

# Chương 5: Denial of Service

Thành viên: Nguyễn Hữu Nghĩa  
Lục tấn Khoa



# Nội dung



01

**Giới thiệu tấn công từ chối dịch vụ (DoS)**

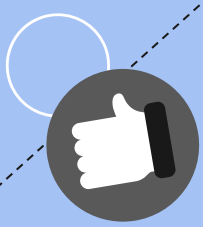
02

**Tấn công ngập lụt (Flooding Attack)**

03

**Các biện pháp phòng thủ và phản ứng trước DoS**





01

# Giới thiệu tấn công từ chối dịch vụ (DoS)



# Định nghĩa DoS

Tấn công từ chối dịch vụ (DoS) là một hành động nhằm ngăn chặn hoặc làm suy yếu khả năng sử dụng của mạng, hệ thống, hoặc các ứng dụng bằng cách làm cạn kiệt nguồn tài nguyên như: Bộ xử lý trung tâm (CPU), bộ nhớ (Memory), băng thông (Bandwidth), và không gian đĩa (Disk space/Storage).



# Mục tiêu của tấn công DoS



## Network Blandwidth (băng thông mạng)

Liên quan đến dung lượng của các liên kết mạng giữa máy máy mục tiêu và internet. Thông thường là làm cho quá tải kết nối giữa mạng nội bộ với nhà cung cấp dịch vụ Internet (ISP)



## System Resource (tài nguyên hệ thống)

Bộ nhớ đệm, lỗ hổng hệ thống, phần mềm xử lý mạng, ... Làm cho quá tải hoặc hỏng tài nguyên hệ thống

## Application Resources (tài nguyên ứng dụng)

Các App requests, database queries, search queries, ... Tấn công liên quan đến yêu cầu hợp lệ, mỗi yêu cầu tiêu thụ tài nguyên đáng kể, do đó hạn chế khả năng máy mục tiêu phản hồi yêu cầu từ người dùng khác



# Phân loại tấn công DoS

## DoS truyền thống

Tấn công từ một nguồn duy nhất



## DDoS (Distributed Denial of Service)

Tấn công từ nhiều nguồn khác nhau





02

# Tấn công ngập lụt (Flooding Attack)





# Định nghĩa tấn công ngập lụt

Tấn công ngập lụt (Flooding Attacks) là một dạng tấn công DoS trong đó kẻ tấn công gửi một lượng lớn yêu cầu hoặc dữ liệu vào mục tiêu để tiêu tốn băng thông hoặc tài nguyên của hệ thống, từ đó làm nó ngừng hoạt động.





# Các loại hình tấn công ngập lụt phổ biến



## ICMP Flood

Gửi một lượng lớn lệnh ping đến mục tiêu để làm tắc nghẽn bản thông.



## UDP Flood

Gửi một lượng lớn gói UDP đến các cổng trên máy chủ làm quá tải băng thông và tài nguyên.

## TCP SYN Flood

Kẻ tấn công gửi một loạt các yêu cầu kết nối TCP SYN mà không hoàn tất quá trình bắt tay ba bước, gây tràn tài nguyên kết nối của máy chủ.



# DDoS (Distributed Denial of Service)

- **Mục tiêu:** Làm cho mục tiêu quá tải vì lưu lượng truy cập quá lớn so với khả năng đáp ứng của mục tiêu
- **Cách hoạt động:** Sử dụng nhiều hệ thống để tạo ra các cuộc tấn công. Kẻ tấn công sử dụng một lỗ hổng trong hệ điều hành hoặc trong một ứng dụng chung để có quyền truy cập và cài đặt chương trình của chúng vào đó. Có thể tạo ra một tập hợp lớn các hệ thống như vậy dưới sự kiểm soát của một kẻ tấn công, hình thành nên một mạng botnet.
- **Mạng botnet:** là tập hợp các thiết bị như máy tính, điện thoại, hoặc các thiết bị IOT bị xâm nhập và điều khiển, các thiết bị này thường được gọi là “bot”, “zombie” vì chúng hoạt động mà không biết là đang bị điều khiển”.



# Các loại hình DDoS phổ biến

## DDoS băng thông dựa trên ứng dụng (Application Layer DDoS Attack)

Application Layer DDoS Attack là một dạng tấn công DDoS nhắm vào tầng ứng dụng (tầng 7 trong mô hình OSI) của hệ thống, nơi các dịch vụ và ứng dụng hoạt động

## DDoS phản xạ và khuếch đại (Reflection & Amplification DDoS)

Reflection & Amplification DDoS là một kỹ thuật tấn công DDoS mà kẻ tấn công tận dụng các dịch vụ phản hồi trên internet để làm ngập mục tiêu bằng lượng lớn lưu lượng truy cập giả mạo

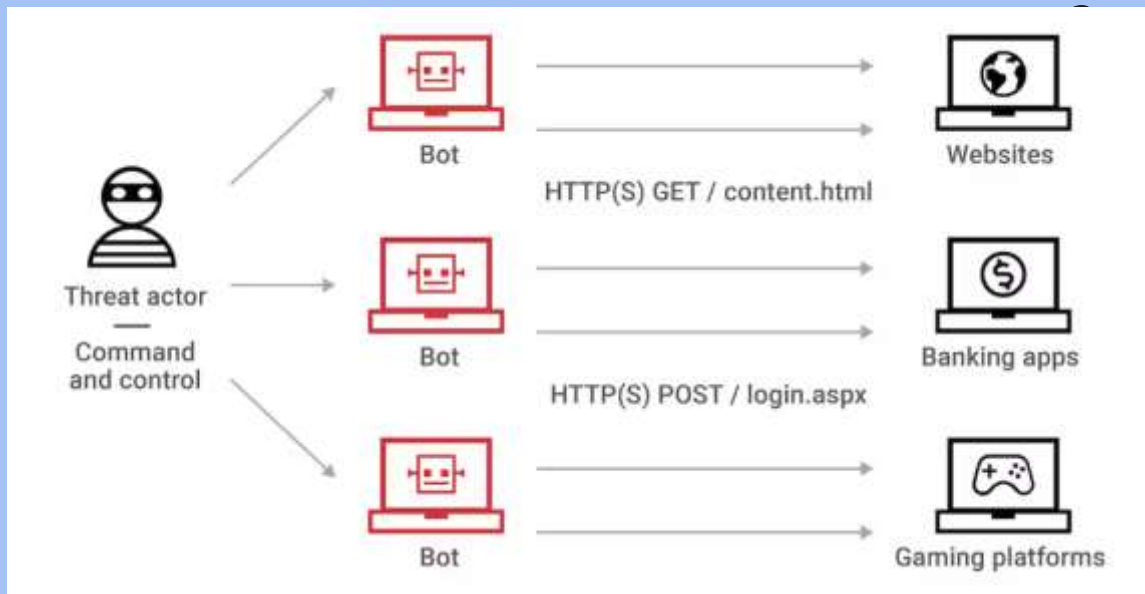


# DDoS bằng thông dựa trên ứng dụng phổ biến



## HTTP Flood

Tấn công vào các trang web bằng cách gửi một lượng lớn HTTP request khiến máy chủ quá tải không thể xử lý thêm các yêu cầu khác



# Các loại hình DDoS dựa trên ứng dụng phổ biến

## Slowloris Attack

Tấn công bằng cách cố gắng độc quyền kết nối đến máy chủ hay nói cách khác là gửi HTTP request không thể hoàn thành được, khiến cho máy chủ luôn trong trạng thái load nên không thể xử lý tác vụ khác làm tiêu tốn dung lượng, tài nguyên lớn

### Normal HTTP Request - Response Connection



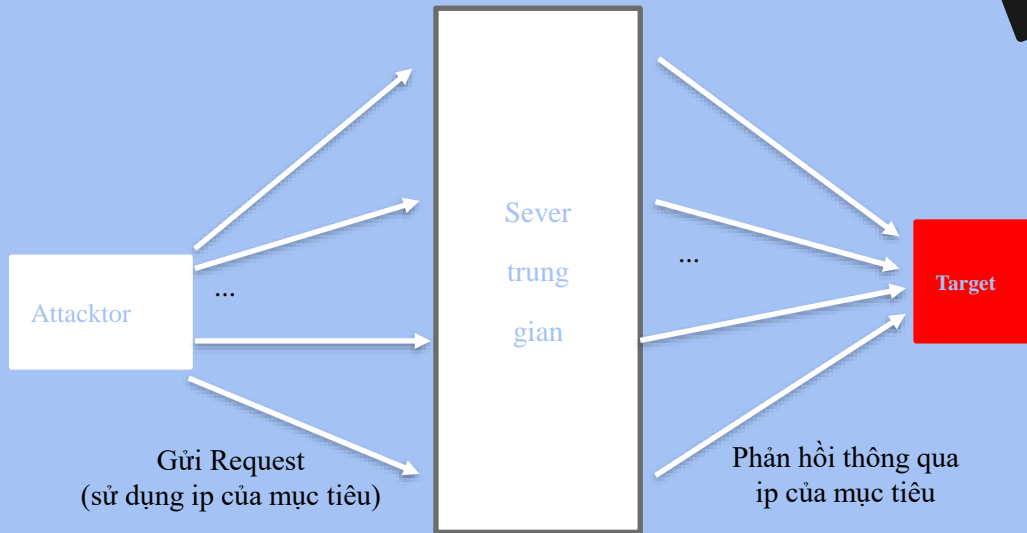
### Slowloris DDoS Attack



# DDoS phản xạ và khuếch đại

## Phản xạ (Reflection)

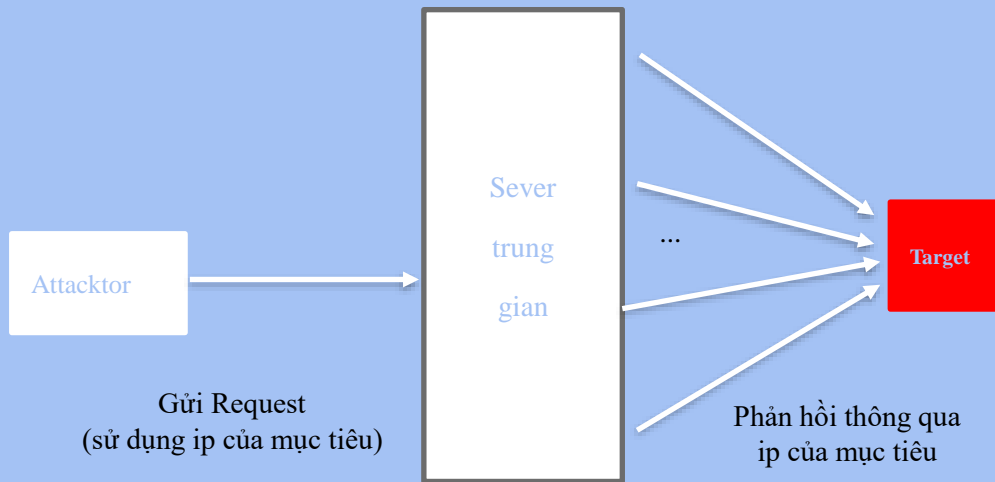
Kẻ tấn công gửi yêu cầu đến một máy chủ trung gian hoặc thiết bị mạng (thường là một dịch vụ công cộng như DNS) với địa chỉ IP nguồn giả mạo (là IP của mục tiêu tấn công). Sau khi máy chủ trung gian nhận được yêu cầu thì nó sẽ gửi phản hồi về địa chỉ IP giả mạo (IP của mục tiêu tấn công). Như vậy kẻ tấn công có thể tạo ra khối lượng lớn liên kết, sau đó lượng lớn liên kết được phản hồi sẽ gửi về mục tiêu thông qua IP. Khiến nó bị quá tải





# DDoS phản xạ và khuếch đại

## Khuếch đại (Amplification)



Kẻ tấn công tạo ra một loạt các yêu cầu DNS chứa IP giả mạo (IP của mục tiêu tấn công) khai thác hành vi DNS để sever trung gian nhận 1 request nhỏ nhưng lại phản hồi lại một lượng lớn và gửi chúng về mục tiêu thông qua IP giả mạo





03

# Các biện pháp phòng thủ và phản ứng trước DoS





# Bốn tuyến phòng thủ chống lại các cuộc tấn công DDoS



➤ Phòng chống tấn công và chủ động dự phòng (trước khi bị tấn công)

➤ Phát hiện và lọc cuộc tấn công (khi đang bị tấn công)

➤ Truy xuất nguồn tấn công và xác định (trong khi bị tấn công và sau đó)

➤ Phản ứng tấn công (sau cuộc tấn công)



# Phòng ngừa trước DoS

- ❖ Chặn IP nguồn giả mạo trên bộ định tuyến càng gần nguồn càng tốt.
- ❖ Sử dụng mã xử lý kết nối TCP đã sửa đổi:
  - Mã hóa bằng mật mã thông tin quan trọng trong cookie được gửi dưới dạng số thứ tự ban đầu của máy chủ. Ứng dụng khách hợp pháp phản hồi bằng gói ACK có chứa cookie số thứ tự tăng dần
  - Thả mục nhập cho kết nối chưa hoàn chỉnh từ bảng kết nối TCP khi nó bị tràn
- ❖ Chặn các quảng bá trực tiếp IP
- ❖ Chặn các dịch vụ và những kết nối đáng ngờ
- ❖ Quản lý các cuộc tấn công ứng dụng bằng một dạng câu đố đồ họa (captcha) để phân biệt các yêu cầu hợp pháp của con người
- ❖ Thực hành các bảo mật hệ thống chung
- ❖ Sử dụng các máy chủ được sao lưu và dự phòng khi có yêu cầu hiệu suất và độ tin cậy cao



# Ứng phó khi bị DDoS

- ❖ Kế hoạch ứng phó sự cố tốt:
  - Liên hệ nhanh chóng với kỹ thuật của ISP
  - Áp đặt bộ lọc các lưu lượng phản hồi
  - Có mô tả chi tiết cách phản ứng trước cuộc tấn công
- ❖ Các bộ lọc chống giả mạo (Antispoofing), bộ lọc lưu lượng quảng bá trực tiếp (Directed broadcast) và bộ lọc giới hạn tốc độ (rate limiting).
- ❖ Lý tưởng nhất là có trình giám sát mạng (Network Monitor) và Hệ thống phát hiện xâm nhập (IDS) để phát hiện và thông báo các mẫu lưu lượng bất thường
- ❖ Xác định kiểu tấn công
- ❖ Yêu cầu theo vết được đường đi của gói tin nguồn
- ❖ Thực hiện kế hoạch dự phòng
- ❖ Cập nhật kế hoạch ứng phó sự cố



Thanks!

