BỘ THÔNG TIN VÀ TRUYỀN THÔNG

HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

BÁO CÁO

Bài tập lớn môn An toàn và bảo mật hệ thống thông tin

Đề tài: Các dạng tấn công DoS và DDoS.

Giảng viên hướng dẫn: Đinh Trường Duy

Sinh viên thực hiện: Vũ Trường Anh – B19DCCN049
Ngô Thị Kiều Oanh – B19DCCN494
Lê Hoàng Dương – B19DCCN149
Lê Văn Hiếu – B19DCCN245
Phạm Xuân Trường – B19DCCN707

Lớp học phần: 04

Nhóm: D1904G03

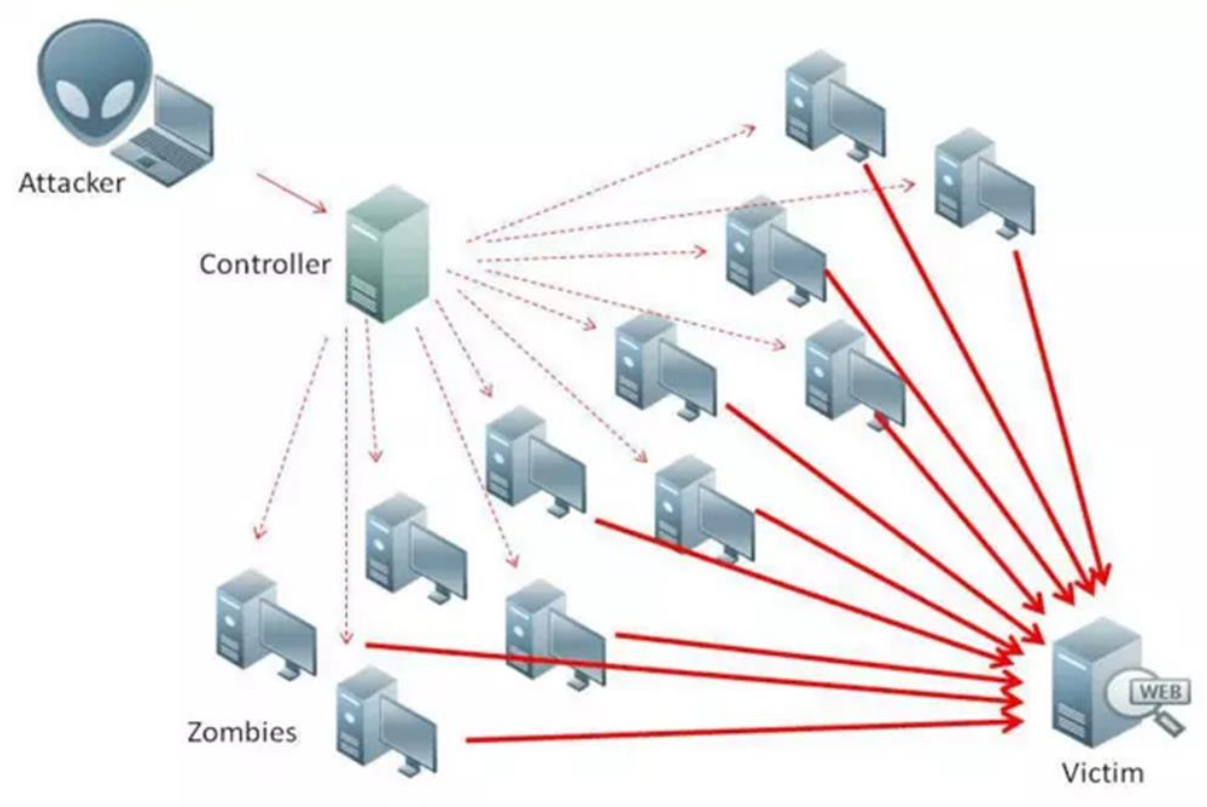
Mục lục

Tấn công DoS

Lời mở đầu:

Mạng của bạn thỉnh thoảng bị chậm bất thường hay mất kết nối đột ngột, nguyên nhân có thể do một cuộc tấn công Denial-of-Service đang được tiến hành, hãy cùng tìm hiểu xem đó là gì? Cách khắc phục như thế nào?

1. Tấn công Denial-of-Service (DoS) là gì?



1.1 Mục đích:

Denial-of-Service (DoS) là một cuộc tấn công nhằm tắt máy hoặc ngắt kết nối, khiến người dùng ngừng truy cập. Các cuộc tấn công DoS thường hoạt động bằng cách áp đảo hoặc làm quá tải mục tiêu với các request cho đến khi không thể xử lý, dẫn đến từ chối dịch vụ cho người dùng. Trong cả hai trường hợp, DoS đều tước quyền sử dụng dịch vụ hoặc tài nguyên hợp pháp của người dùng. Một cuộc tấn công DoS được đặc trưng bằng cách sử dụng một máy tính duy nhất để khởi động cuộc tấn công.

1.2 Mục tiêu

Nạn nhân của các cuộc tấn công DoS thường là email, website, tài khoản trực tuyến... ngoài ra còn có mạng, máy hoặc một chương trình. Mặc dù DoS khó để đánh cắp thông tin quan trọng, nhưng chúng có thể khiến nạn nhân phải mất rất nhiều thời gian và tiền bạc để giải quyết hậu quả. Bởi vì một cuộc tấn công DoS có thể dễ dàng được thực hiện từ bất kỳ đối tượng nào, việc tìm kiếm người chịu trách nhiệm rất khó khăn.

1.3 Phân loại

Có hai phương pháp tấn công DoS: Logic attacks và Flooding attacks.

1.3.1 Logic attacks

- Khai thác các lỗ hổng hệ thống hoặc dịch vụ.

- Làm dịch vụ ngừng hoạt động hoặc giảm hiệu năng hệ thống.

1.3.2 Flooding attacks

- Kẻ tấn công gửi một lượng lớn yêu cầu.

- Gây cạn kiệt tài nguyên hệ thống hoặc băng thông đường truyền mạng.

1.4 Một số kỹ thuật

Có nhiều kỹ thuật tấn công DoS đã được phát hiện trên thực tế. Các kỹ thuật tấn công DoS thường gặp bao gồm: SYN Flood, Smurf, Teardrop, Ping of Death, Land Attacks, ICMP Flood, HTTP Flood, UDP Flood,... Tuy nhiên 2 loại phổ biến nhất là SYN Flood và Smurf.

1.4.1 Tấn công SYN flood

a, Giới thiệu

- Tấn công SYN Flood là kỹ thuật tấn công DoS khai thác điểm yếu trong thủ tục bắt tay 3 bước (3-way handshake).

- Khi bên tham gia truyền thông thiết lập kết nối TCP để bắt đầu 1 phiên trao đổi.

- SYN là bit cờ điều khiển của giao thức TCP dùng để đồng bộ số trình tự gói tin.

- Thủ tục bắt tay khi một người dùng hợp pháp thiết lập một kết nối TCP đến máy chủ.

- Người dùng thông qua máy khách gửi yêu cầu mở kết nối (SYN hay SYN-REQ)
- Máy chủ nhận được lưu yêu cầu kết nối vào Bảng kết nối (Backlog) và gửi lại xác nhận kết nối SYN-ACK cho máy khách;
- Khi nhận được SYN-ACK từ máy chủ, máy khách gửi lại xác nhận kết nối ACK đến máy chủ. Khi máy chủ nhận được xác nhận kết nối ACK từ máy khách, nó xác nhận kết nối mở thành công, máy chủ và máy khách bắt đầu phiên truyền thông TCP. Bản ghi mở kết nối được xóa khỏi Bảng kết nối.

b, Kịch bản tấn công

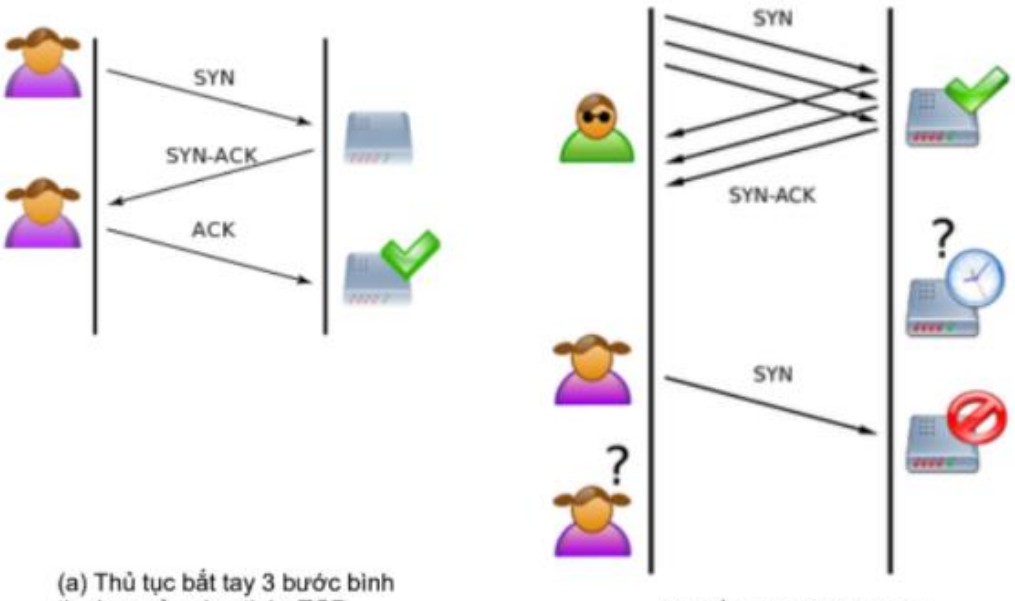
- Kẻ tấn công gửi một lượng lớn yêu cầu mở kết nối (SYN-REQ) đến máy nạn nhân;

- Nhận được yêu cầu mở kết nối, máy nạn nhân lưu yêu cầu kết nối vào Bảng kết nối trong bộ nhớ;

- Máy nạn nhân sau đó gửi xác nhận kết nối (SYN-ACK) đến kẻ tấn công;

- Do kẻ tấn công không gửi lại xác nhận kết nối ACK, nên máy nạn nhân vẫn phải lưu tất cả các yêu cầu kết nối chưa được xác nhận trong Bảng kết nối. Khi Bảng kết nối bị điền đầy thì các yêu cầu mở kết nối của người dùng hợp pháp sẽ bị từ chối;

- Máy nạn nhân chỉ có thể xóa một yêu cầu kết nối đang mở khi nó hết hạn (timed-out).



(a) Thủ tục bắt tay 3 bước bình thường của giao thức TCP

(b) Tấn công SYN Flood

c, Phòng chống

- Sử dụng kỹ thuật lọc địa chỉ giả mạo (Spoofed IP Filtering): Kỹ thuật này đòi hỏi chỉnh sửa giao thức TCP/IP không cho phép kẻ tấn công giả mạo địa chỉ;

- Tăng kích thước Bảng kết nối: Tăng kích thước Bảng kết nối cho phép tăng khả năng chấp nhận các yêu cầu mở kết nối;

- Giảm thời gian chờ (SYN-RECEIVED Timer): Các yêu cầu mở kết nối chưa được xác nhận sẽ bị xóa sớm hơn khi thời gian chờ ngắn hơn;

- SYN cache: Một yêu cầu mở kết nối chỉ được cấp phát không gian nhớ đầy đủ khi nó được xác nhận;

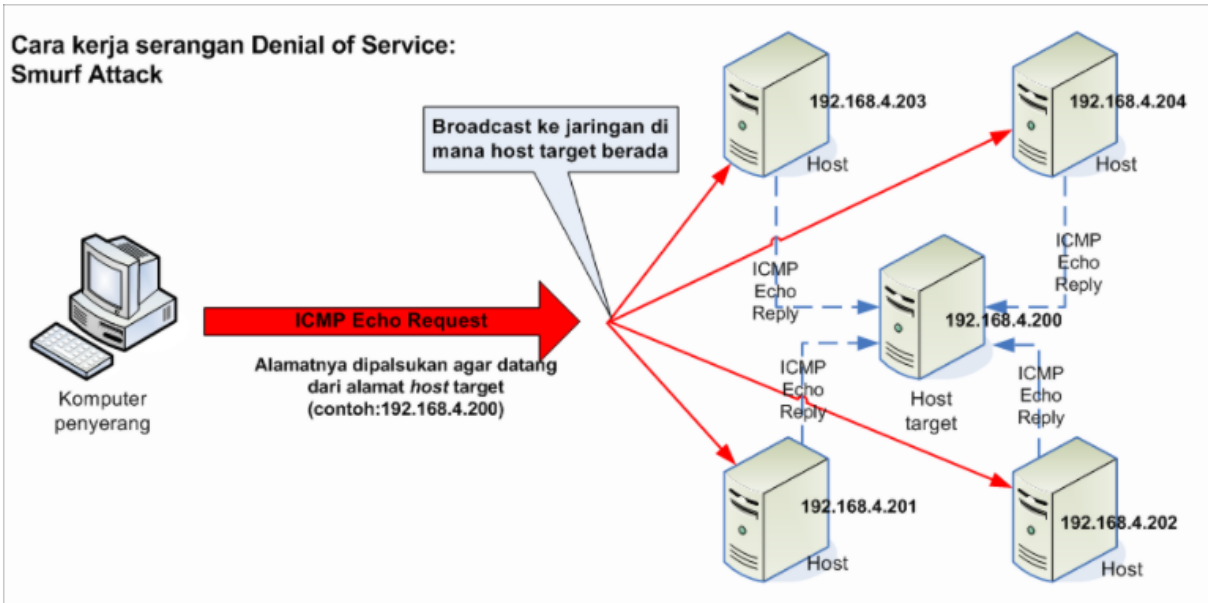
- Sử dụng tường lửa (Firewall) và Proxy: Tường lửa và proxy có khả năng nhận dạng các địa chỉ IP nguồn là địa chỉ không có thực, đồng thời chúng có khả năng tiếp nhận yêu cầu mở kết nối, chờ đến khi có xác nhận mới chuyển cho máy chủ đích.

1.4.2 Tấn công Smurf

a, Giới thiệu

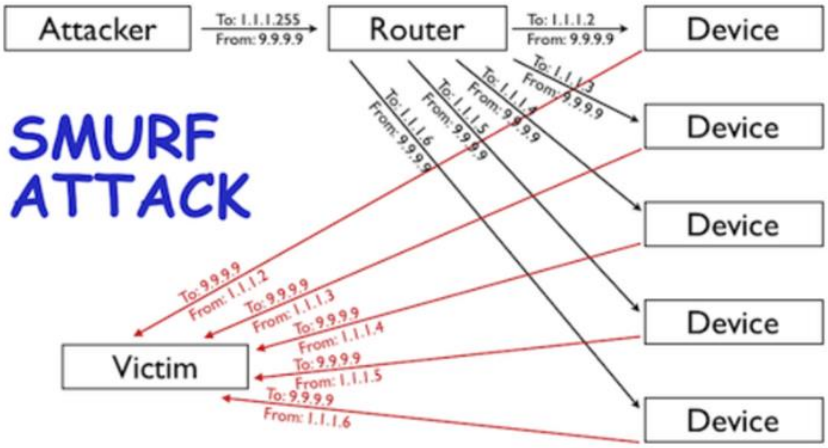
- Smurf attack là dạng tấn công từ chối dịch vụ (DDOS), kẻ tấn công cố gắng tấn công đến máy chủ của nạn nhân bằng gói tin Internet Control Message Protocol (ICMP).

- Bằng cách gửi yêu cầu bằng IP giả mạo máy chủ của nạn nhân và gửi gói tin đến một hoặc nhiều máy tính trong cùng mạng, các máy này sau khi nhận được yêu cầu sẽ phản hồi lại gói tin trả lời đến máy nạn nhân và khuếch đại cuộc tấn công này lên sẽ làm cho máy chủ quá tải và dẫn đến từ chối dịch vụ.



b, Kịch bản tấn công

- Kẻ tấn công gửi một lượng lớn gói tin chứa yêu cầu ICMP (Ping) với địa chỉ IP nguồn là địa chỉ của máy nạn nhân đến một địa chỉ quảng bá (IP Broadcast address) của một mạng;
- Router của mạng nhận được yêu cầu ICMP gửi đến địa chỉ quảng bá sẽ tự động chuyển yêu cầu này đến tất cả các máy trong mạng;
- Các máy trong mạng nhận được yêu cầu ICMP sẽ gửi trả lời (reply) đến máy có địa chỉ IP là địa nguồn trong yêu cầu ICMP (là máy nạn nhân). Nếu số lượng máy trong mạng rất lớn thì máy nạn nhân sẽ bị ngập lụt đường truyền, hoặc ngừng hoạt động.



c, Phòng chống

Có thể sử dụng các biện pháp sau để phòng chống tấn công Smurf:

- Cấu hình các máy trong mạng 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 ICMP 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. Cách DoS attack hoạt động

- Trọng tâm chính của một cuộc tấn công DoS là làm quá tải công suất của máy được nhắm mục tiêu, dẫn đến việc từ chối dịch vụ đối với các yêu cầu bổ sung.

2.1 Triệu chứng

- Có nhiều điểm tương đồng giữa một cuộc tấn công DoS và các lỗi kết nối mạng không độc hại như: Sự cố kỹ thuật mạng, hệ thống bảo trì.. Tuy nhiên, các triệu chứng sau đây có thể chỉ ra một cuộc tấn công DoS:

· Hiệu suất mạng chậm một cách bất thường như tải tệp hoặc website chậm

· Không thể tải bất kỳ website nào

- Mất kết nối đột ngột giữa các thiết bị trên cùng một mạng

2.2 Một số cách Dos attack hoạt động

- Một cuộc tấn công DoS ngăn người dùng truy cập dịch vụ bằng cách làm quá tải các tài nguyên vật lý hoặc kết nối mạng của họ. Cuộc tấn công về cơ bản làm ngập dịch vụ với rất nhiều lưu lượng hoặc dữ liệu mà không ai khác có thể sử dụng cho đến khi luồng độc hại được xử lý.

- Một cách để làm quá tải tài nguyên vật lý của dịch vụ là gửi cho nó rất nhiều yêu cầu trong một thời gian ngắn đến mức nó chiếm hết hard disk space, memory hoặc CPU time có sẵn. Trong trường hợp cực đoan, điều này thậm chí có thể dẫn đến thiệt hại của các thành phần vật lý cho các tài nguyên này.

- Tương tự, để phá vỡ các kết nối mạng của dịch vụ, một cuộc tấn công DoS có thể gửi input không hợp lệ, không đúng định dạng hoặc chỉ là một số lượng lớn yêu cầu kết nối đến nó. Trong khi những điều này đang được giải quyết, các yêu cầu kết nối từ người dùng hợp pháp không thể được hoàn thành.

2.3 Nguyên nhân

Có nhiều nguyên nhân gây ra cuộc tấn công DoS, nhưng phần lớn vì lợi nhuận:

- Rất nhiều trường hợp các cuộc tấn công DoS được đưa ra vì lý do cá nhân. Các dịch vụ bị tấn công có thể bị chậm lại hoặc bị sập trong khoảng thời gian từ vài giờ đến vài ngày. Đối với nhiều doanh nghiệp gây gián đoạn kết nối, thậm chí tổn thất tài chính.

- Vì sự cạnh tranh của công ty hoặc chính trị.

3. Cách ngăn chặn DoS attack

Một quy tắc chung: Bạn càng sớm xác định được một cuộc tấn công đang diễn ra, bạn càng có thể nhanh chóng ngăn chặn thiệt hại. Dưới đây là một số điều bạn có thể làm.

3.1 Phương pháp 1: Dùng các công cụ nhận biết các cuộc tấn công

Các công ty thường sử dụng công nghệ hoặc dịch vụ chống DDoS để giúp tự vệ. Những thứ này có thể giúp bạn nhận ra giữa các đột biến hợp pháp bất thường trong lưu lượng mạng và một cuộc tấn công DDoS.

3.2 Phương pháp 2: Liên hệ với nhà cung cấp dịch vụ Internet

Nếu bạn thấy công ty của mình đang bị tấn công, bạn nên thông báo cho nhà cung cấp dịch vụ Internet của mình càng sớm càng tốt.

3.3 Phương pháp 3: Black hole routing

Các nhà cung cấp dịch vụ Internet có thể sử dụng black hole routing. Nó hướng lưu lượng truy cập quá mức vào một tuyến đường rỗng, còn được gọi là black hole. Điều này có thể giúp ngăn chặn website hoặc mạng mục tiêu bị sập. Cả lưu lượng hợp pháp và bất hợp pháp đều được định tuyến.

3.4 Phương pháp 4: Cấu hình firewalls và routers

Firewalls và routers nên được cấu hình để từ chối lưu lượng không có thật. Hãy cập nhật firewalls và routers với các bản vá bảo mật mới nhất.

3.5 Phương pháp 5: Front-end hardware

Front-end hardware được tích hợp vào mạng trước khi lưu lượng truy cập đến máy chủ có thể giúp phân tích và sàng lọc các gói dữ liệu. Ngoài ra cũng có thể giúp chặn dữ liệu đe dọa.

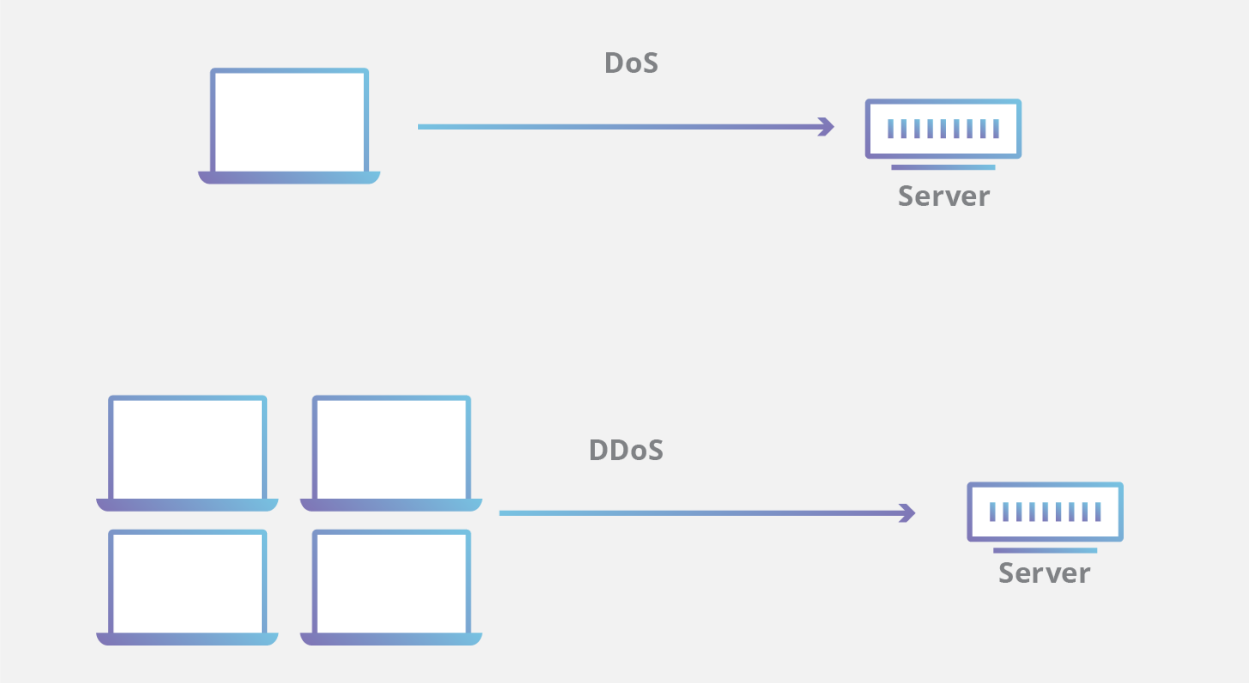
Nếu không có biện pháp phòng vệ đầy đủ, chỉ cần khởi động lại dịch vụ, nhưng có thể không có hiệu quả nếu cuộc tấn công chưa chấm dứt.

Tấn công DDoS

1. Tấn công Distributed Denial of Service (DDoS) là gì?

1.1 Giới thiệu

- DDoS là một dạng tấn công của DoS
- DDoS là một cuộc tấn công khi mà nhiều (hàng ngàn -> triệu) hệ thống cùng tấn công DoS đến một mục tiêu.
- Mục tiêu và mục đích của DDoS tương tự với DoS
- "*All DDoS = DoS but not all DoS = DDoS*"

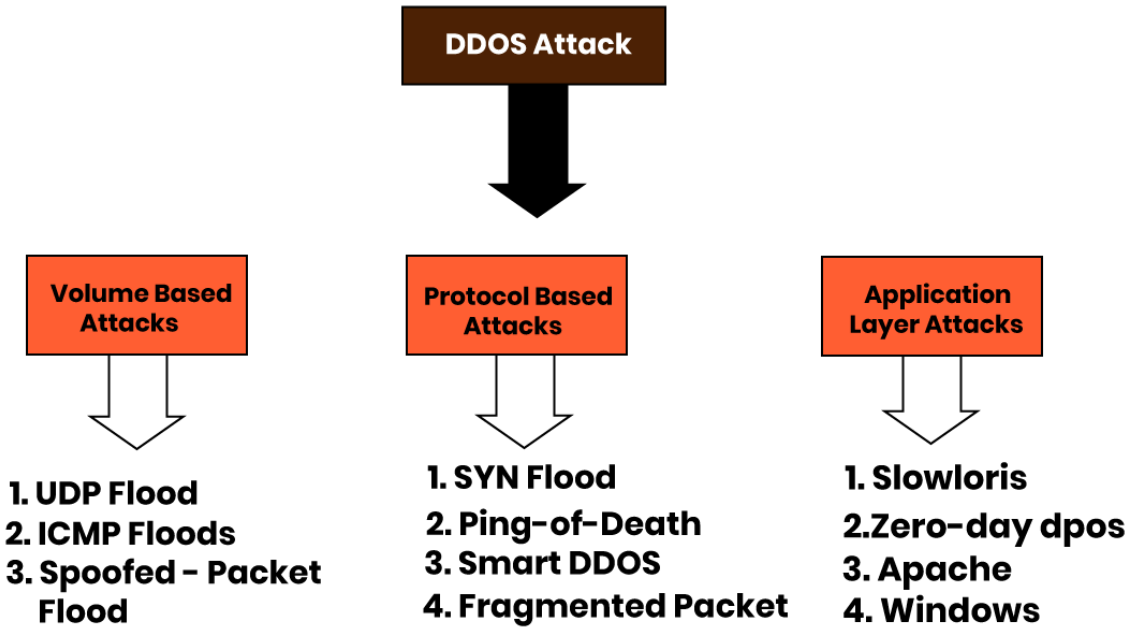


1.2 Phân loại

Tổng quát, tấn công DDoS thường được chia làm 3 loại:

- Volume Based Attacks:
  - Bao gồm: UDP floods, ICMP floods, Spoofed-packet Flood
  - Mục đích: làm nghẽn băng thông của mục tiêu bị tấn công khiến cho các truy cập hợp pháp không thể ra, vào mục tiêu
  - Cường độ tấn công được đo bằng Bps (Bits per second)
- Protocol Attacks:
  - Bao gồm: SYN floods, fragmented packet attacks, Ping of Death, Smurf DDoS, …

    - Mục đích: tiêu hao tài nguyên thật của server, các thiết bị trung gian như firewalls (tường lửa) hay load balancers (bộ cân bằng tải)
    - Cường độ tấn công đo bằng Pps (Packet per second)
- Application Layer Attacks:
    - Bao gồm: low-and-slow attacks, zero-day dpos ,GET/POST floods, các dạng tấn công nhằm vào phần mềm như Apache, Windows, v.v
    - Mục đích: làm sập các ứng dụng (thường là web server) bằng cách gửi các request có vẻ vô hại nhắm vào các điểm yếu của ứng dụng
    - Cường độ tấn công đo bằng Rps (Request per second)



2. Cách hoạt động của DDoS

2.1 Giai đoạn chuẩn bị:

- Chuẩn bị công cụ cho cuộc tấn công, công cụ này thông thường hoạt động theo mô hình Client- Server.
- Tiếp theo, hacker chiếm quyền điều khiển các máy tính trên mạng, tiến hành tải và cài đặt ngầm các chương trình độc hại trên máy tính đó. Để làm được điều này, hacker thường lừa cho người dùng click vào một link quảng cáo có chứa Trojan, worm.
- Kết thúc giai đoạn này, hacker sẽ có một attack-network (botnet)

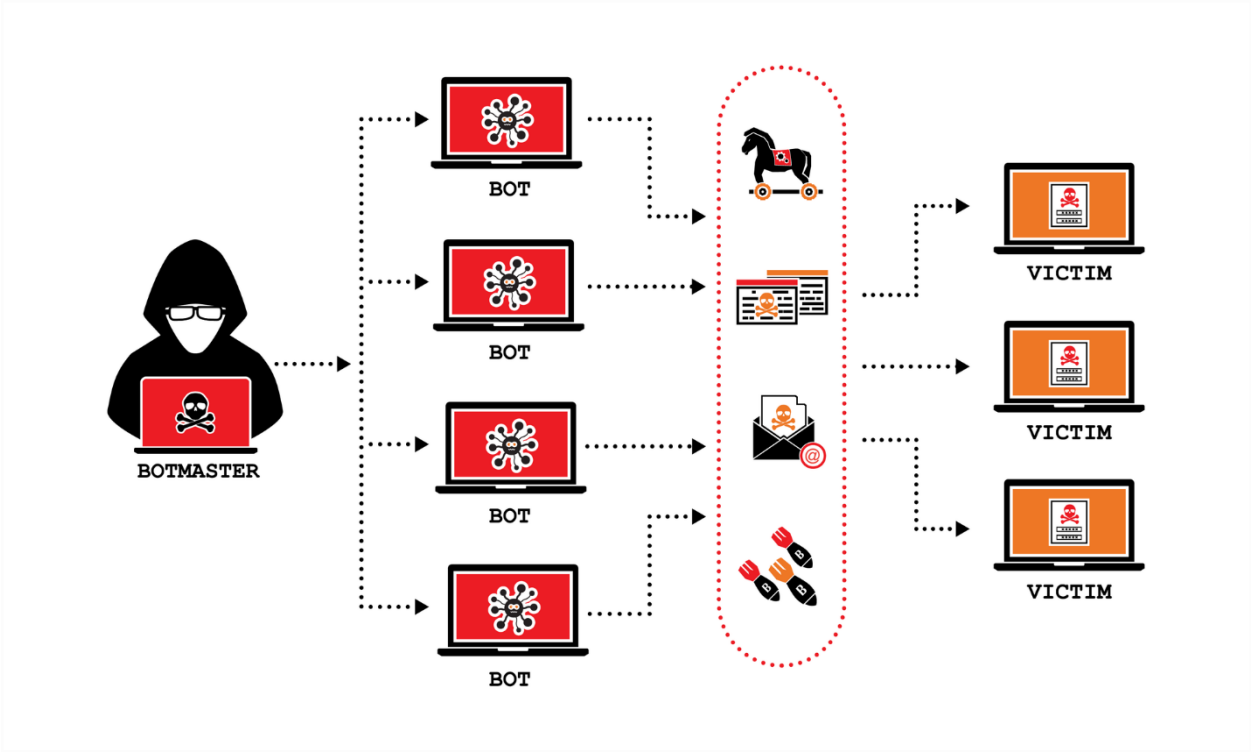
2.2 Giai đoạn xác định mục tiêu và thời điểm tấn công:

- Xác định được mục tiêu cần tấn công.
- Hacker sẽ điều chỉnh attack-network (botnet) chuyển hướng tấn công mục tiêu đó.
- Yếu tố thời điểm sẽ quyết định mức độ thiệt hại của cuộc tấn công.

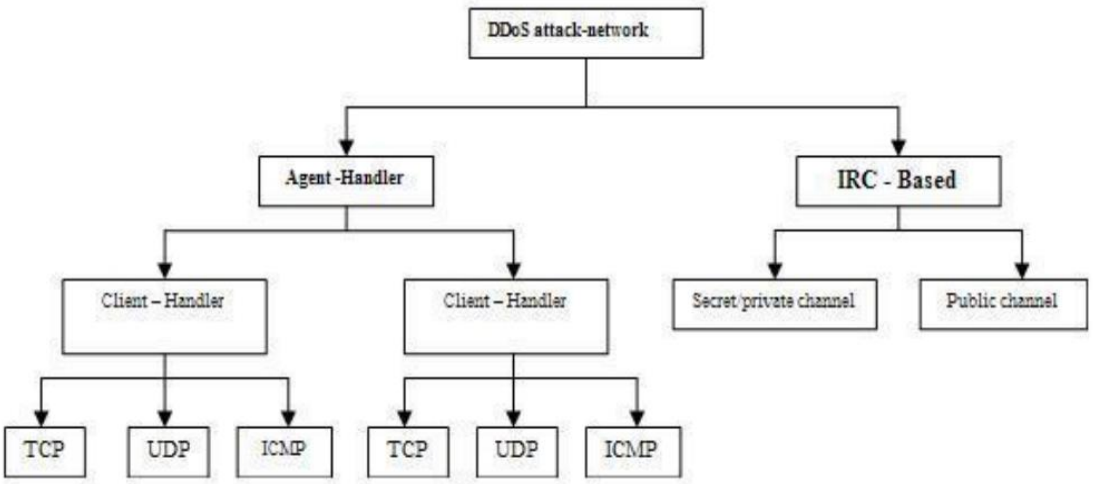
2.3 Giai đoạn phát động tấn công và xóa dấu vết:

- Hacker phát động lệnh tấn công từ máy của mình.
- Toàn bộ attack-network (có thể lên đến hàng ngàn, hàng vạn máy) đồng loạt tấn công mục tiêu, mục tiêu sẽ nhanh chóng bị cạn kiệt băng thông và không thể tiếp tục hoạt động.
- Sau một khoảng thời gian tấn công, hacker tiến hành xóa dấu vết có thể truy ngược đến mình.

***Botnet là gì?** Botnet thuật ngữ đầy đủ là "Bots network" dùng để chỉ một mạng lưới các máy tính bị chi phối bởi ai đó và bị điều khiển bởi một con máy tính khác từ xa. Thường được sử dụng để tấn công DDoS



4. Mô hình tấn công DDoS



Sơ đồ mô hình tấn công DDoS

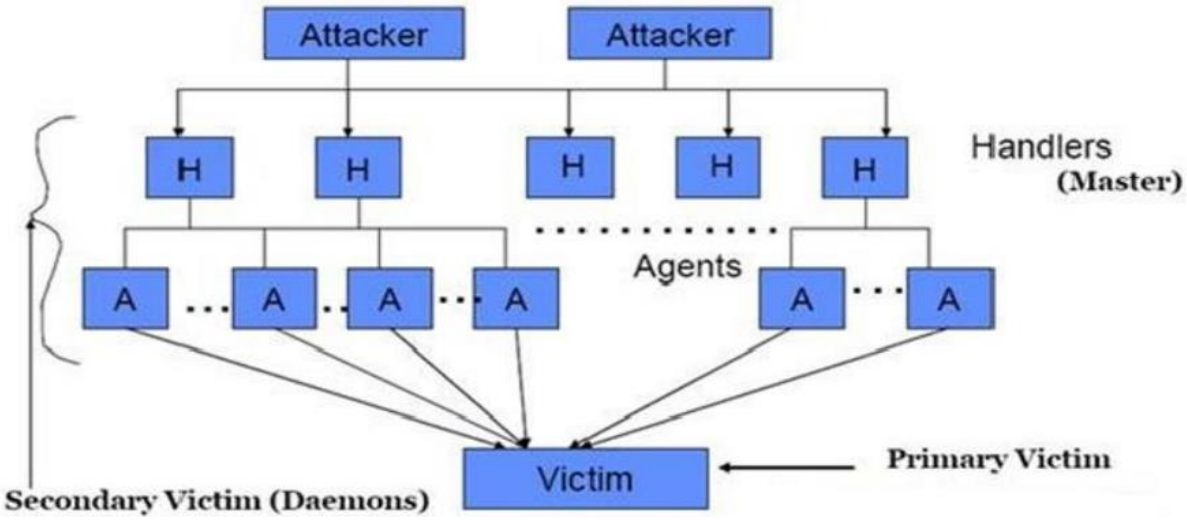
Tấn công DDoS có 2 mô hình chính:

- Mô hình Agent- Handler
- Mô hình IRC- Based

4.1 Mô hình tấn công Agent- Handler

Theo mô hình này, attack- network gồm 3 thành phần chính: Agent, Client và Handler.

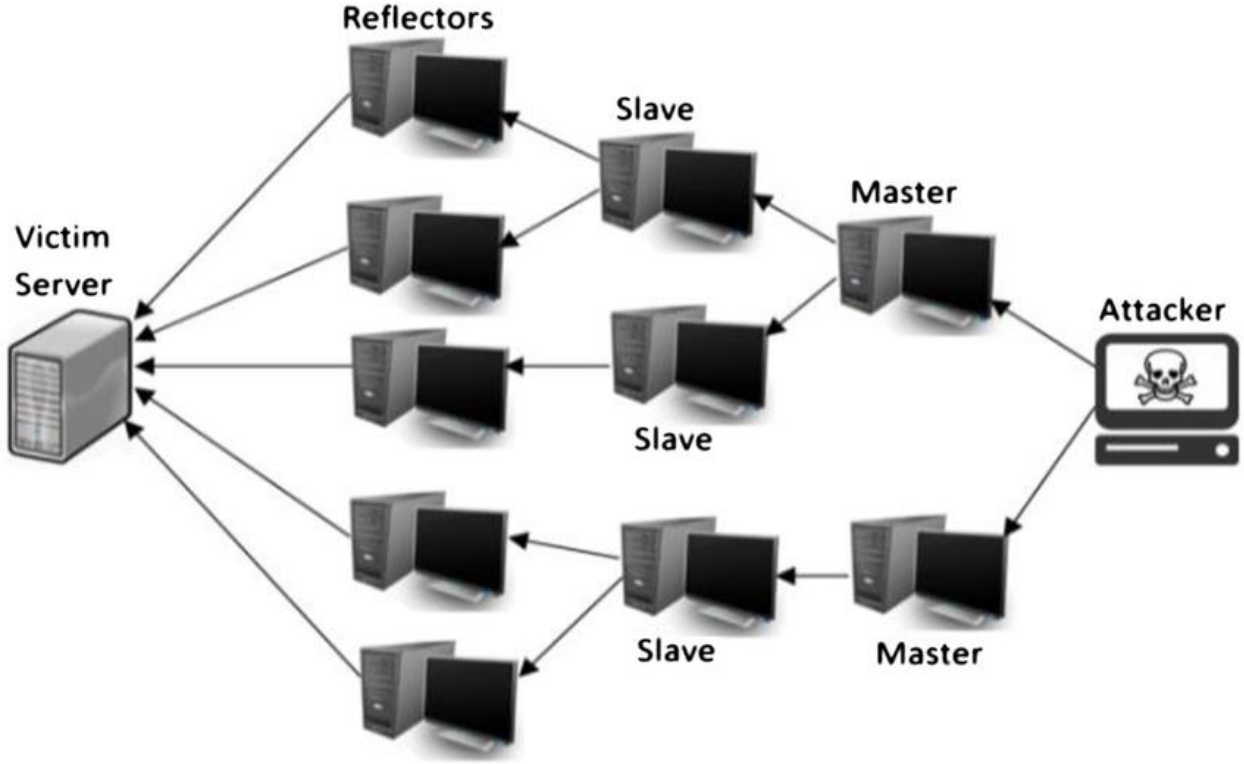
- Client: là phần mềm cơ sở để hacker điều khiển mọi hoạt động của attack-network.
- Handler: là phần mềm trung gian giữa Agent và Client
- Agent: là phần mềm thực hiện tấn công mục tiêu, nhận điều khiển từ Client thông qua các Handler.



Kẻ tấn công sẽ từ Client giao tiếp với các Handler để xác định số lượng Agent đang online, điều chỉnh thời điểm tấn công và cập nhật các Agent. Tùy theo cách kẻ tấn công cấu hình attack- network, các Agent sẽ chịu sự quản lý của một hay nhiều Handler.

Chủ nhân thực sự của các Agent thông thường không hề hay biết họ bị lợi dụng vào cuộc tấn công kiểu DDoS, do họ không đủ kiến thức hoặc các chương trình backdoor Agent chỉ sử dụng rất ít tài nguyên hệ thống nên họ hầu như không thấy ảnh hưởng gì đến hiệu năng của hệ thống.

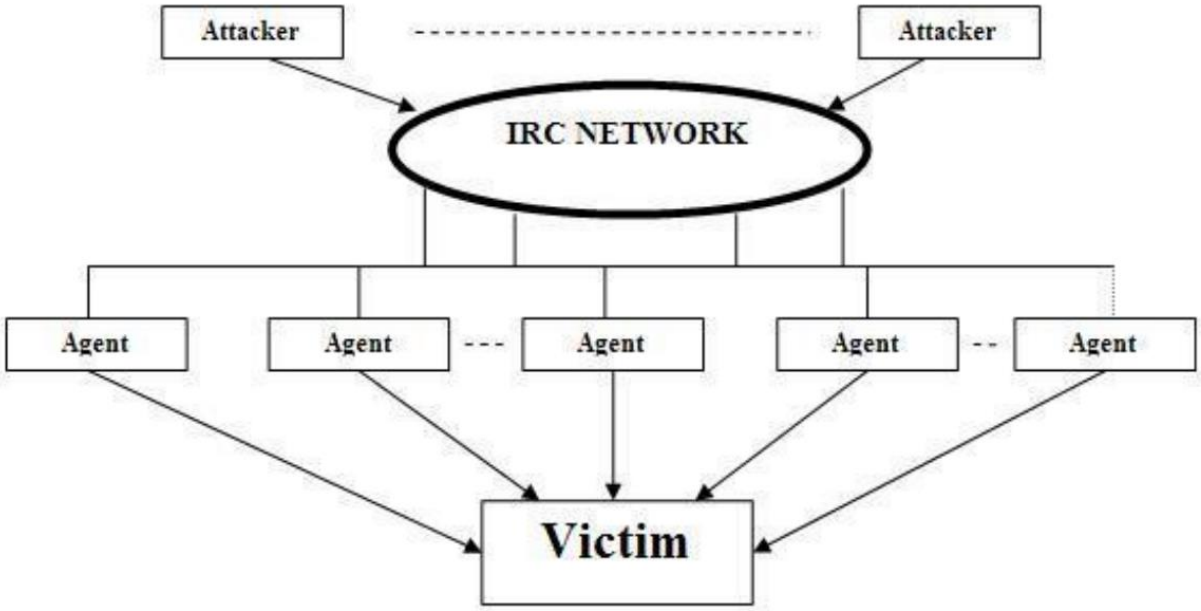
*Mô hình Reflective DDoS attack



- So với mô hình Agent-Handler thì reflective DDoS có thêm các Reflectors:
    - Reflectors là các máy tính trên mạng bình thường nhưng bị gửi các request giả mạo địa chỉ của máy nạn nhân từ đó gửi một lượng lớn reply đến máy nạn nhân => gây ngập lụt máy nạn nhân
- Thường khó để lần vết và phòng chống hơn DDoS bình thường

4.2 Mô hình tấn công IRC- Based

- Internet Relay Chat (IRC) là một hệ thống online chat multi-user (hệ thống trò chuyện trực tuyến đa người dùng). IRC cho phép người dùng tạo một kết nối đến nhiều server khác và chat thời gian thực.
- Kiến trúc của IRC network bao gồm nhiều IRC server trên khắp internet, giao tiếp với nhau trên nhiều kênh (channel). IRC network cho phép người dùng tạo 3 loại channel: public, private và secret.



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, kẻ tấn công còn có thêm một số lợi thế như:

- Các giao tiếp dưới dạng chat message làm cho việc phát hiện chúng là vô cùng khó khăn.
- Các message 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 đang nhập vào IRC server là có thể nhận được các báo cáo về trạng thái các Agent do các channel gửi về.

5. Phòng chống cuộc tấn công DDoS

Giải pháp tổng thể về phòng, chống DDOS được chia thành 3 giai đoạn chính:

(1) Giai đoạn ngăn ngừa: Tối thiểu hóa lượng Agent, tìm và vô hiệu hoá Handler.

(2) Giai đoạn đối đầu với cuộc tấn công: Phát hiện và ngăn chặn cuộc tấn công, làm suy giảm và dừng cuộc tấn công, chuyển hướng cuộc tấn công.

(3) Giai đoạn sau khi cuộc tấn công xảy ra: thu thập chứng cứ và rút kinh nghiệm.

Các cách để phòng chống DDoS

- Người dùng tự bảo vệ mình bằng các phần mềm chống virus, mã độc để tránh bị lây nhiễm => giảm số lượng slaves(zombie)
- Ngăn cản việc gửi lệnh, giao tiếp giữa Handler và Agent từ đó ngăn cuộc tấn công xảy ra.

Tài liệu tham khảo:

- What is a denial of service attack (DoS) ?
- What is a Denial-of-Service (DoS) Attack?
- What are Denial of Service (DoS) attacks? DoS attacks explained
- Denial of Service (DoS)

- https://www.imperva.com/learn/ddos/ddos-attacks/
- https://repository.vnu.edu.vn/bitstream/VNU_123/8236/5/LuanVan_NguyenThanhHuu.pdf