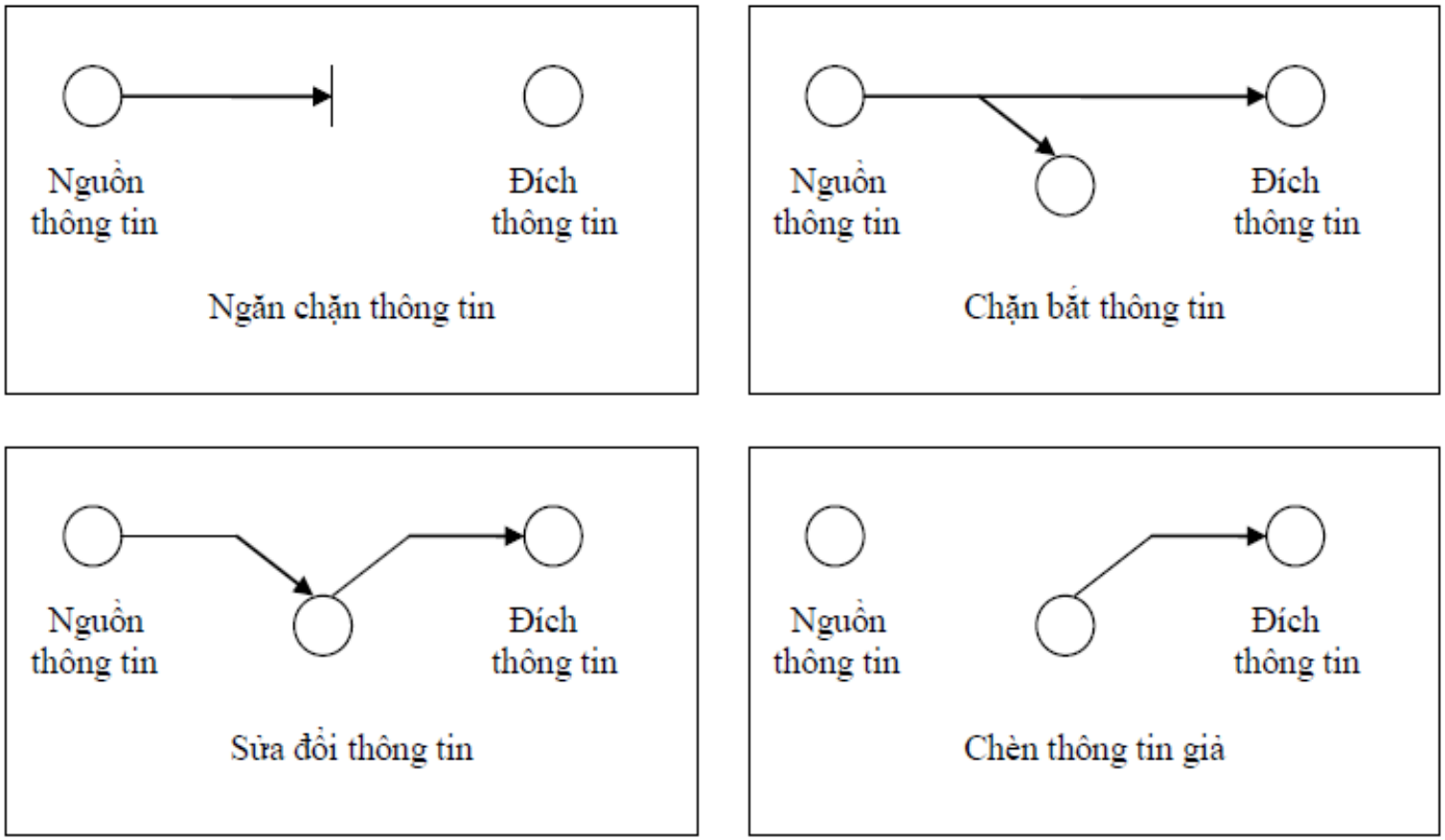
2. Mô hình tấn công phân tán

- Khác với mô hình truyền thống trong mô hình tấn công phân tán sử dụng quan hệ "nhiều đến một" và "nhiều đến nhiều".
- Tấn công phân tán dựa trên các cuộc tấn công "cổ điển" thuộc nhóm "từ chối dịch vụ", chính xác hơn là dựa trên các cuộc tấn công như Flood hay Storm (những thuật ngữ trên có thể hiểu tương đương như "bão", "lũ lụt" hay "thác tràn").

3. Các bước tấn công



Các tấn công đối với thông tin trên mạng



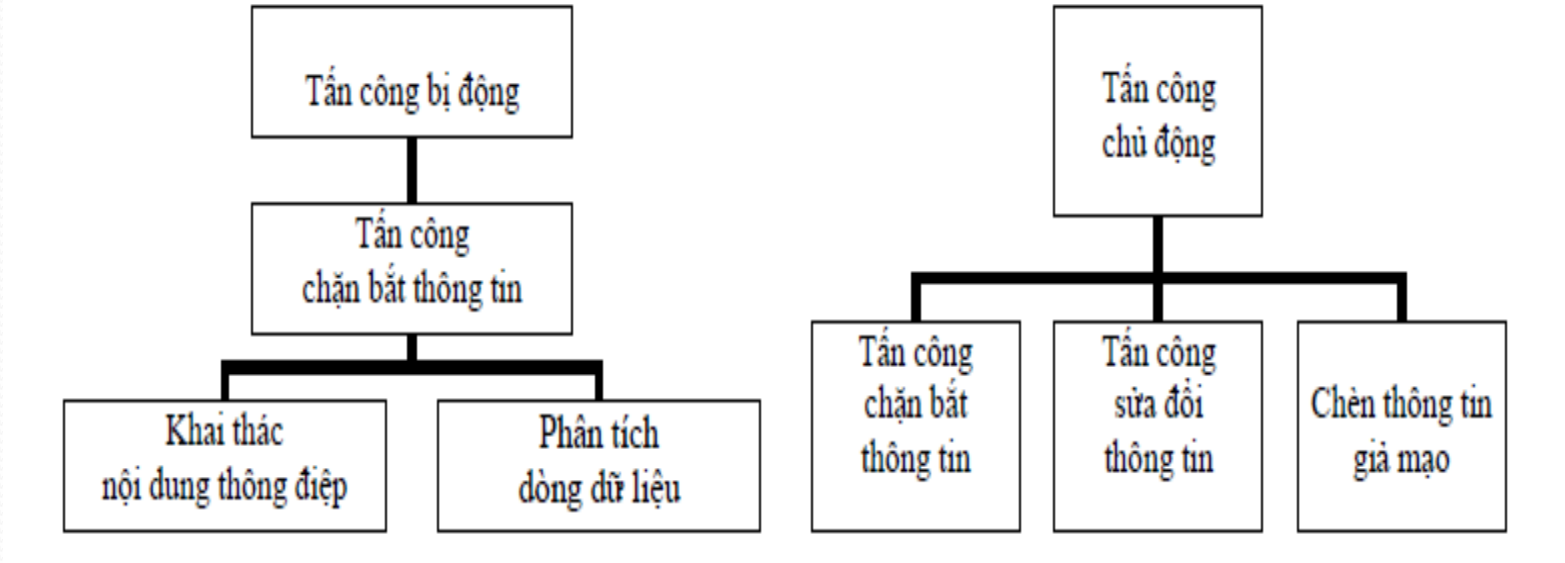
Các tấn công đối với thông tin trên mạng

- **Tấn công ngăn chặn thông tin (interruption)**
- Tài nguyên thông tin bị phá hủy, không sẵn sàng phục vụ hoặc không sử dụng được. Đây là hình thức tấn công làm mất khả năng sẵn sàng phục vụ của thông tin.
- **Tấn công chặn bắt thông tin (interception)**
- Kẻ tấn công có thể truy nhập tới tài nguyên thông tin. Đây là hình thức tấn công vào tính bí mật của thông tin.

Các tấn công đối với thông tin trên mạng

- **Tấn công sửa đổi thông tin (Modification)**
  - Kẻ tấn công truy nhập, chỉnh sửa thông tin trên mạng.
  - Đây là hình thức tấn công vào tính toàn vẹn của thông tin.
- **Chèn thông tin giả mạo (Fabrication)**
  - Kẻ tấn công chèn các thông tin và dữ liệu giả vào hệ thống.
  - Đây là hình thức tấn công vào tính xác thực của thông tin.

Tấn công bị động (passive attacks) và chủ động (active attacks)



Tấn công bị động (passive attacks)

- Mục đích của kẻ tấn công là biết được thông tin truyền trên mạng.
- Có hai kiểu tấn công bị động là khai thác nội dung thông điệp và phân tích dòng dữ liệu.
- Tấn công bị động rất khó bị phát hiện vì nó không làm thay đổi dữ liệu và không để lại dấu vết rõ ràng. Biện pháp hữu hiệu để chống lại kiểu tấn công này là ngăn chặn (đối với kiểu tấn công này, ngăn chặn tốt hơn là phát hiện).

Tấn công chủ động (active attacks)

- Tấn công chủ động được chia thành 4 loại nhỏ sau:
  - Giả mạo (Masquerade): Một thực thể (người dùng, máy tính, chương trình…) đóng giả thực thể khác.
  - Dùng lại (replay): Chặn bắt các thông điệp và sau đó truyền lại nó nhằm đạt được mục đích bất hợp pháp.
  - Sửa thông điệp (Modification of messages): Thông điệp bị sửa đổi hoặc bị làm trễ và thay đổi trật tự để đạt được mục đích bất hợp pháp.
  - Từ chối dịch vụ (Denial of Service - DoS): Ngăn cấm việc sử dụng bình thường hoặc quản lý các tiện ích truyền thông.

3. Một số kỹ thuật tấn công mạng

1) Tấn công thăm dò.
2) Tấn công sử dụng mã độc.
3) Tấn công xâm nhập mạng.
4) Tấn công từ chối dịch vụ.

1) Tấn công thăm dò

- Thăm dò là việc thu thập thông tin trái phép về tài nguyên, các lỗ hổng hoặc dịch vụ của hệ thống.
- Tấn công thăm dò thường bao gồm các hình thức:
  - Sniffing
  - Ping Sweep
  - Ports Scanning

(a) Sniffing (Nghe lén)

- Sniffer là một hình thức nghe lén trên hệ thống mạng dựa trên những đặc điểm của cơ chế TCP/IP.
- Sniffer ban đầu là một kỹ thuật bảo mật, được phát triển nhằm giúp các nhà quản trị mạng khai thác mạng hiệu quả hơn, và có thể kiểm tra các dữ liệu ra vào mạng cũng như các dữ liệu trong mạng (kiểm tra lỗi).
- Sau này, hacker dùng phương pháp này để lấy cắp mật khẩu hay các thông tin nhạy cảm khác.
  - Biến thể của sniffer là các chương trình nghe lén bất hợp pháp như: công cụ nghe lén yahoo, ăn cắp password email…

Active sniffer

- Môi trường hoạt động: Chủ yếu hoạt động trên các mạng sử dụng thiết bị chuyển mạch (switch).
- Cơ chế hoạt động: Thay đổi đường đi của dòng dữ liệu, áp dụng cơ chế ARP và RARP (hai cơ chế chuyển đổi từ IP sang MAC và từ MAC sang IP) bằng cách phát đi các gói tin đầu độc.
- Đặc điểm: Do phải gửi gói tin đi nên chiếm băng thông của mạng, nếu sniff quá nhiều trong mạng thì lượng gói tin gửi đi sẽ rất lớn (do liên tục gửi đi các thông tin giả mạo) có thể dẫn tới nghẽn mạng hay gây quá tải lên chính NIC của máy (thắt nút cổ chai)

Active sniffer

- Một số kỹ thuật ép dòng dữ liệu đi qua NIC của mình như:
  - ARP poisoning: thay đổi thông tin ARP
  - MAC flooding: làm tràn bộ nhớ switch, từ đó switch sẽ chạy chế độ forwarding mà không chuyển mạch gói.
  - Giả MAC: các sniffer sẽ thay đổi MAC của mình thành một MAC của một máy hợp lệ và qua được chức năng lọc MAC của thiết bị.
  - Đầu độc DHCP để thay đổi gateway của máy client.
  - DNS spoofing: làm phân giải sai tên miền.

Passtive sniffer

- Môi trường hoạt động: Chủ yếu hoạt động trong môi trường không có thiết bị switch mà dùng hub.
- Cơ chế hoạt động: Hoạt động dựa trên cơ chế broadcast gói tin trong mạng; do không có thiết bị switch nên các các gói tin được broadcast đi trong mạng; có thể bắt các gói tin lại để xem (dù host nhận gói tin không phải là nơi gói tin đó gửi tới)
- Đặc điểm: Do máy tự broadcast gói tin nên hình thức Passtive sniff này rất khó phát hiện.

So sánh

- Acctive:
  - Môi trường mạng sử dụng switch.
  - Đầu độc ARP.
- Passive:
  - Môi trường mạng sử dụng hub.
  - Broadcast gói tin.
- **Một số công cụ sniffer**
  - Ettercap
  - Cain & Abel
  - HTTP sniffer
  - …

Phát hiện và phòng chống sniff

- Dựa vào quá trình đầu độc ARP của sniff để phát hiện:
  - Vì phải đầu độc ARP nên sniffer sẽ liên tục gửi gói tin đầu độc tới các victim. Do đó ta có thể dùng các công cụ bắt gói tin trong mạng để phát hiện
  - Một cách khác ta có thể kiểm tra bảng ARP của host. Nếu thấy trong bảng APR có 2 MAC giống nhau thì có thể mạng đang bị sniffer.

Phát hiện và phòng chống sniff

- Dựa trên băng thông:
  - Do quá trình gửi gói tin đầu độc của sniffer nên quá trình này có thể chiếm băng thông từ đây có thể dùng một số công cụ kiểm tra băng thông để phát hiện.
- Các công cụ phát hiện sniffer:
  - Xarp
  - ARPwatch
  - Simantec endpoint protection

Phòng chống Active sniff

- Người quản trị:
  - Công cụ:
    - Kiểm tra băng thông.
    - Bắt các gói tin.
  - Thiết bị:
    - Dùng các loại thiết bị có chức năng lọc MAC.
    - Với mạng switch có thể dùng thêm chức năng VLAN trunking, kết hợp thêm chức năng port security (tương đối hiệu quả trong mô hình mạng VLAN và kết hợp thêm tính bảo mật).
- Người dùng:
  - Sử dụng ARP dạng tĩnh.
  - Dùng các công cụ phát hiện sniffer để cảnh báo cho người dùng.

Phòng chống Passive sniff

- Dạng snif này khó phát hiện cũng như phòng chống.
- Thay hub bằng switch lúc đó các gói tin không còn broadcast nữa.

(b) Ping sweep

- Ping: Đưa ra một gói yêu cầu ICMP và đợi trả một thông báo trả lời từ một máy hoạt động.
- Ping Sweep: Xác định hệ thống đang "sống" hay không rất quan trọng vì có thể hacker ngừng ngay tấn công khi xác định hệ thống đó đã "chết". Việc xác định trạng thái hệ thống có thể sử dụng kỹ thuật Ping Scan hay còn gọi với tên Ping Sweep.
- Bản chất của quá trình này là gửi một ICMP Echo Request đến máy chủ mà hacker đang muốn tấn công và mong đợi một ICMP Reply.
- Ngoài lệnh ping có sẵn trên Windows, còn có một số công cụ ping sweep như: Pinger, Friendly Pinger, Ping Pro…

(c) Ports scanning

- **Khái niệm**
  - Port scanning là một quá trình kết nối các cổng (TCP và UDP) trên một hệ thống mục tiêu nhằm xác định xem dịch vụ nào đang "chạy" hoặc đang trong trạng thái "nghe". Xác định các cổng nghe là một công việc rất quan trọng nhằm xác định được loại hình hệ thống và những ứng dụng đang được sử dụng.
- **Chức năng**
  - Xác định máy đang mở cổng nào.
  - Xác định hệ thống đang sử dụng dịch vụ nào.

Hoạt động Ports scanning

- Mỗi công cụ có cơ chế port scan riêng.
- Ví dụ: hoạt động của công cụ Nmap.
  - Nmap hỗ trợ nhiều kỹ thuật scan port như: TCP scan, SYN scan, Null scan, Windows scan, ACK scan…
  - Ví dụ TCP scan: kỹ thuật TCP scan tức là Nmap sẽ kiểm tra cổng trên hệ thống đích mở hay đóng bằng cách thực hiện kết nối TCP đầy đủ.
- **Một số công cụ Ports scanning**
  - Nmap
  - Super scan

2. Tấn công xâm nhập (access attack)

- Tấn công xâm nhập là một thuật ngữ rộng miêu tả bất kỳ kiểu tấn công nào đòi hỏi người xâm nhập lấy được quyền truy cập trái phép của một hệ thống bảo mật với mục đích thao túng dữ liêu, nâng cao đặc quyền.
- Tấn công truy nhập hệ thống: Là hành động nhằm đạt được quyền truy cập bất hợp pháp đến một hệ thống mà ở đó hacker không có tài khoản sử dụng.
- Tấn công truy nhập thao túng dữ liệu: Kẻ xâm nhập đọc, viết, xóa, sao chép hay thay đổi dữ liệu.

3. Tấn công từ chối dịch vụ (DoS)

- Về cơ bản, tấn công từ chối dịch vụ là tên gọi chung của cách tấn công làm cho một hệ thống nào đó bị quá tải không thể cung cấp dịch vụ, làm gián đoạn hoạt động của hệ thống hoặc hệ thống phải ngưng hoạt động.
- Tùy theo phương thức thực hiện mà nó được biết dưới nhiều tên gọi khác nhau. Khởi thủy là lợi dụng sự yếu kém của giao thức TCP (Transmision Control Protocol) để thực hiện tấn công từ chối dịch vụ DoS (Denial of Service), mới hơn là tấn công từ chối dịch vụ phân tán DDoS (Distributed DoS), mới nhất là tấn công từ chối dịch vụ theo phương pháp phản xạ DRDoS (Distributed Reflection DoS).

(a) Tấn công từ chối dịch vụ cổ điển DoS (Denial of Service)

- Bom thư
- Đăng nhập liên tiếp
- Làm ngập SYN (Flooding SYN)
- Tấn công Smurf
- Tấn công gây lụt UDP
- Tấn công ping of death
- Tấn công tear drop

SYN Attack

- Được xem là một trong những kiểu tấn công DoS kinh điển nhất. Lợi dụng sơ hở của thủ tục TCP khi "bắt tay ba bước", mỗi khi client muốn thực hiện kết nối với server thì nó thực hiện việc bắt tay ba bước thông qua các gói tin (packet)
- Bước 1: client sẽ gửi gói tin (packet chứa SYN=1) đến máy chủ để yêu cầu kết nối.

SYN Attack

- Bước 2: khi nhận được gói tin này, server gửi lại gói tin SYN/ACK để thông báo cho client biết là nó đã nhận được yêu cầu kết nối và chuẩn bị tài nguyên cho việc yêu cầu này. Server sẽ dành một phần tài nguyên để nhận và truyền dữ liệu. Ngoài ra, các thông tin khác của client như địa chỉ IP và cổng (port) cũng được ghi nhận.
- Bước 3: cuối cùng client hoàn tất việc bắt tay ba bước bằng cách hồi âm lại gói tin chứa ACK cho server và tiến hành kết nối.

SYN Attack

- Do TCP là thủ tục tin cậy trong việc giao nhận nên trong lần bắt tay thứ hai, server gửi gói tin SYN/ACK trả lời lại client mà không nhận lại được hồi âm của client để thực hiện kết nối thì nó vẫn bảo lưu nguồn tài nguyên chuẩn bị kết nối đó và lặp lại việc gửi gói tin SYN/ACK cho client đến khi nhận được hồi đáp của client.
- Điểm mấu chốt ở đây là làm cho client không hồi đáp cho Server, và có càng nhiều, càng nhiều client như thế trong khi server vẫn lặp lại việc gửi packet đó và giành tài nguyên để chờ trong lúc tài nguyên của hệ thống là có giới hạn. Các hacker tấn công sẽ tìm cách để đạt đến giới hạn đó.

SYN Attack

- Thường, để giả địa chỉ IP, các hacker hay dùng Raw Sockets (không phải gói tin TCP hay UDP) để giả mạo hay ghi đè giả lên IP gốc của gói tin. Khi một gói tin SYN với IP giả mạo được gửi đến server, nó cũng như bao gói tin khác, vẫn hợp lệ đối với server và server sẽ cấp vùng tài nguyên cho đường truyền này, đồng thời ghi nhận toàn bộ thông tin và gửi gói SYN/ACK ngược lại cho client.
- Vì địa chỉ IP của client là giả mạo nên sẽ không có client nào nhận được SYN/ACK packet này để hồi đáp cho máy chủ. Sau một thời gian không nhận được gói tin ACK từ client, server nghĩ rằng gói tin bị thất lạc nên lại tiếp tục gửi tiếp SYN/ACK, cứ như thế, các kết nối tiếp tục mở.

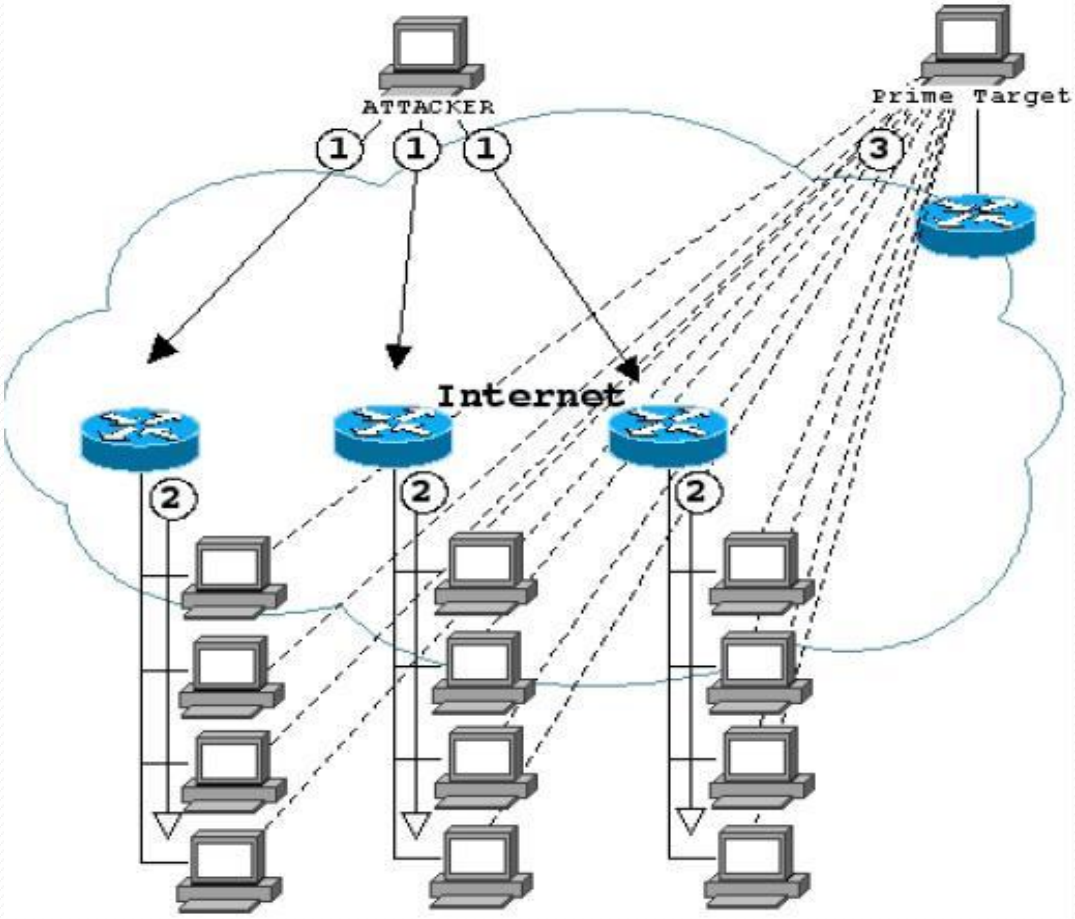
Flood attack

- Một kiểu tấn công DoS nữa cũng rất hay được dùng vì tính đơn giản của nó và vì có rất nhiều công cụ sẵn có hỗ trợ đắc lực cho kẻ tấn công là Flood Attack, chủ yếu thông qua các website.
- Về nguyên tắc, các website đặt trên máy chủ khi chạy sẽ tiêu tốn một lượng tài nguyên nhất định của máy chủ. Dựa vào đặc điểm đó, những kẻ tấn công dùng các phần mềm như smurf chẳng hạn để liên tục yêu cầu máy chủ phục vụ trang web đó để chiếm dụng tài nguyên.

Smurf attack

- Thủ phạm sinh ra cực nhiều giao tiếp ICMP (ping) tới địa chỉ Broadcast của các mạng với địa chỉ nguồn là mục tiêu cần tấn công.
- Khi ping tới một địa chỉ là quá trình hai chiều – Khi máy A ping tới máy B máy B reply lại hoàn tất quá trình. Khi ping tới địa chỉ Broadcast của mạng nào đó thì toàn bộ các máy tính trong mạng đó sẽ Reply lại. Nhưng nếuthay đổi địa chỉ nguồn (máy C) và ping tới địa chỉ Broadcast của một mạng nào đó, thì toàn bộ các máy tính trong mạng đó sẽ reply lại vào máy C và đó là tấn công Smurf.

Smurf attack



(b) Tấn công dịch vụ phân tán DDoS

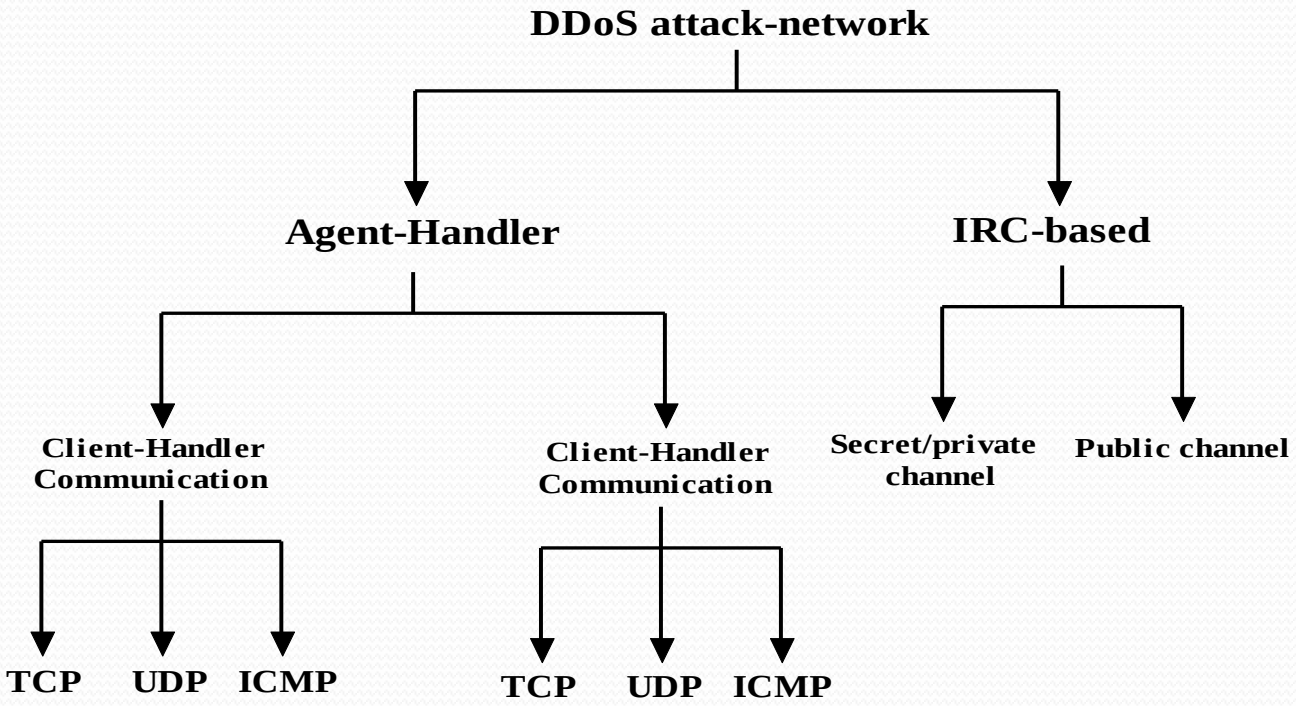
- Xuất hiện vào năm 1999, so với tấn công DoS cổ điển, sức mạnh của DDoS cao hơn gấp nhiều lần.
- Hầu hết các cuộc tấn công DDoS nhằm vào việc chiếm dụng băng thông (bandwidth) gây nghẽn mạch hệ thống dẫn đến hệ thống ngưng hoạt động.
- Để thực hiện thì kẻ tấn công tìm cách chiếm dụng và điều khiển nhiều máy tính/mạng máy tính trung gian (đóng vai trò zombie) từ nhiều nơi để đồng loạt gửi ào ạt các gói tin với số lượng rất lớn nhằm chiếm dụng tài nguyên và làm tràn ngập đường truyền của một mục tiêu xác định nào đó.

DDoS

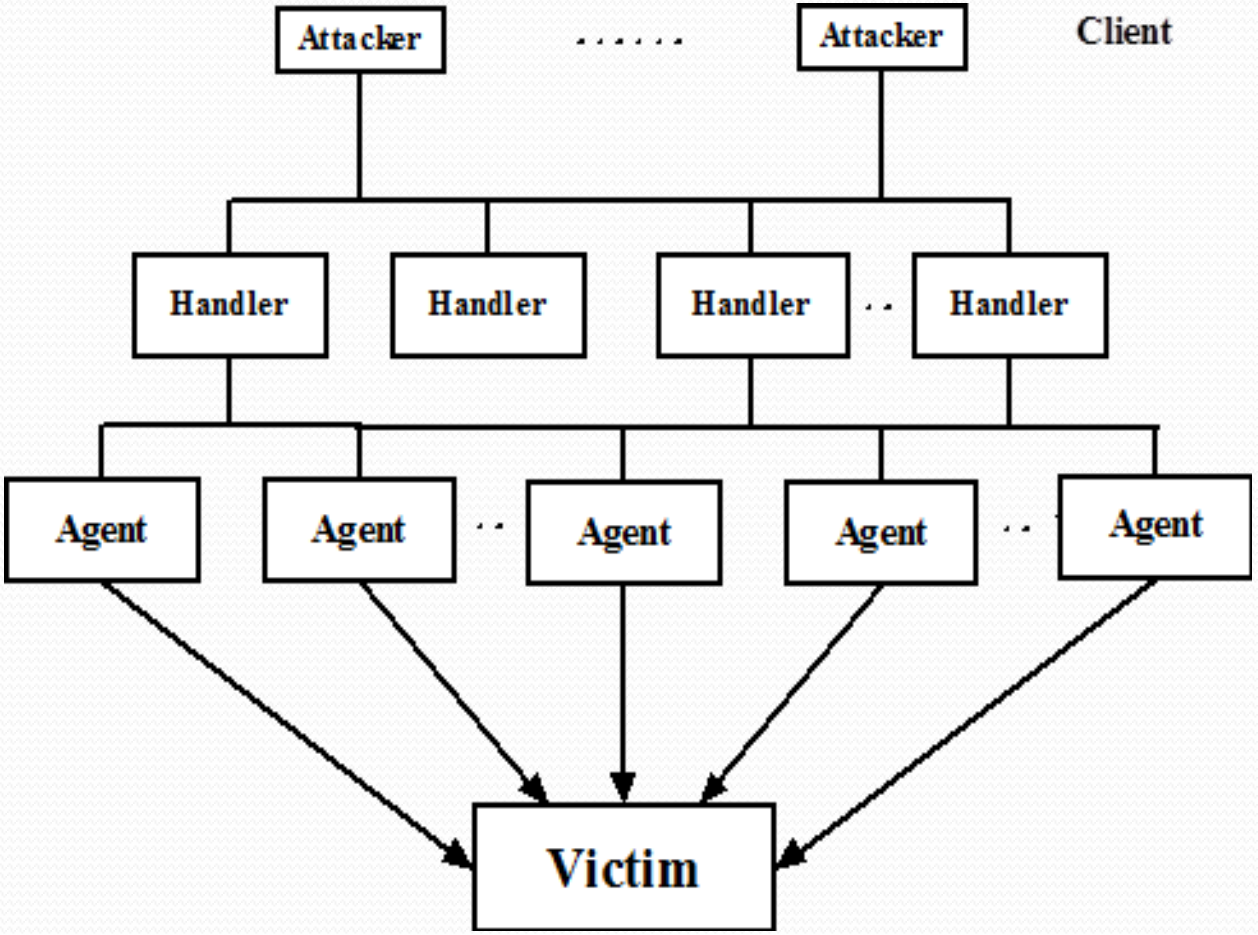
- Các giai đoạn của một cuộc tấn công kiểu DDoS:
  - *Giai đoạn chuẩn bị.*
  - *Giai đoạn xác định mục tiêu và thời điểm.*
  - *Phát động tấn công.*
  - *Xoá dấu vết.*

Kiến trúc tổng quan của DDoS attack-network

- *Mô hình Agent-Handler và Mô hình IRC-based.*



Mô hình Agent-Handler



Mô hình Agent-Handler

- Theo mô hình này, attack-network gồm 3 thành phần: Agent, Client và Handler
- Client: Là software cơ sở để hacker điều khiển mọi hoạt động của attack-network
- Handler: Là một thành phần software trung gian giữa Agent và Client
- Agent: Là thành phần software thực hiện sự tấn công mục tiêu, nhận điều khiển từ Client thông qua các Handler

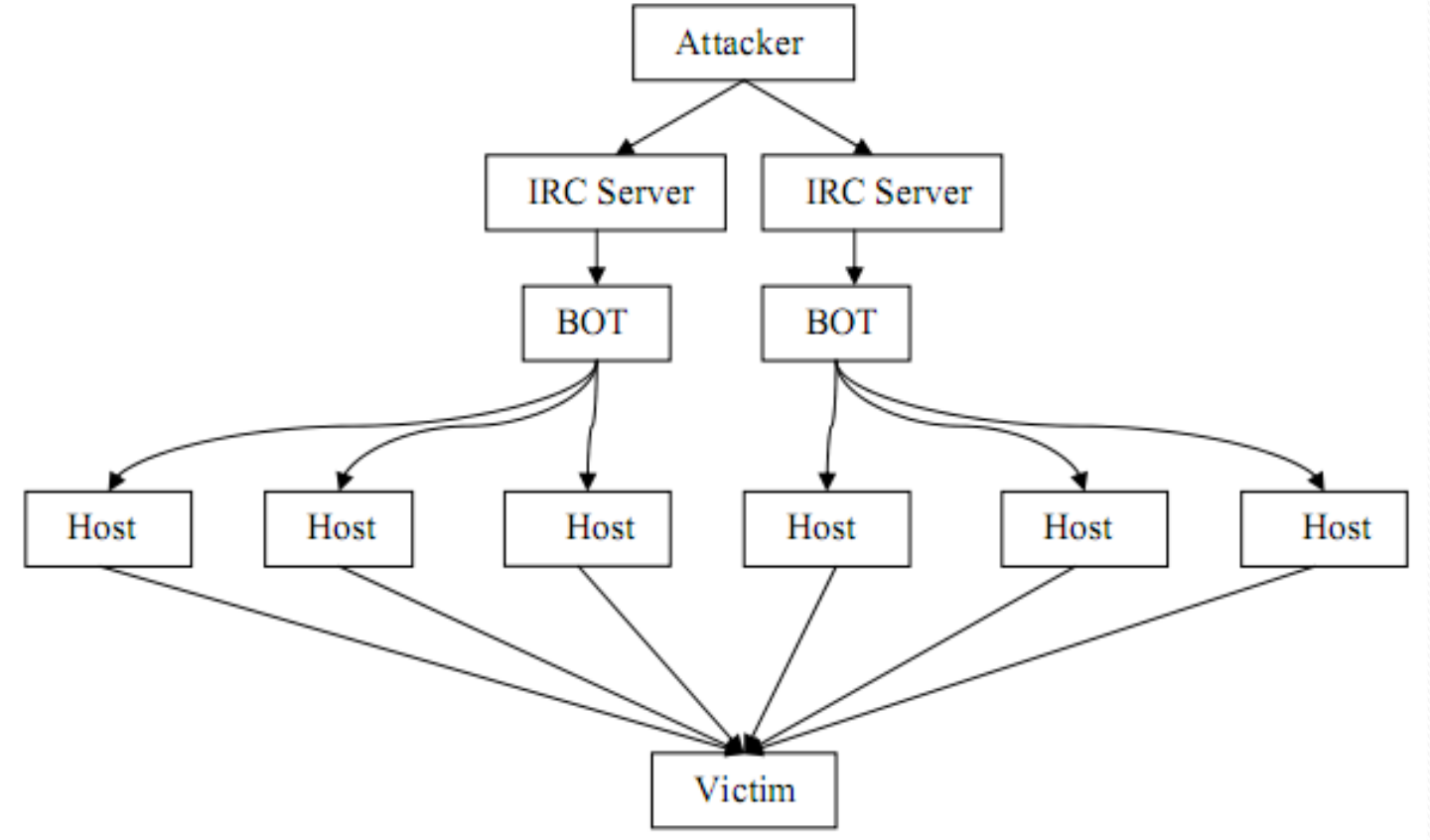
Mô hình IRC – Based

- Internet Relay Chat (IRC) là một hệ thống online chat multiuser, IRC cho phép user tạo một kết nối đến đa điểm (multipoint) đến nhiều user khác và chat thời gian thực.
- Kiến trúc của mạng IRC (IRC network) bao gồm nhiều IRC server trên khắp internet, giao tiếp với nhau trên nhiều kênh (channel).
- IRC network cho phép user tạo ba loại kênh: public, private và serect.

Mô hình IRC – Based

- Public channel: Cho phép user của kênh đó thấy IRC name và nhận được message của mọi user khác trên cùng kênh.
- Private channel: Được thiết kế để giao tiếp với các đối tượng cho phép. Không cho phép các user không cùng channel thấy IRC name và message trên channel. Tuy nhiên, nếu user ngoài channel dùng một số lệnh channel locator thì có thể biết được sự tồn tại của private channel đó.
- Secrect channel: Tương tự private channel nhưng không thể xác định bằng channel locator.

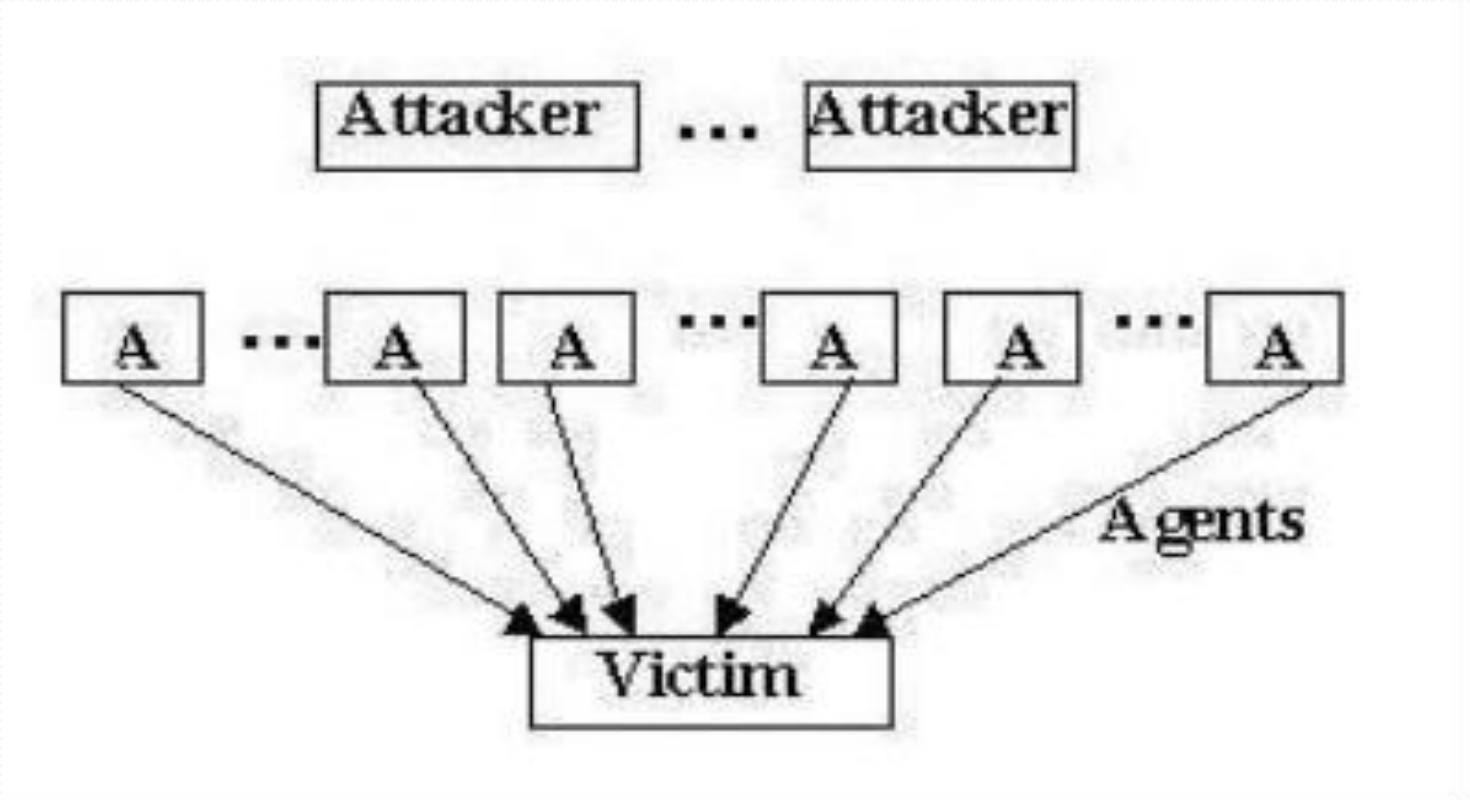
Mô hình IRC – Based



Mô hình IRC – Based

- IRC – Based network cũng tương tự như Agent – Handler network nhưng mô hình này sử dụng các kênh giao tiếp IRC làm phương tiện giao tiếp giữa Client và Agent (không sử dụng Handler).
- Sử dụng mô hình này, attacker còn có thêm một số lợi thế khác như:
  - Các giao tiếp dưới dạng chat message làm cho việc phát hiện chúng là vô cùng khó khăn.
  - IRC traffic có thể di chuyển trên mạng với số lượng lớn mà không bị nghi ngờ.
  - Không cần phải duy trì danh sách các Agent, hacker chỉ cần log on vào IRC server là đã có thể nhận được report về trạng thái các Agent do các channel gửi về.
  - IRC cũng là một môi trường file sharing tạo điều kiện phát tán các Agent code lên nhiều máy khác.

Mô hình Scattered



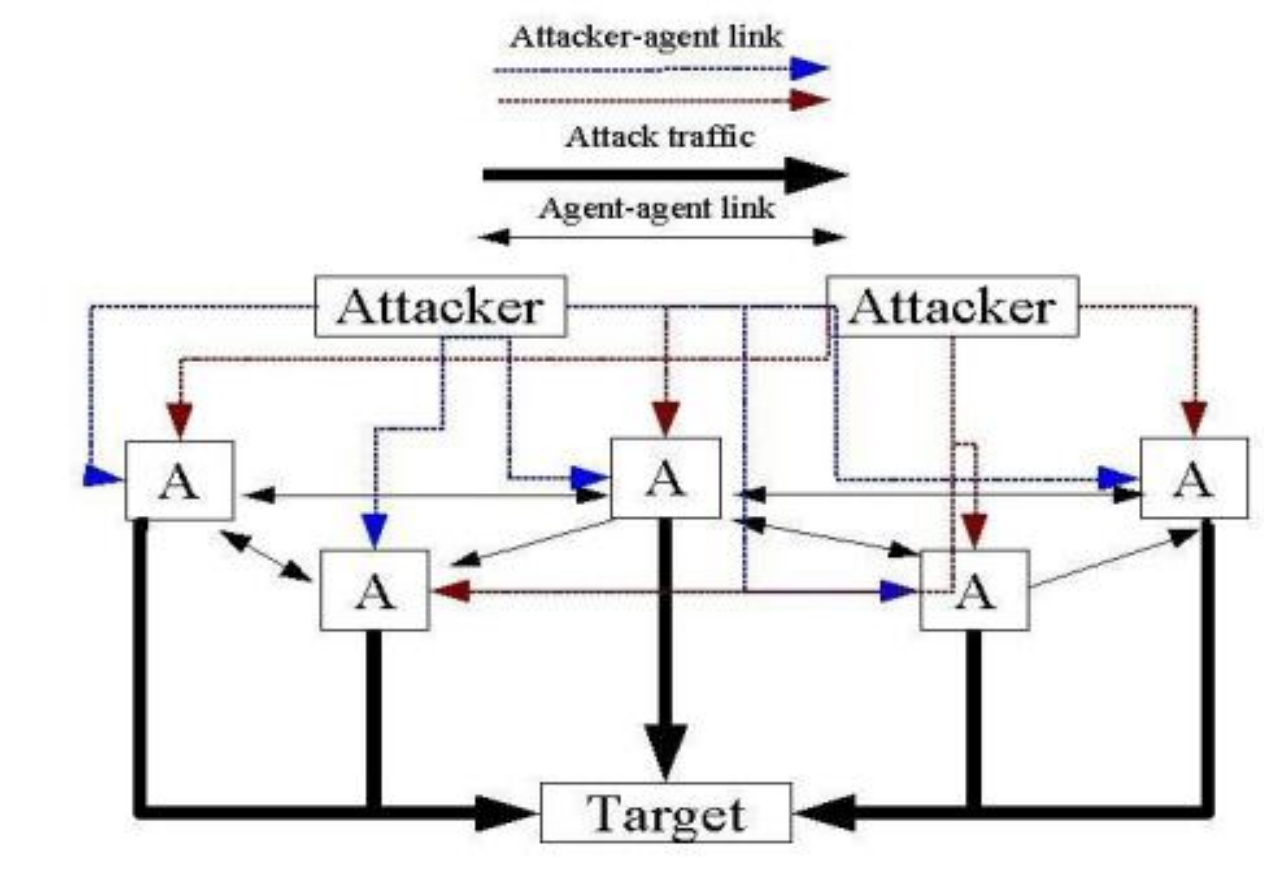
Mô hình Scattered

- Mô hình tán xạ khác với các mô hình DDoS khác đó là nó không có bất kỳ sự liên lạc đầy đủ có nghĩa là các node của mạng phân tán có nghĩa là các chúng không biết nhau một cách đầy đủ.
- Mặc dù Attacker thường không biết được vị trí của các node. Topo của các node là tự ý được xác định và chỉ được liên kế tới đích thông qua traffic tấn công cũng có nghĩa là nó không sinh ra các traffic nào khác.
- Theo nghĩa khác mạng DDOS của mô Scattered được xây dựng có sự độc lập của các Agent.

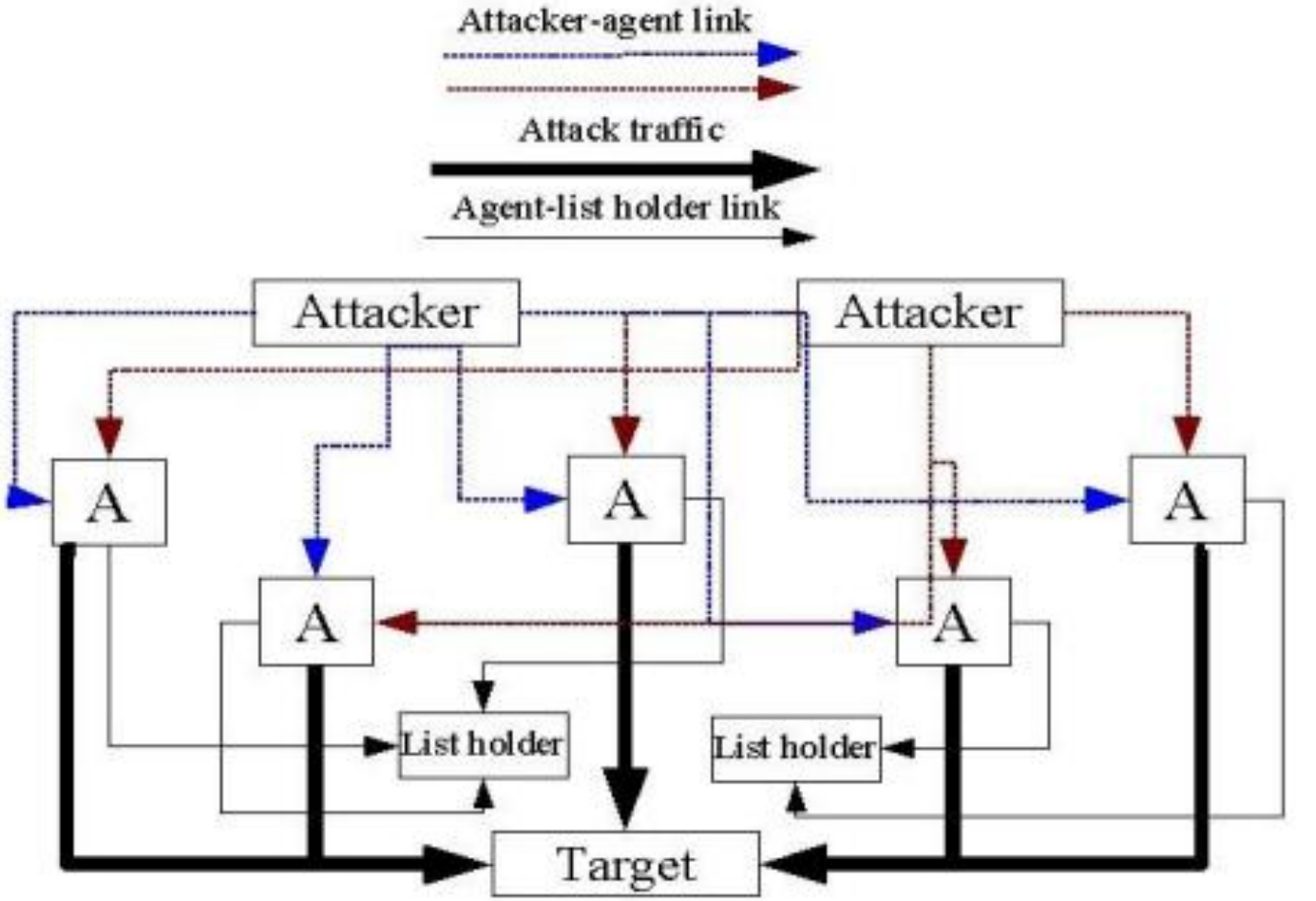
Mô hình peer to peer

- Mô hình này có nhiều đặc điểm thuận lợi hơn so với các mô hình trước.
- Mô hình này có nguyên lý của mạng peer to peer.
- Một mạng phân tán có cấu trúc được gọi là mạng Peer to peer nếu những người tham gia chia sẻ một phần tài nguyên phần cứng của họ (sức mạnh xử lý, khả năng lưu trữ, khả năng kết nối mạng, máy in).

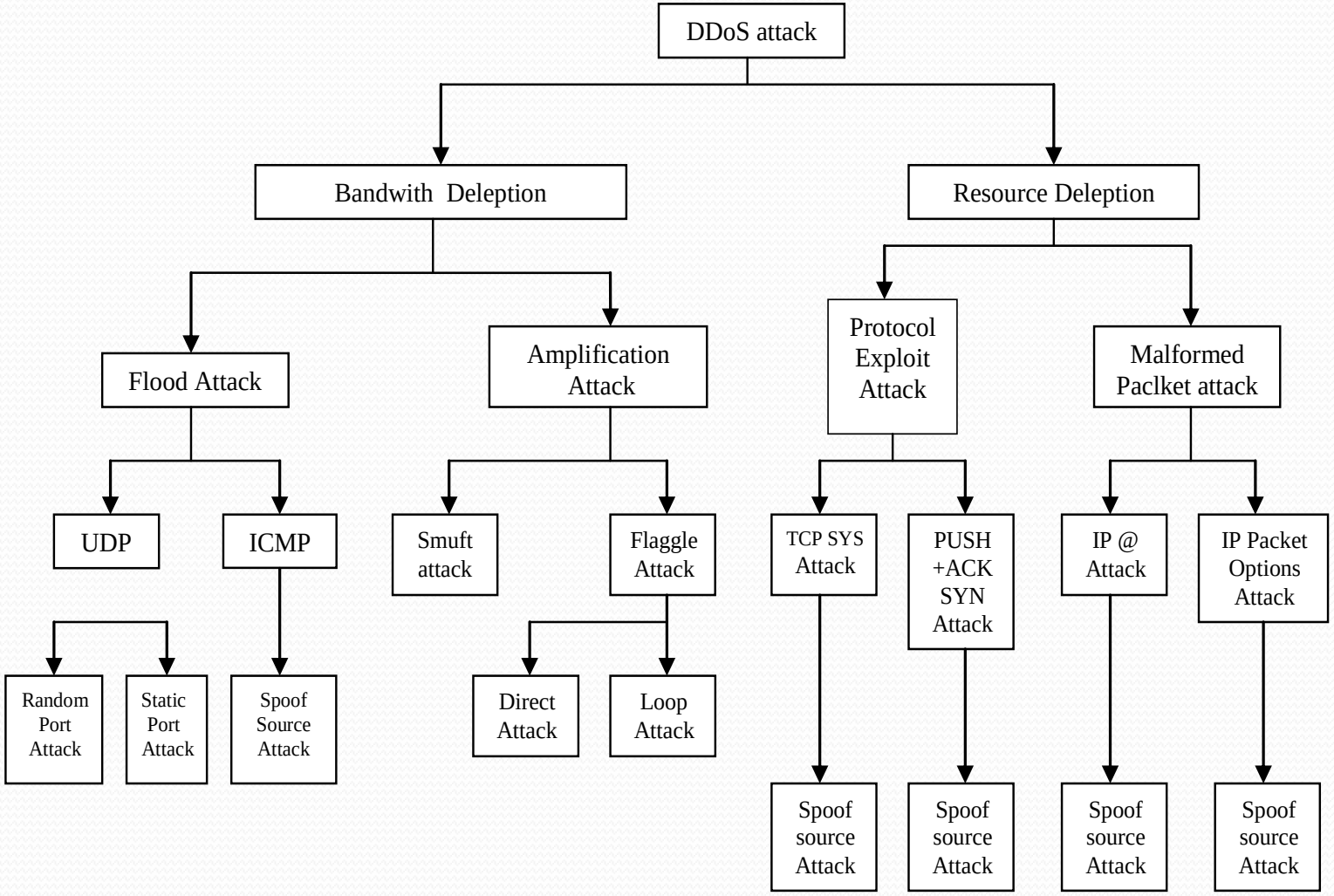
Mô hình pure peer to peer



Mô hình hybrid peer to peer



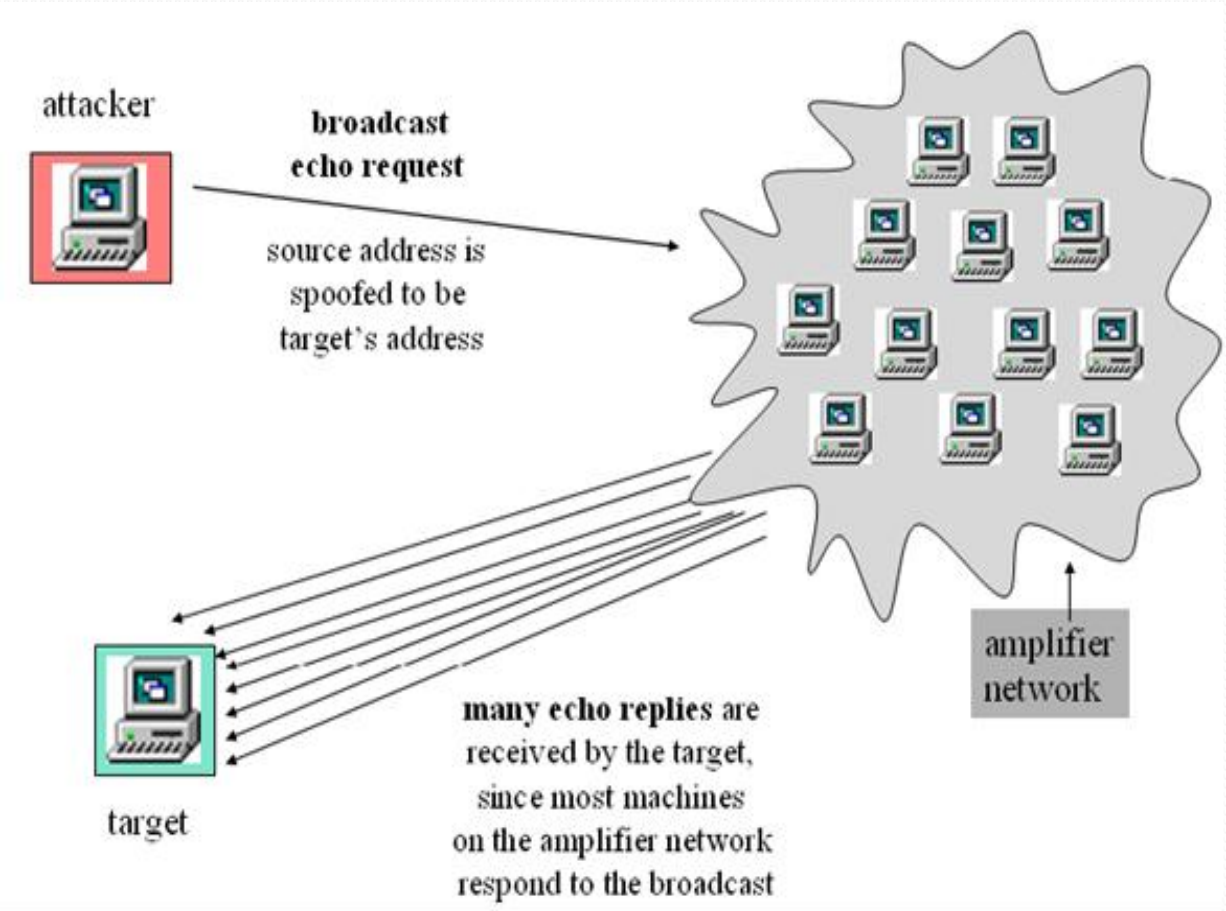
Phân loại tấn công kiểu DDOS



BandWith Depletion Attack

- Được thiết kế nhằm làm tràn ngập mạng mục tiêu với những traffic không cần thiết, với mục đích làm giảm tối thiểu khả năng của các traffic hợp lệ đến được hệ thống cung cấp dịch vụ của mục tiêu.
- *Flood attack*: Điều khiển các Agent gửi một lượng lớn traffic đến hệ thống dịch vụ của mục tiêu, làm dịch vụ này bị hết khả năng về băng thông.
- *Amplification attack*: Điều khiển các agent hay Client tự gửi message đến một địa chỉ IP broadcast, làm cho tất cả các máy trong subnet này gửi message đến hệ thống dịch vụ của mục tiêu. Phương pháp này làm gia tăng traffic không cần thiết, làm suy giảm băng thông của mục tiêu.

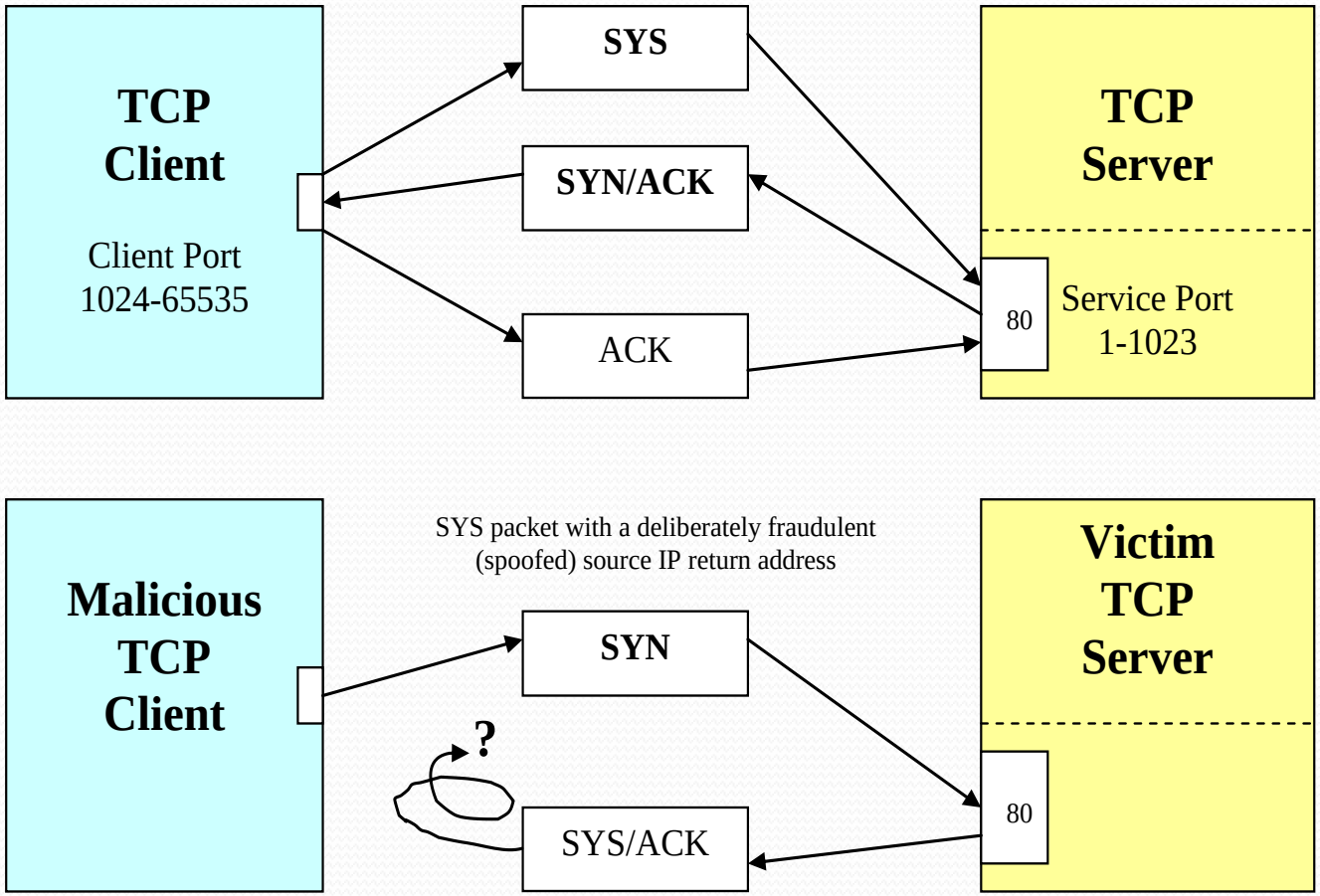
Amplification Attack



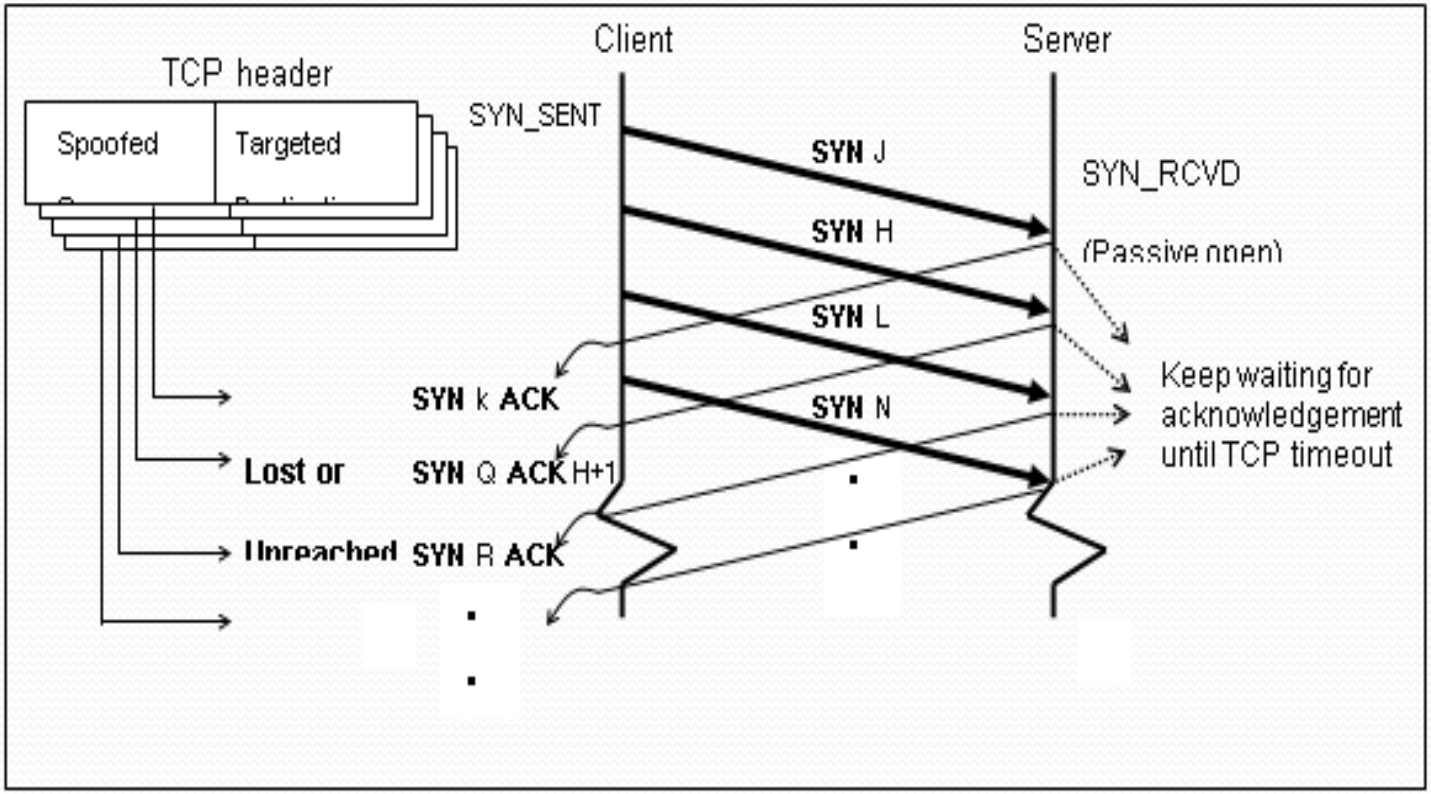
Resource Deleption Attack

- Resource Deleption Attack là kiểu tấn công trong đó Attacker gửi những packet dùng các protocol sai chức năng thiết kế, hay gửi những packet với dụng ý làm tắt nghẽn tài nguyên mạng làm cho các tài nguyên này không phục vụ user thông thường khác được.
- **Protocol Exploit Attack.**
- **Malformed Packet Attack.**

Protocol Exploit Attack



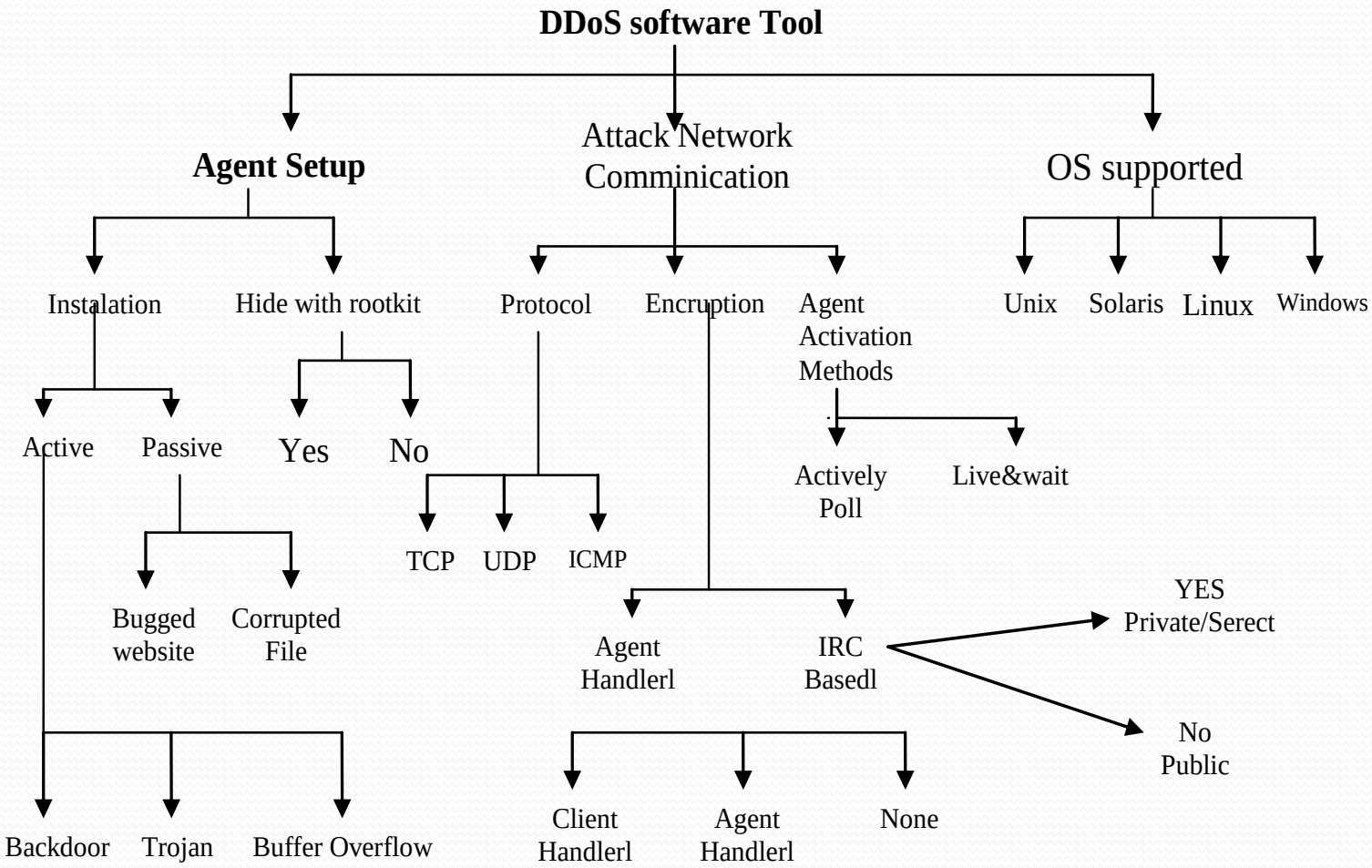
Protocol Exploit Attack



Malformed Packet Attack

- Là cách tấn công dùng các Agent để gửi các packet có cấu trúc không đúng chuẩn nhằm làm cho hệ thống của nạn nhân bị treo.
- Có hai loại Malformed Packet Attack:
- IP address attack: dùng packet có địa chỉ gửi và nhận giống nhau làm cho hệ điều hành của nạn nhân không xử lý nổi và bị treo.
- IP packet options attack ngẫu nhiên hóa vùng OPTION trong IP packet và thiết lập tất cả các bit QoS lên 1, điều này làm cho hệ thống của nạn nhân phải tốn thời gian phân tích, nếu sử dụng số lượng lớn Agent có thể làm hệ thống nạn nhân hết khả năng xử lý.

Một số đặc tính của công cụ DDoS



4. Tấn công sử dụng mã độc

- Malicious code often masquerades as good software or attaches itself to good software
- Some malicious programs need host programs
  - Trojan horses, logic bombs, viruses
- Others can exist and propagate independently
  - Worms, automated viruses
- Many infection vectors and propagation methods
- Modern malware often combines trojan, rootkit, and worm functionality

Trojans

- A Trojan horse is malicious code hidden in an apparently useful host program
- When the host program is executed, trojan does something harmful or unwanted
  - User must be tricked into executing the host program
  - In 1995, a program distributed as PKZ300B.EXE looked like a new version of PKZIP… when executed, it formatted your hard drive
- Old-style trojans did not replicate, but today many are spread by virus- and worm-like mechanisms

Example of a Trojan

- Discover a helpdesk application on a Web server
  - Via misconfigured FrontPage, which allows arbitrary uploads and downloads from webroot directory
- Modify its input validation routine
  - Change the list of invalid characters to contain only spaces and ~
- Use SQL injection to log in with admin privileges
- Hijack a dormant VPN account and log into the internal network via VPN

More Trojans

- 1987: Login program on NASA computers hacked by Chaos Computer Club, steals passwords
- 1999: Hacked login program at U. of Michigan steals 1534 passwords within 23 hours
- 2003: AOL employees tricked into accepting trojans via AIM, hackers get complete remote control over their machines via IRC
  - Also social engineering to steal passwords
- 2003: Badtrans worm installs a keystroke-logging trojan, sends log to one of 22 email accounts

Viruses

- Virus propagates by infecting other programs
  - Automatically creates copies of itself, but to propagate, a human has to run an infected program
  - Self-propagating malware usually called worm
- Many propagation methods
  - Insert a copy into every executable (.COM, .EXE)
  - Insert a copy into boot sectors of disks
    - PC era: "Stoned" virus infected PCs booted from infected floppies, stayed in memory, infected every inserted floppy
  - Infect TSR (terminate-and-stay-resident) routines
    - By infecting a common OS routine, a virus can always stay in memory and infect all disks, executables, etc.

First Virus: Creeper

- Written in 1971 at BBN
- Infected DEC PDP-10 machines running TENEX OS
- Jumped from machine to machine over ARPANET
  - Copied its state over, tried to delete old copy
- Payload: displayed a message "I'm the creeper, catch me if you can!"
- Later, Reaper was written to hunt down Creeper

Virus Techniques

- Macro viruses
  - A macro is an executable program embedded in a word processing document (MS Word) or spreadsheet (Excel)
  - When an infected document is opened, virus copies itself into global macro file and makes itself auto-executing (invoked whenever any document is opened)
- Stealth techniques
  - Rootkit: infect OS so that infected files appear normal
  - Code mutation and obfuscation

Polymorphic Viruses

- Encrypted viruses: constant decryptor followed by the encrypted virus body
- Polymorphic viruses: constantly create new random encryptions of the same virus body
  - Virus includes an engine for creating new keys and new encryptions of the virus body
- Decryptor code constant and can be detected
  - Historical note: "Crypto" virus decrypted its body by brute-force key search to avoid explicit decryptor code

Metamorphic Viruses

- Obvious next step: mutate the virus body, too!
- Apparition: early Win32 metamorphic virus
  - Carries its source code (contains useless junk)
  - Looks for compiler on infected machine
  - Changes junk in its source and recompiles itself
  - New binary copy looks different!
- Mutation is common in macro and script viruses
  - Macros/scripts are usually interpreted, not compiled

Virus Detection

- Simple anti-virus scanners
  - Look for signatures (fragments of known virus code)
  - Heuristics for recognizing code associated with viruses
    - Example: polymorphic viruses often use decryption loops
  - Integrity checking to find modified files
    - Record file sizes, checksums, keyed HMACs of contents
- Generic decryption and emulation
  - Emulate CPU execution for a few hundred instructions, recognize known body after virus decrypts
    - Does not work very well against metamorphic viruses and viruses not located near beginning of infected executable
  - What if decryptor starts with millions of NOPs?

Rootkits

- Rootkit is a set of trojan system binaries
  - Main characteristic: stealthiness
  - Hides infection from the host's owner
  - Often includes a sniffer (to record users' passwords)
  - Originally on Unix
- Typical infection path
  - Use stolen password or dictionary attack to log in
  - Use a buffer overflow in a vulnerable local program to gain root privileges
    - rdist, sendmail, loadmodule, rpc.ypupdated, lpr, passwd
  - Download rootkit, unpack, compile, install

Hiding Rookit's Presence on Unix

- Create a hidden directory
  - /dev/.lib, /usr/src/.poop and similar
  - Often use invisible characters in directory name (why?)
- Install hacked binaries for system programs such as netstat, ps, ls, du, login

Can't detect attacker's processes, files or network connections by running standard UNIX commands!

- Modified binaries have same checksum as originals
  - What should be used instead of checksum?

Function Hooking

- Idea: replace the pointer to a legitimate function with the address of malicious code
- Pointer hooking
  - Modify the pointer in OS's Global Offset Table, where function addresses are stored
- "Detour" or "inline" hooking
  - Insert a jump in first few bytes of a legitimate function
  - This requires subverting memory protection!
- Detectable by a clever rootkit detector
  - Hard to hide user-land rootkit from kernel-level detector

Kernel Rootkits

- Get loaded into kernel as an external module
  - For example, via compromised device driver or a badly implemented “digital rights” module (e.g., Sony XCP)
- Replace addresses in system call table, interrupt descriptor table, etc.
- If kernel modules disabled, directly patch kernel memory through /dev/kmem (SucKIT rootkit)
- Inject malicious code into a running process via PTRACE_ATTACH and PTRACE_DETACH
  - Security software is often the first injection target!

Mebroot (Windows)

- Replaces the host's Master Boot Record (MBR)
  - First physical sector of the hard drive
  - Launches before Windows loads
- No registry changes, very little hooking
- Stores data in physical sectors, not files
  - Invisible through the normal OS interface
- Uses its own version of network driver API to send and receive packets
  - Invisible to "personal firewall" in Windows
- Used in the Torpig botnet

Detecting Rootkit's Presence

- Sad way to find out
  - Run out of physical disk space because of sniffer logs
  - Logs are invisible because du and ls have been hacked!
- Manual confirmation
  - Reinstall clean ps and see what processes are running
- Automatic detection
  - Rootkit does not alter the data structures normally used by netstat, ps, ls, du, ifconfig
  - Host-based intrusion detection can find rootkit files
    - …assuming an updated version of rootkit did not disable the intrusion detection system!