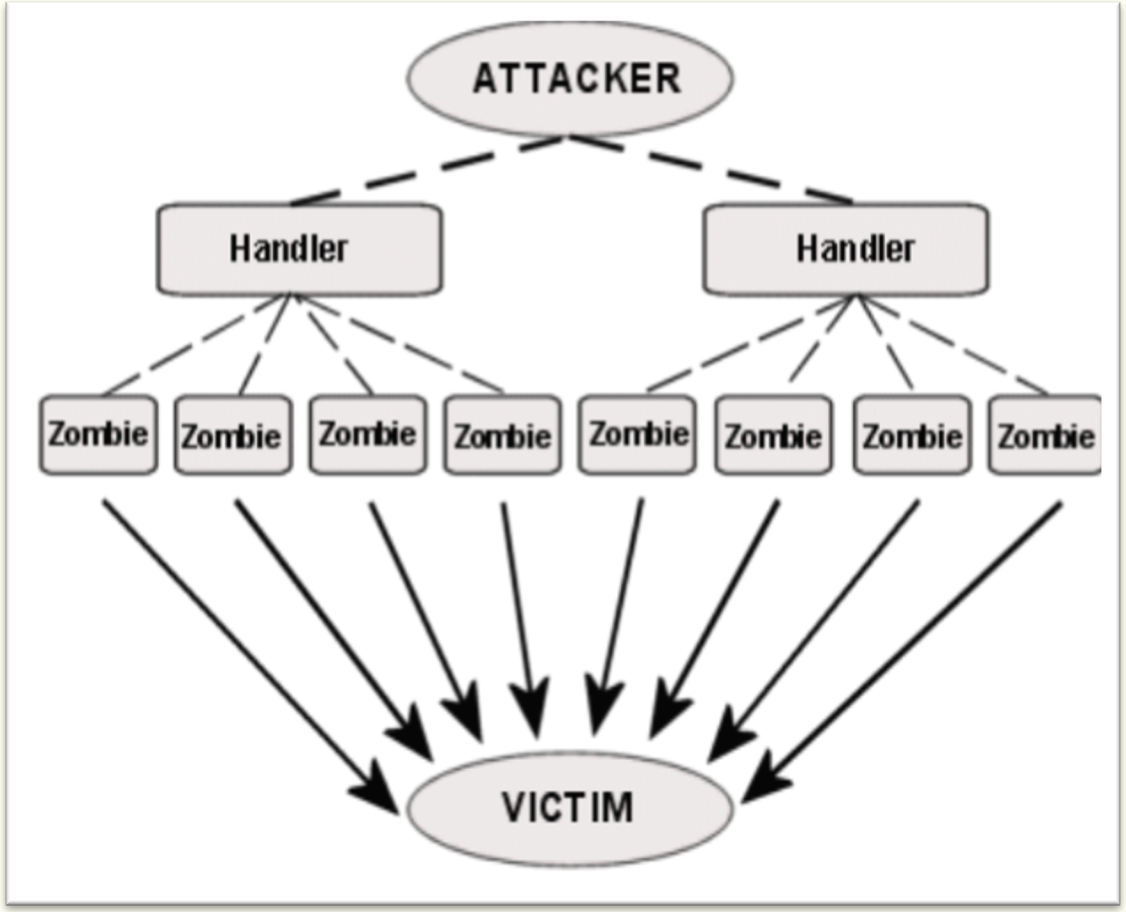
# CÁC DẠNG TẤN CÔNG DDOS

Nhóm 27:
- Trần Cao Minh Bách
- Vũ Thị Ánh
- Trần Thị Dung

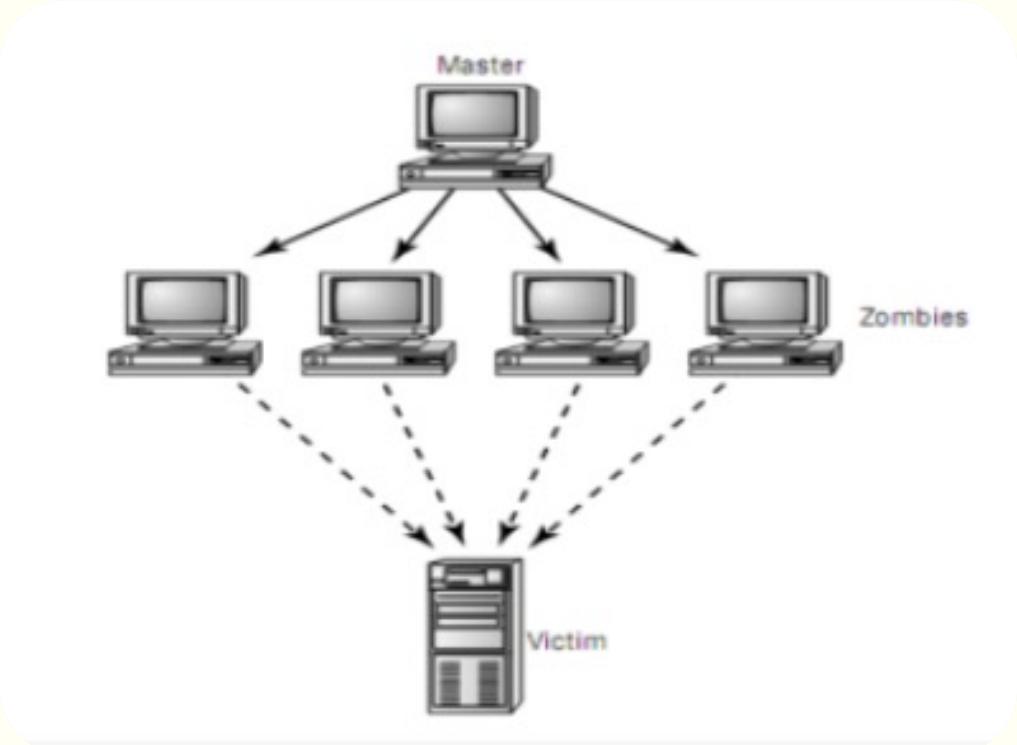


# Nội dung

1) Khái niệm DDoS
2) Các giai đoạn tấn công DDoS
3) Phân loại tấn công từ chối dịch vụ phân tán
4) Mạng Botnet
5) Các kỹ thuật tấn công
6) Một vài công cụ tấn công DDoS phổ biến hiện nay

# 1. Khái niệm DDoS

- Tấn công DDoS (Distributed Denial of Service) tấn công từ chối dịch vụ phân tán.
- Là hành động ngăn cản những người dùng hợp pháp của một dịch vụ nào đó truy cập và sử dụng dịch vụ đó, bằng cách làm cho server không thể đáp ứng được các yêu cầu sử dụng dịch vụ từ các client.



# 2. Các giai đoạn tấn công DDoS

Giai đoạn chuẩn bị

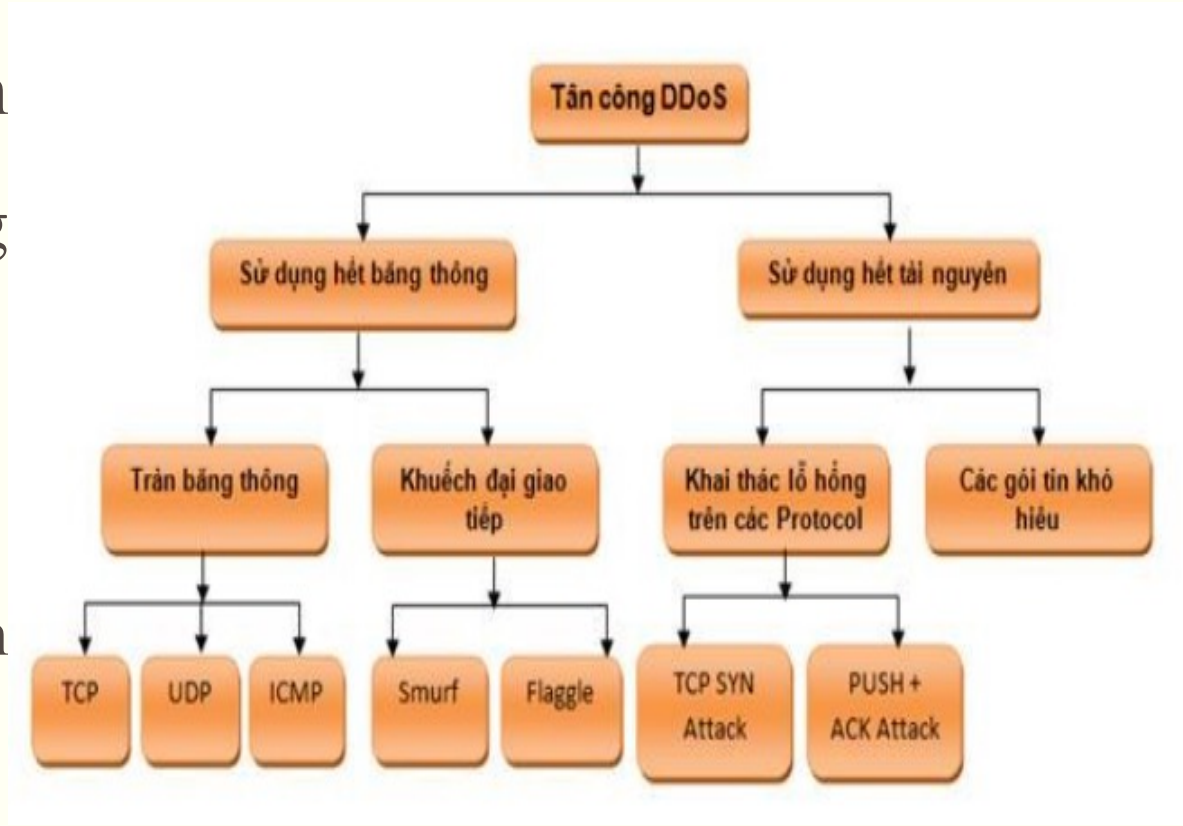
Giai đoạn xác định mục tiêu và thời điểm tấn công

Giai đoạn phát động tấn công và xoá dấu vết

# 3. Phân loại tấn công

Dựa vào mục đích của cuộc tấn công, thì chia thành 2 loại tấn công chính:

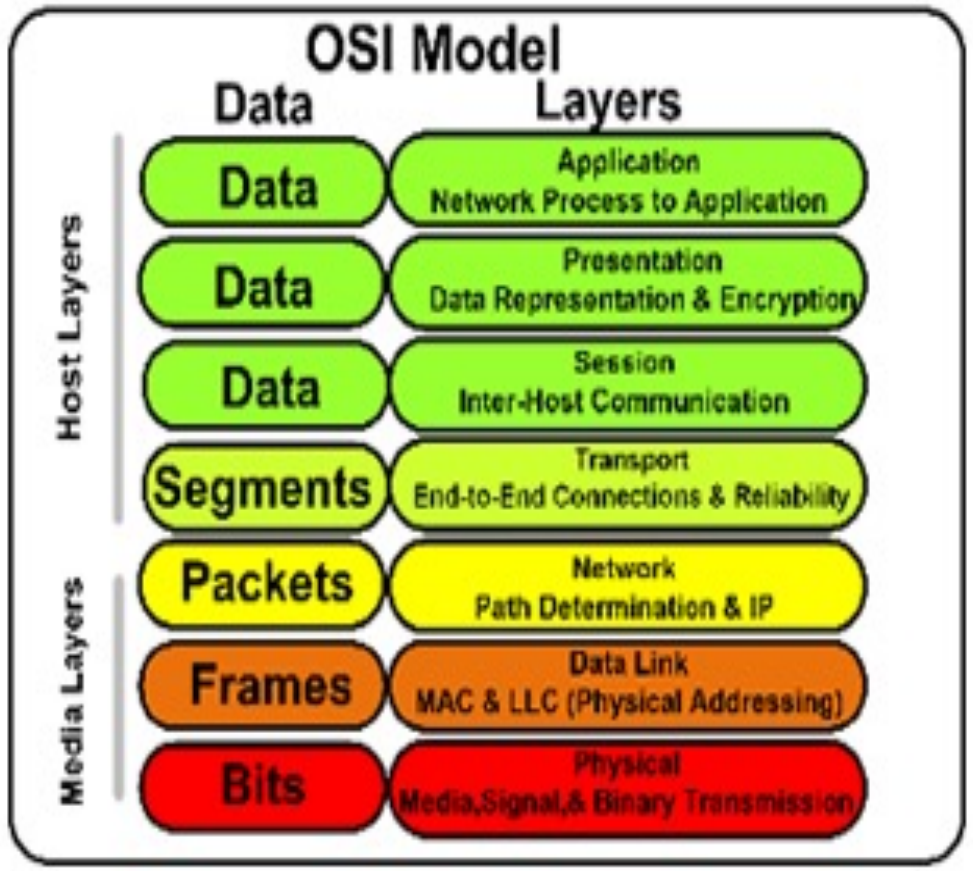
- Tấn công làm cạn kiệt băng thông
- Tấn công làm cạn kiệt tài nguyên hệ thống



# 3. Phân loại tấn công

Phân loại tấn công DDoS dựa trên mô hình OSI 07 tầng:

- Các cuộc tấn công IP nhằm vào băng thông – tấn công vào lớp 3 (tầng mạng).
- Các cuộc tấn công TCP trên máy chủ sockets – tấn công vào lớp 4 (tầng vận chuyển).
- Các cuộc tấn công HTTP trên máy chủ web – tấn công vào lớp 7 (tầng ứng dụng).
- Tấn công vào ứng dụng web, đánh vào tài nguyên CPU – tấn công trên lớp 7.



# 4. Mạng botnet

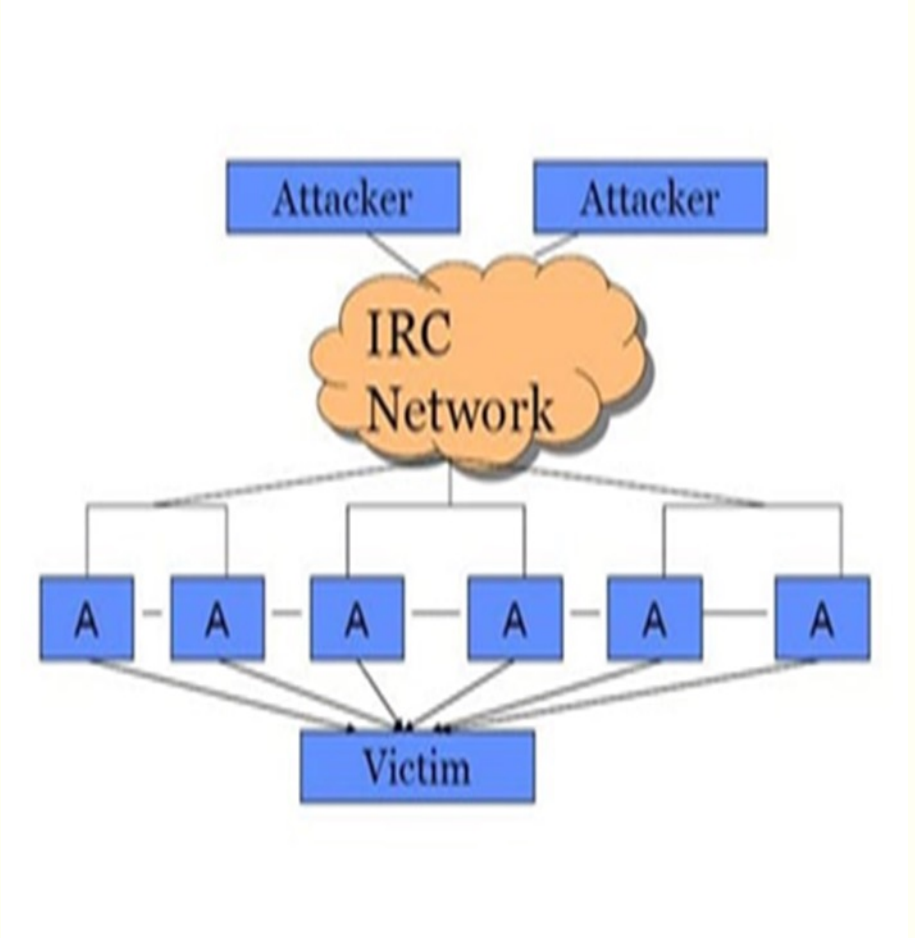
## a) Mạng Internet Relay Chat

- Mạng Internet Relay Chat (IRC) là một dạng truyền dữ liệu thời gian thực trên Internet.
- Cho phép các nhóm người trong một phòng thảo luận (channel) liên lạc với nhau.

# 4. Mạng botnet

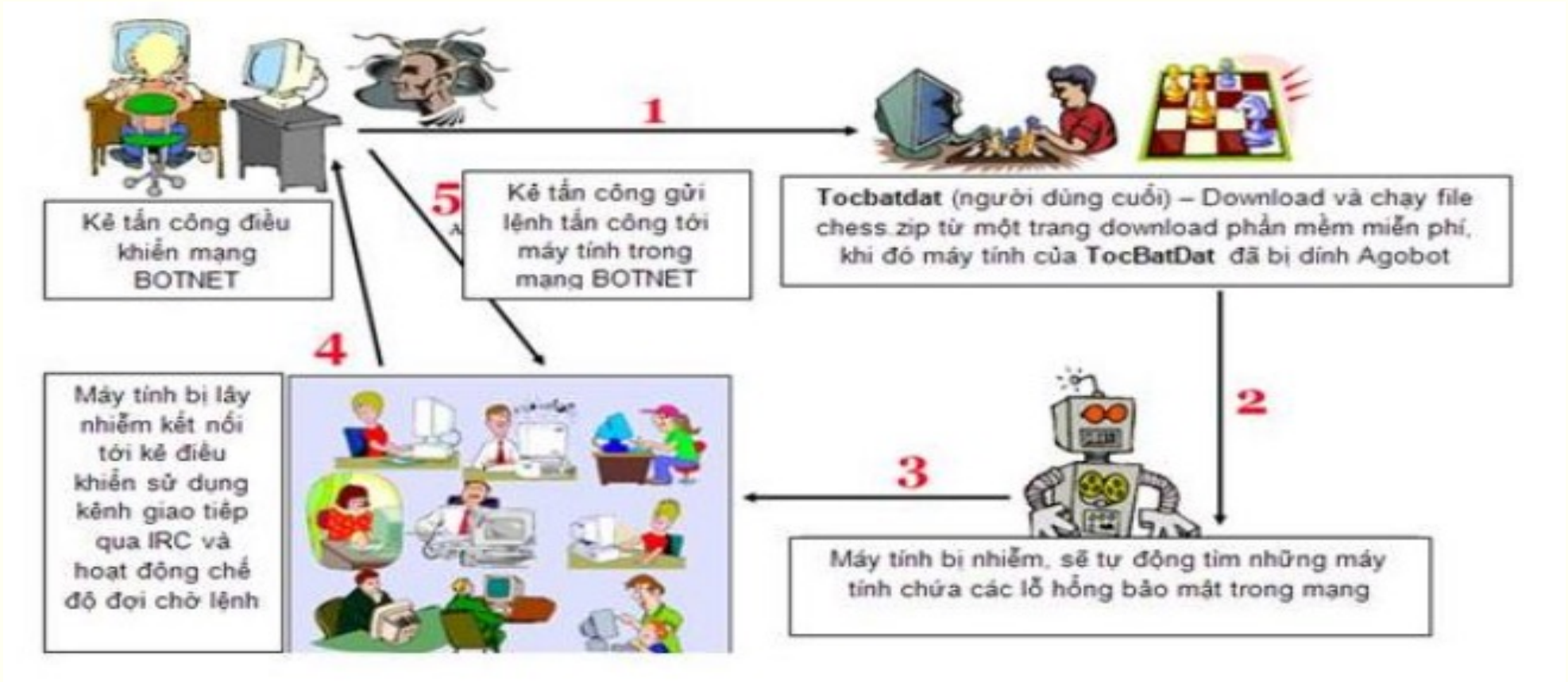
b) Mạng Botnet

- Botnet là một tập hợp các máy tính bị lây nhiễm bởi bot.
- Nó được sử dụng cho mục đích tấn công DDoS.
- Một mạng Botnet nhỏ có thể chỉ bao gồm 1000 máy tính.
- Botnet nổi tiếng: Mirai Botnet



# 4. Mạng botnet

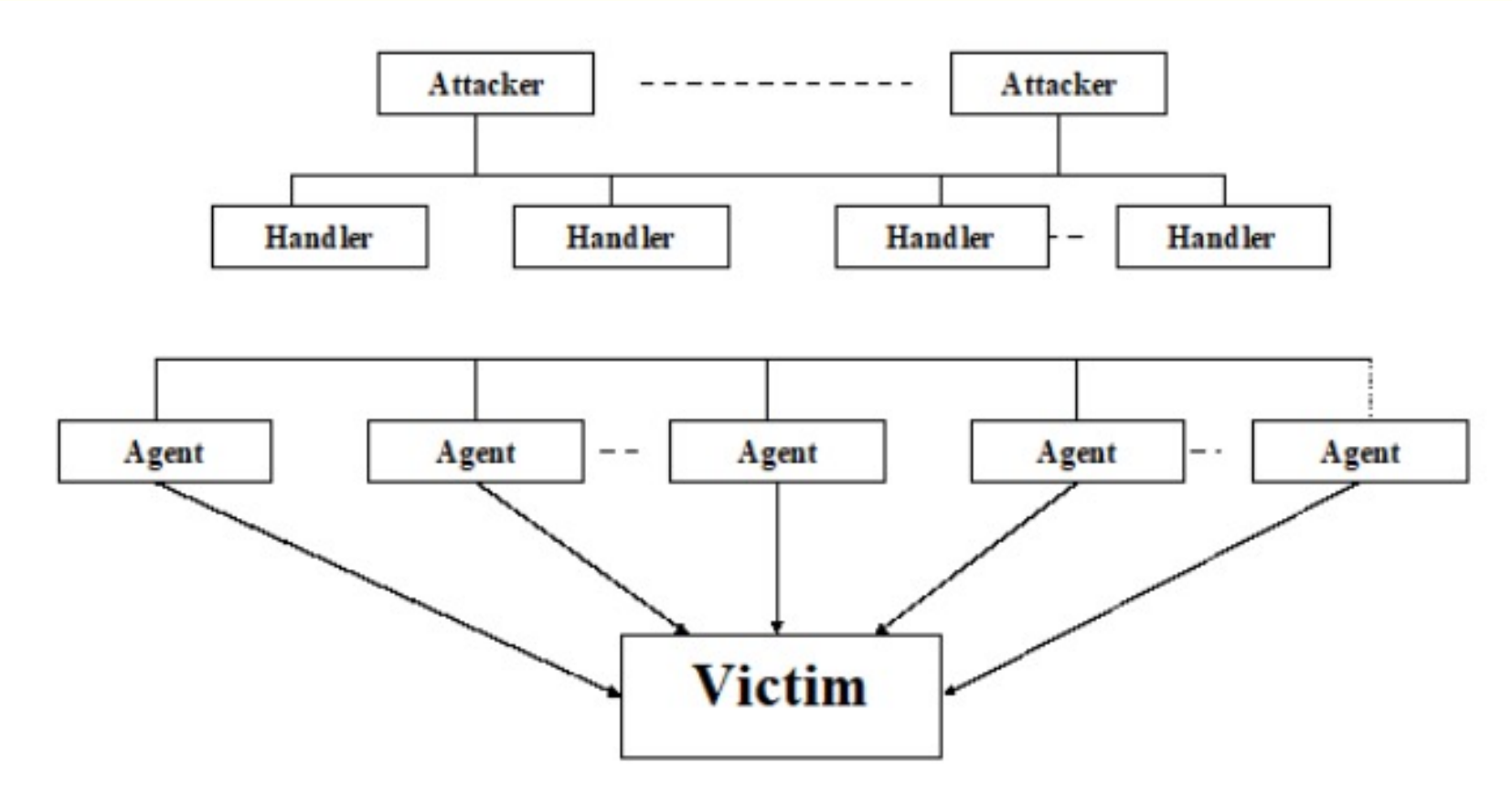
c) Các bước xây dựng mạng Botnet.



# 4. Mạng botnet

d) Các mô hình tấn công DDoS.

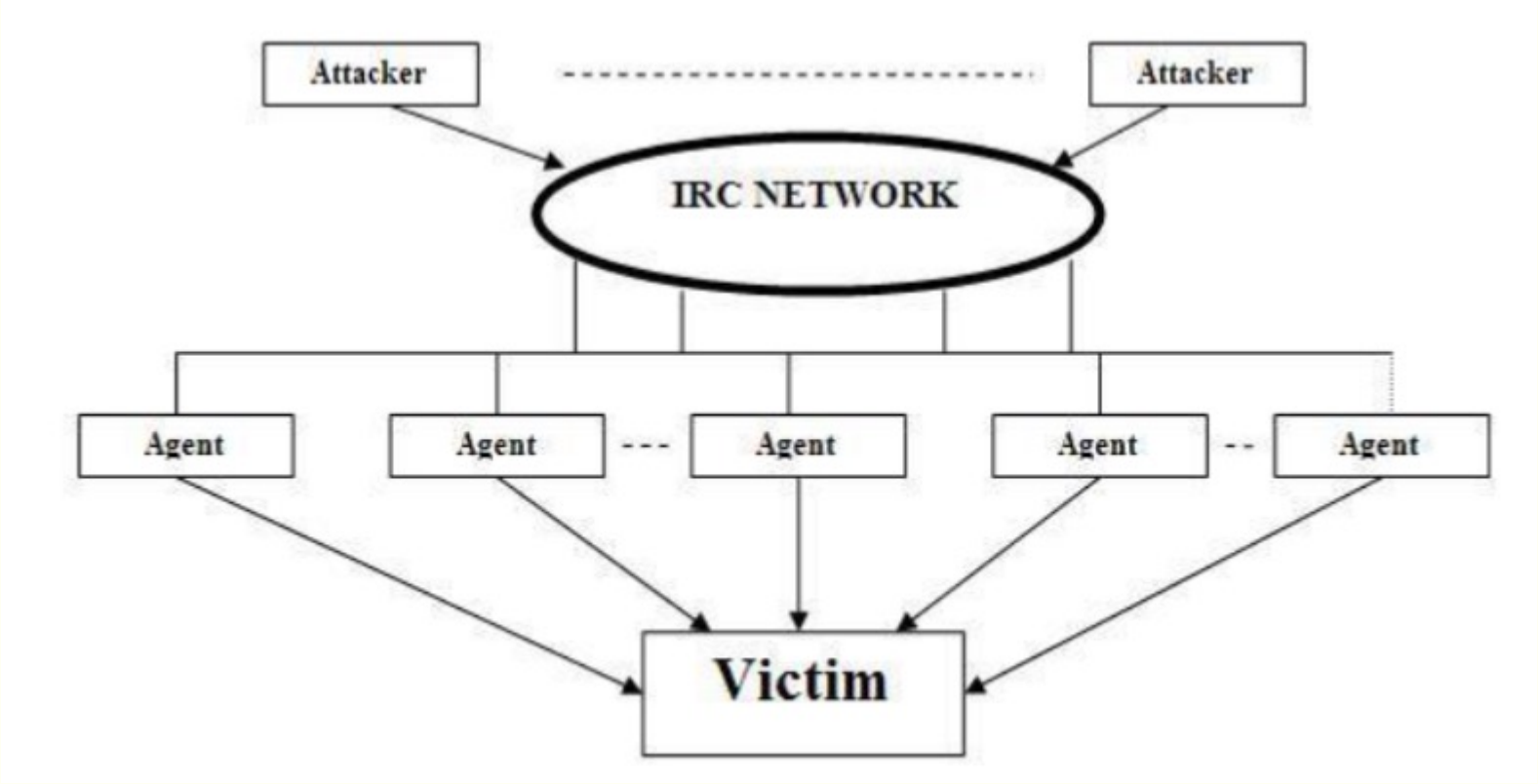
- Mô hình Agent-Handler



# 4. Mạng botnet

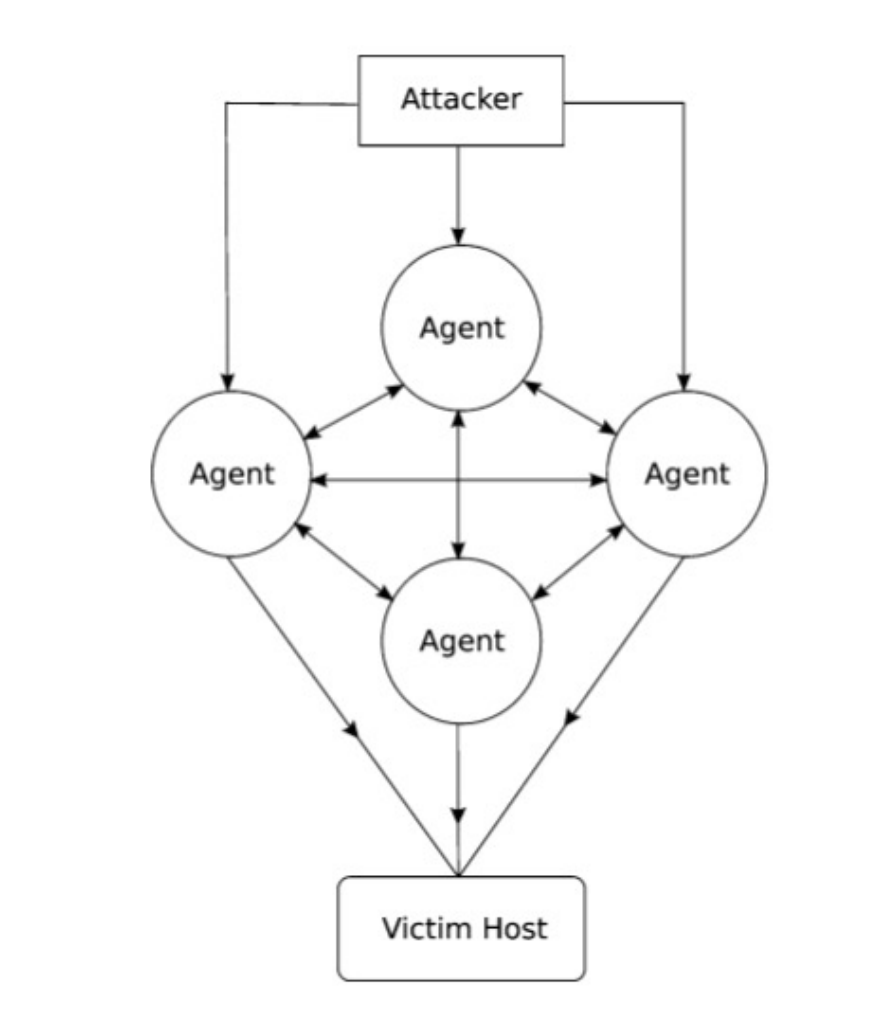
d) Các mô hình tấn công DDoS.

➢Mô hình tấn công IRC-Based



# 4. Mạng botnet

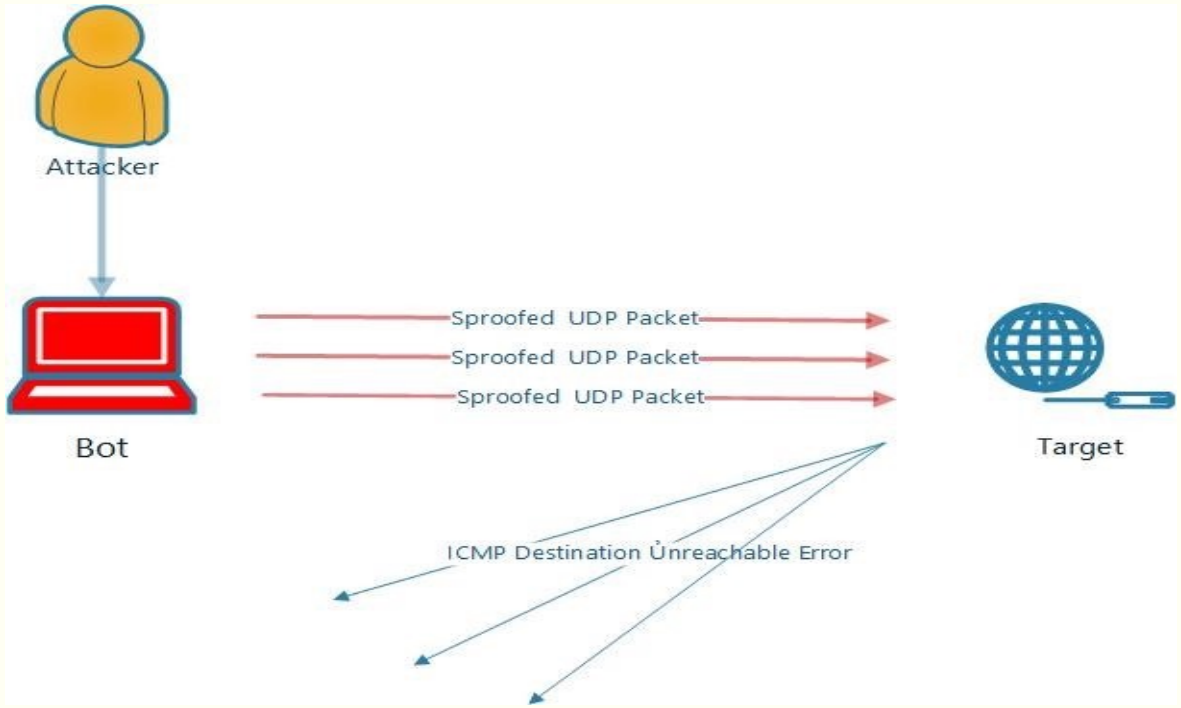
e) Peer-to-Peer



# 5. Các kĩ thuật tấn công

a) Tấn công làm cạn kiệt băng thông (Band with Deleption)

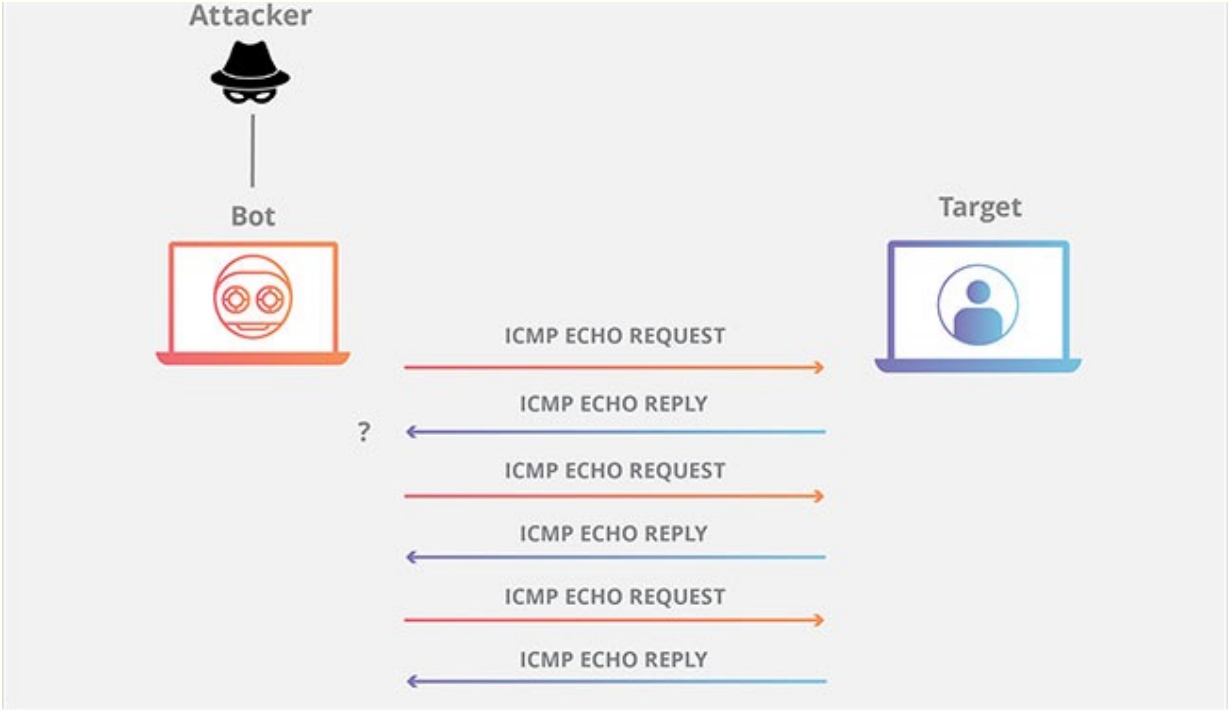
- Tấn công tràn băng thông.
  - Tấn công tràn băng thông bằng gói tin UDP



# 5. Các kĩ thuật tấn công

a) Tấn công làm cạn kiệt băng thông (Band with Deleption)

- Tấn công tràn băng thông.
  - Tấn công tràn băng thông bằng gói tin ICMP



# 5. Các kĩ thuật tấn công

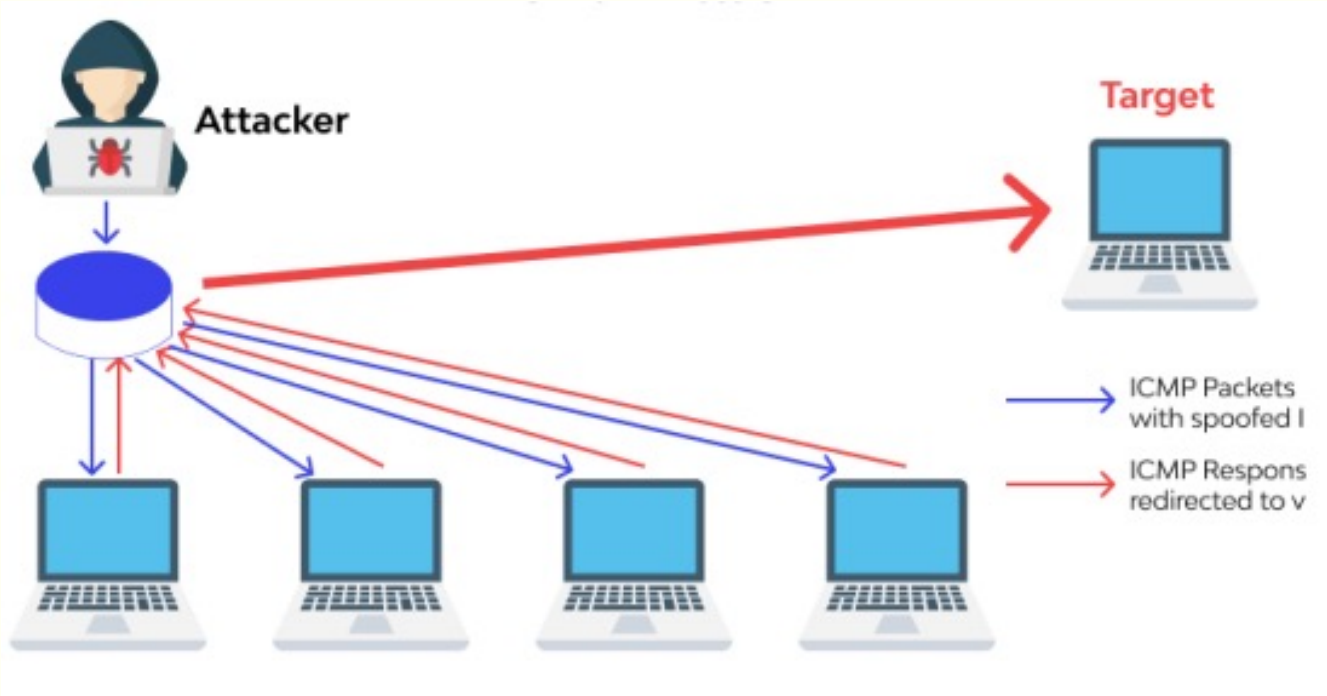
a) Tấn công làm cạn kiệt băng thông (Band with Deleption)

- Tấn công tràn băng thông.
  - DNS Flood
    - ✓ Là một biến thể của UDP Flood mục tiêu tập trung vào các máy chủ DNS.
  - VoIP Flood
    - ✓ Là một hình thức phổ biến của UDP Flood nhắm vào máy chủ "giao thức thoại" qua giao thức Internet (VoIP)
  - SSDP Flood

# 5. Các kĩ thuật tấn công

a) Tấn công làm cạn kiệt băng thông (Band with Deleption)

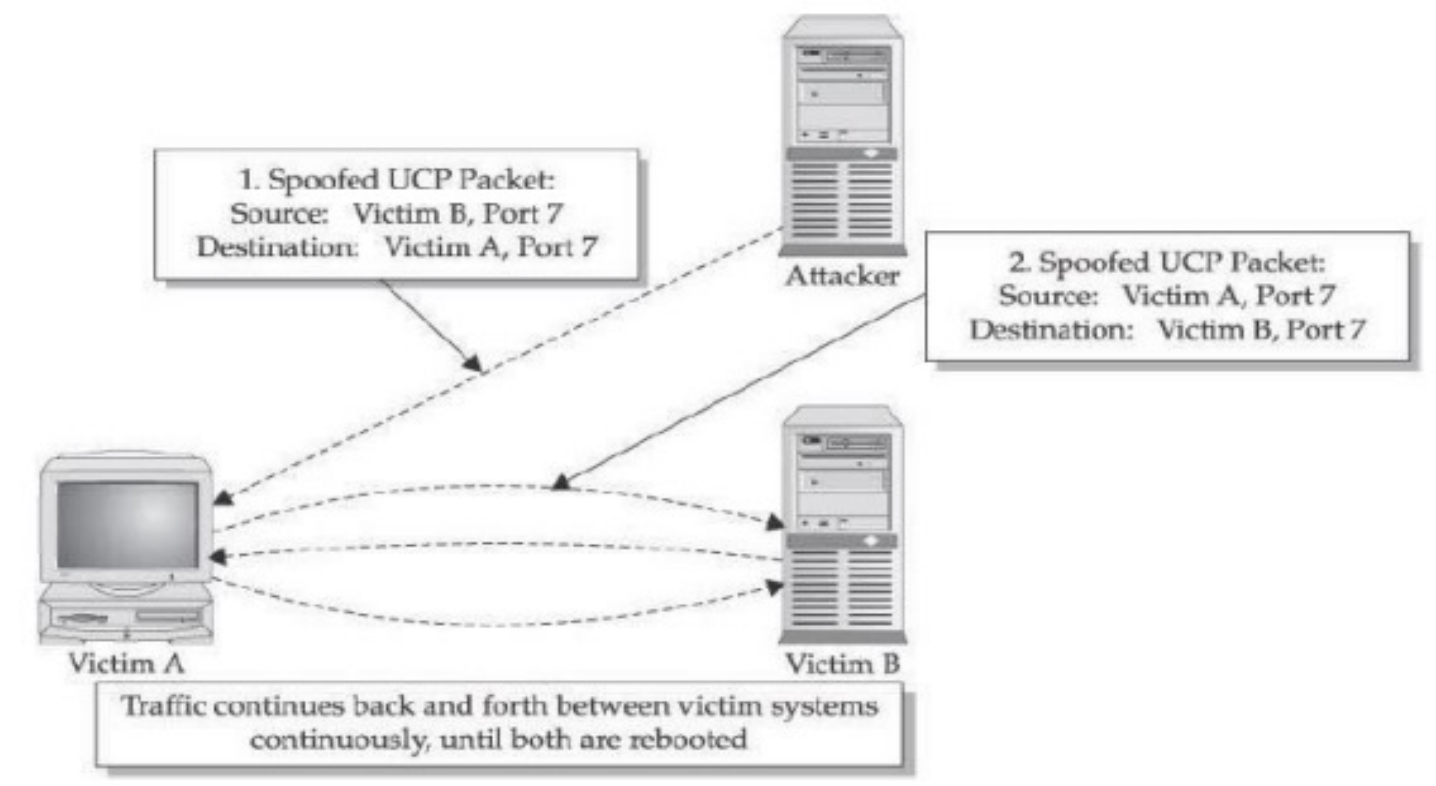
- Tấn công khuếch đại.
  - Tấn công kiểu Smuft



# 5. Các kĩ thuật tấn công

a) Tấn công làm cạn kiệt băng thông (Band with Deleption)

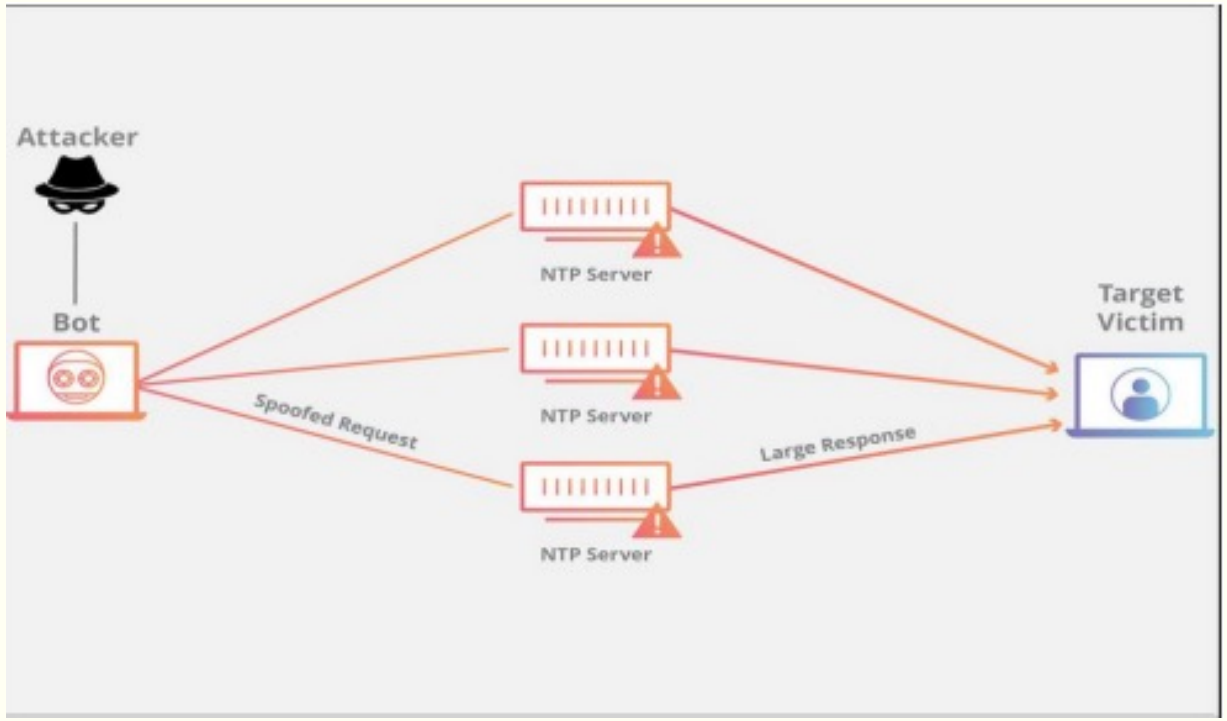
- Tấn công khuếch đại.
  - Tấn công kiểu Fraggle



# 5. Các kĩ thuật tấn công

a) Tấn công làm cạn kiệt băng thông (Band with Deleption)

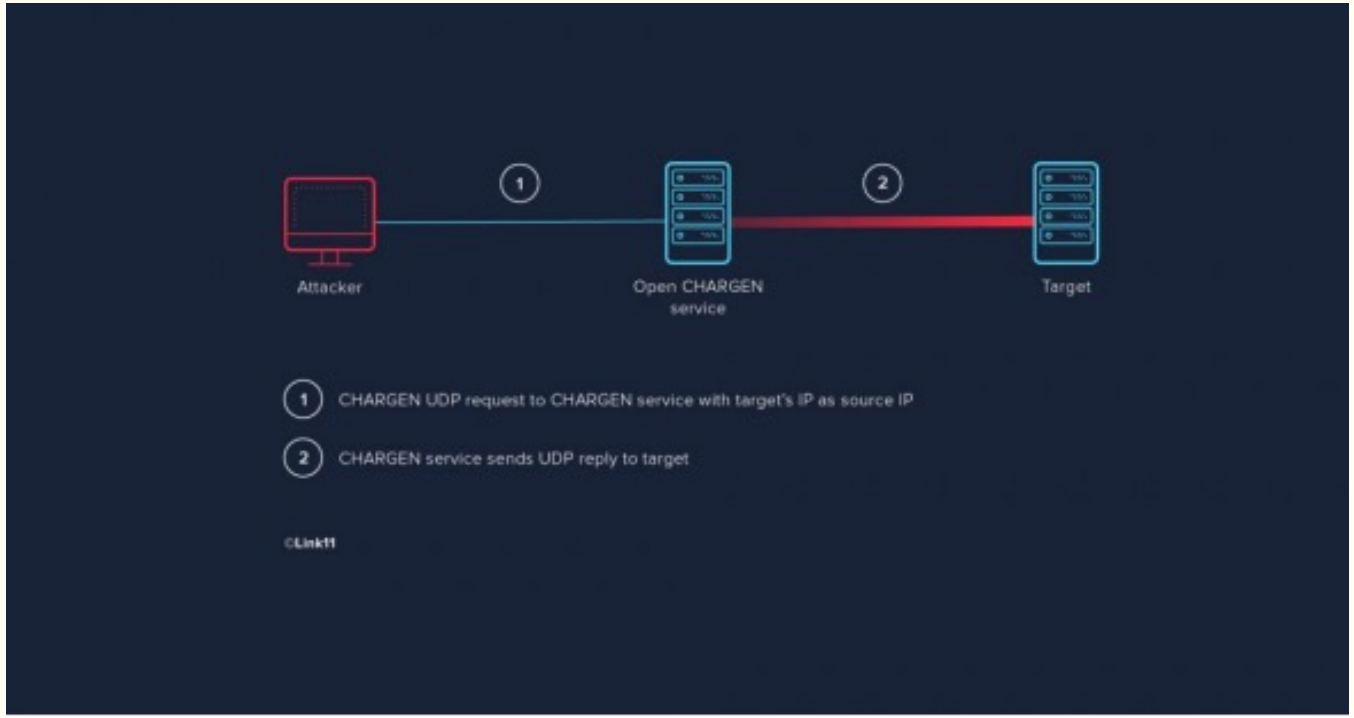
- Tấn công khuếch đại.
  - NTP Amplification



# 5. Các kĩ thuật tấn công

a) Tấn công làm cạn kiệt băng thông (Band with Deleption)

- Tấn công khuếch đại.
  - CHARGEN Flood



# 5. Các kĩ thuật tấn công

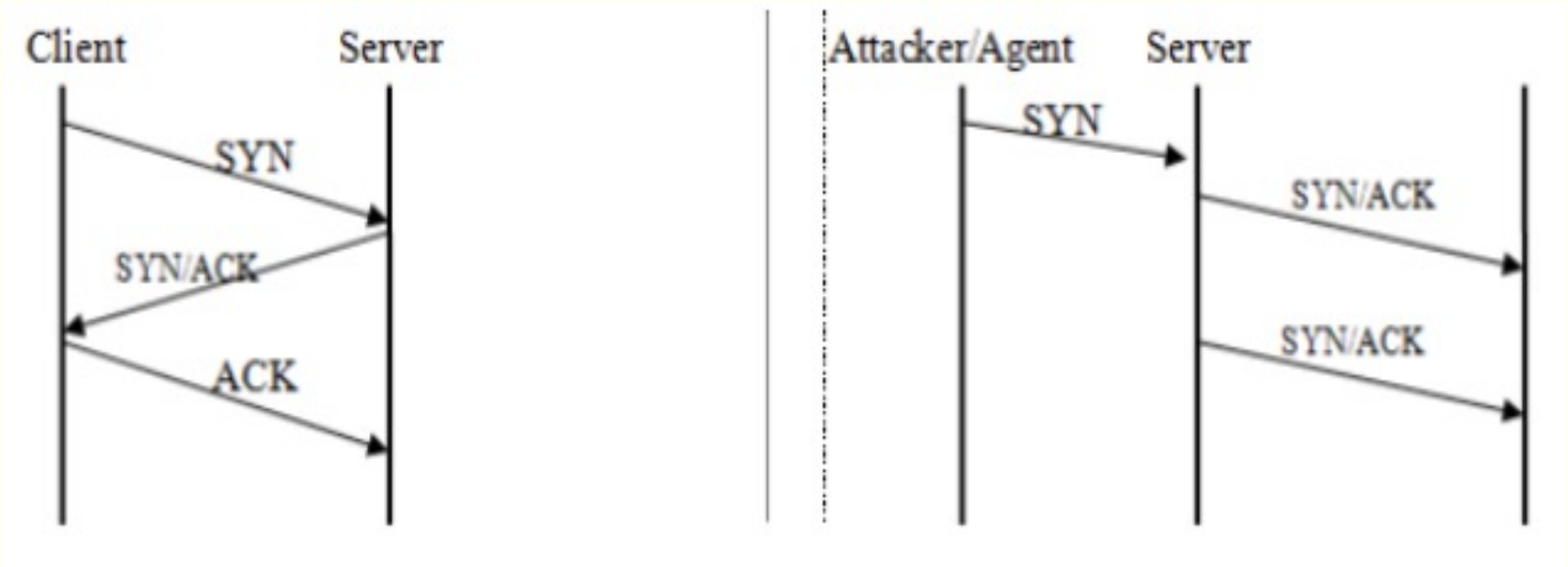
a) Tấn công làm cạn kiệt băng thông (Band with Deleption)

- Tấn công khuếch đại.
  - SNMP Flood
    - ✓ Kiểm tra các thiết bị mạng như router, switch hay server có đang vận hành.
    - ✓ Hỗ trợ vận hành các thiết bị này một cách tối ưu.
    - ✓ Quản lý các thiết bị mạng từ xa.
  - Misused Application Attack
    - ✓ Ký sinh trên các máy khách hợp pháp chạy các ứng dụng sử dụng nhiều tài nguyên như công cụ P2P.

# 5. Các kĩ thuật tấn công

b) Tấn công làm cạn kiệt tài nguyên (Resoure Deleption)

- Tấn công tràn SYN



# 5. Các kĩ thuật tấn công

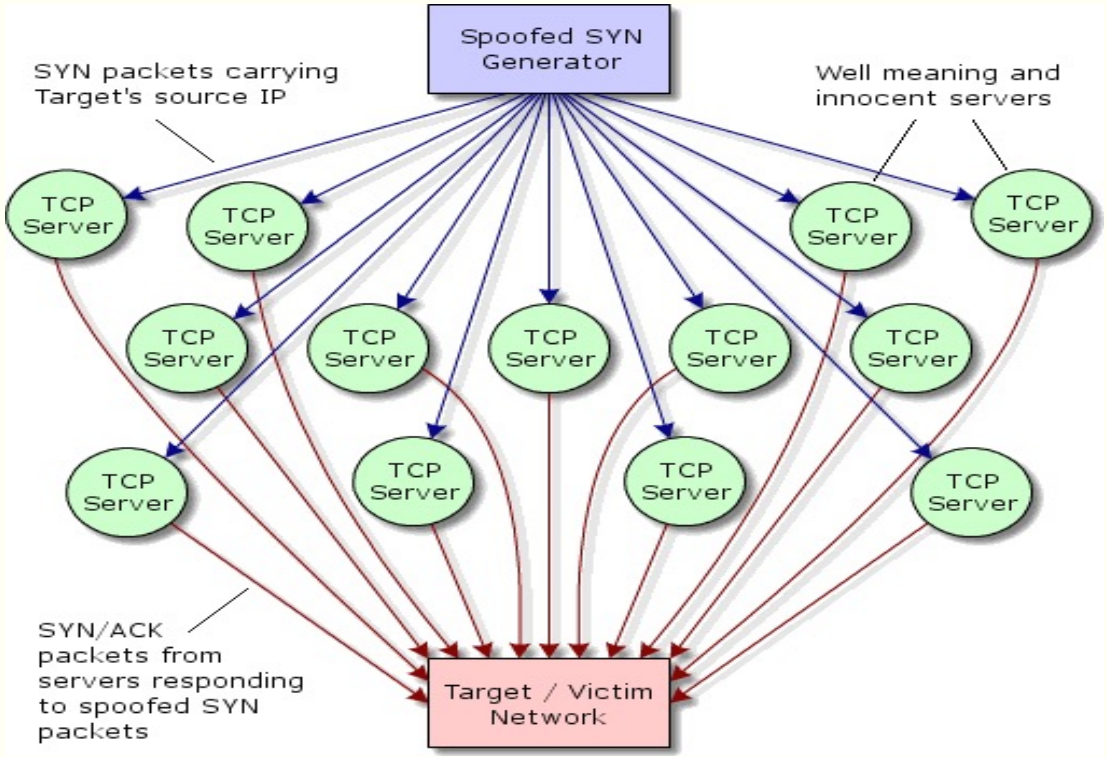
b) Tấn công làm cạn kiệt tài nguyên (Resoure Deleption)

- SYN-ACK Flood
- ACK & PUSH ACK Flood
- Fragmented ACK Flood
- Spoofed Session Flood
- LAND attack

# 5. Các kĩ thuật tấn công

c) Các biến thể của tấn công DDoS

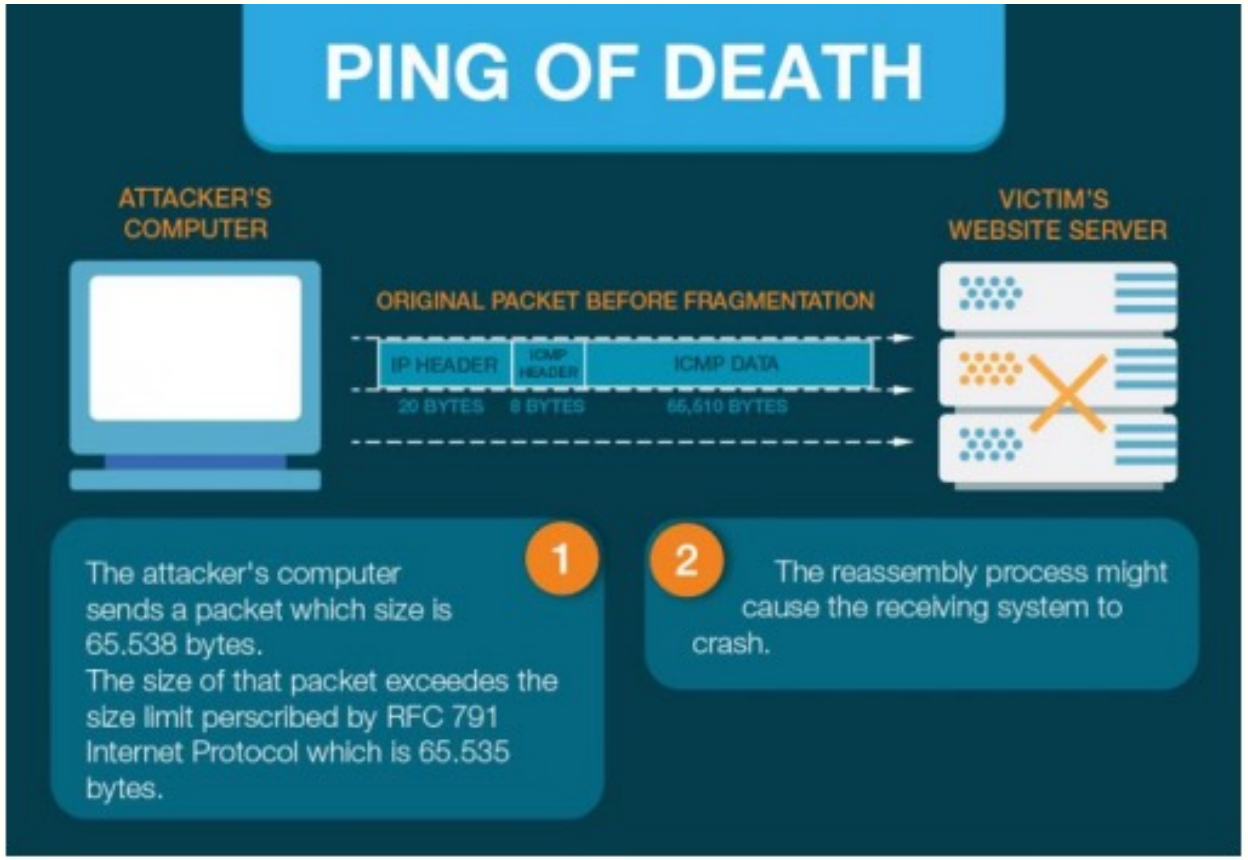
- Tấn công kiểu Flash DDoS.
- Tấn công kiểu DRDoS (Distributed Reflection Denial of Service)



# 5. Các kĩ thuật tấn công

c) Các biến thể của tấn công DDoS

- Tấn công Ping of Death



# 6. Một vài công cụ tấn công DDoS phổ biến hiện nay

a) Công cụ tấn công LOIC (Low Orbit Ion Canon)

b) Công cụ tấn công XOIC

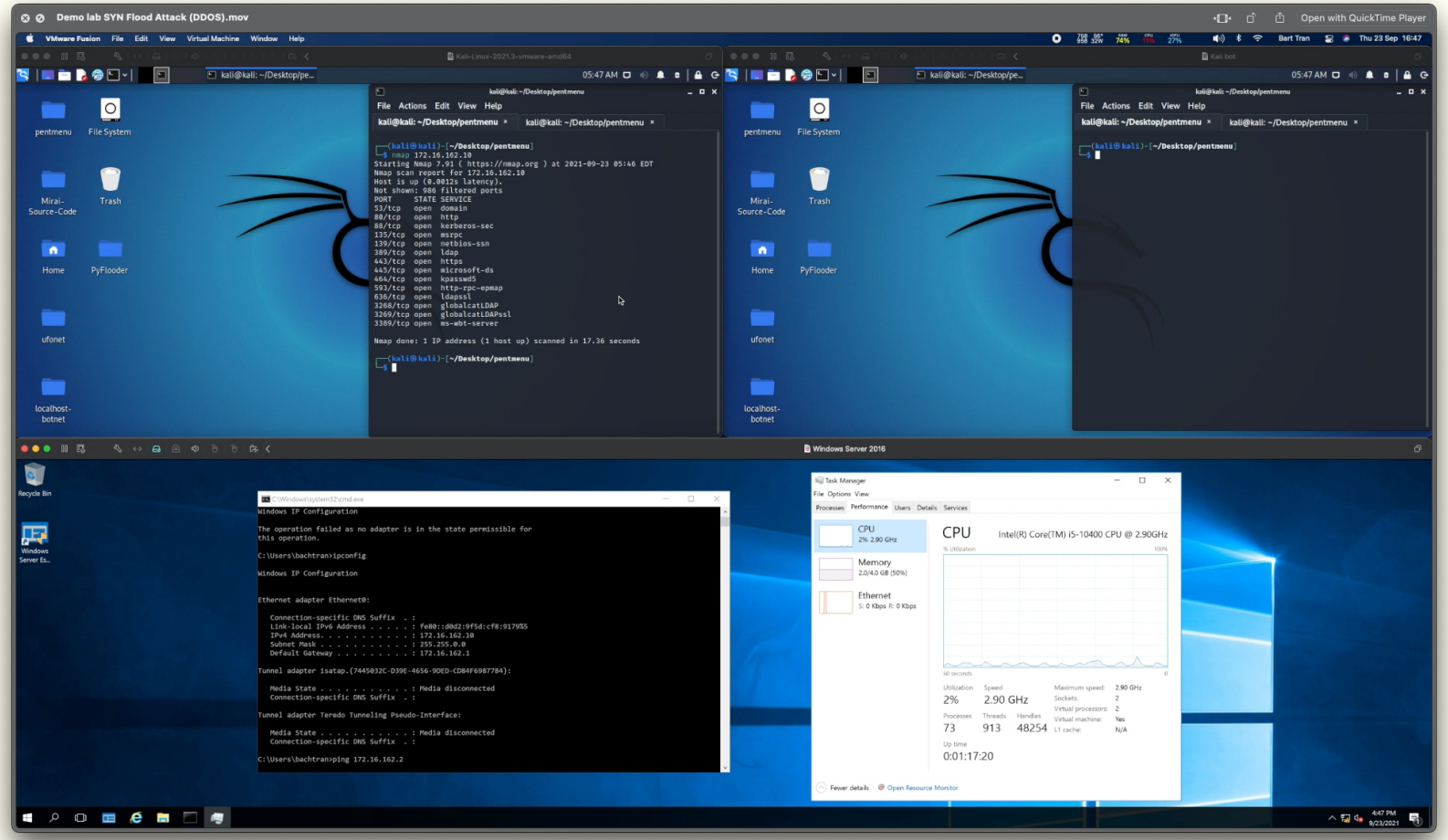
c) Công cụ tấn công HULK (HTTP Unbearable Load King)

d) Công cụ tấn công DDoSIM – Layer 7 DDoS Simulator

e) Công cụ tấn công OWASP DOS HTTP POST

f) Công cụ tấn công R-U-Dead-Yet

# Demo


Demo lab SYN Flood Attack (DDOS).mov
Open with QuickTime Player
pentmenu
File System
Mirai-Source-Code
Trash
Home
PyFlooder
ufonet
localhost-botnet
Windows Server 2016
Recycle Bin
Windows Server Es...
Task Manager
CPU
Intel(R) Core(TM) i5-10400 CPU @ 2.90GHz
Memory
Ethernet