HỌC VIỆN KỸ THUẬT MẬT MÃ

**KHOA AN TOÀN THÔNG TIN**



BÁO CÁO MÔN HỌC

**KỸ THUẬT LẬP TRÌNH**

**Đề tài:**

**TẤN CÔNG DDOS VÀ CÁCH PHÒNG CHỐNG**

Hà Nội, 2-2023

HỌC VIỆN KỸ THUẬT MẬT MÃ

**KHOA AN TOÀN THÔNG TIN**



BÁO CÁO MÔN HỌC

**KỸ THUẬT LẬP TRÌNH**

**Đề tài:**

**TẤN CÔNG DDOS VÀ CÁCH PHÒNG CHỐNG**

Sinh viên thực hiện: TẠ XUÂN CƯỜNG – AT170107

THÁI HOÀNG LONG – AT170130

ĐỖ CÔNG MINH – AT170634

CAO ĐẮC QUÂN – AT170640

Nhóm 12

Hà Nội, 2-2023

# **MỤC LỤC**

[MỤC LỤC iii](#_Toc128551172)

[DANH MỤC VIẾT TẮT v](#_Toc128551173)

[DANH MỤC HÌNH ẢNH vi](#_Toc128551174)

[TÓM TẮT NỘI DUNG ĐỀ TÀI vii](#_Toc128551175)

[LỜI NÓI ĐẦU viii](#_Toc128551176)

[CHƯƠNG 1: TỔNG QUAN VỀ TẤN CÔNG TỪ CHỐI DỊCH VỤ PHÂN TÁN (DDOS) 1](#_Toc128551177)

[1.1 Định nghĩa cuộc tấn công DDoS 1](#_Toc128551178)

[1.2 Đặc trưng của cuộc tấn công DDoS 2](#_Toc128551179)

[1.3 Tìm hiểu về mạng Botnet 2](#_Toc128551180)

[1.3.1 Khái niệm về mạng Botnet 2](#_Toc128551181)

[1.3.2 Quy trình hoạt động của Botnet 3](#_Toc128551182)

[1.3.3 Mạng IRC botnet 3](#_Toc128551183)

[1.4 Các giai đoạn của một cuộc tấn công DDoS 4](#_Toc128551184)

[1.4.1 Giai đoạn chuẩn bị 4](#_Toc128551185)

[1.4.2 Giai đoạn xác định mục tiêu và thời điểm tấn công 4](#_Toc128551186)

[1.4.3 Giai đoạn phát động tấn công và xóa dấu vết 4](#_Toc128551187)

[1.5 Phân loại tấn công DDoS 4](#_Toc128551188)

[1.5.1 Tấn công chiếm băng thông 5](#_Toc128551189)

[1.5.2 Chiếm tài nguyên 5](#_Toc128551190)

[CHƯƠNG 2: CÁC KỸ THUẬT TẤN CÔNG DDOS PHỔ BIẾN 6](#_Toc128551191)

[2.1 Tấn công làm tràn băng thông (Flood Attack) 6](#_Toc128551192)

[2.1.1 SYN Flood Attack 6](#_Toc128551193)

[2.1.2 UDP Flood Attack 8](#_Toc128551194)

[2.2 Smurf Attack 9](#_Toc128551195)

[2.3 Application Layer Attack 10](#_Toc128551196)

[2.3.1 HTTP Flood Attack 10](#_Toc128551197)

[2.3.2 Slowloris Attack 11](#_Toc128551198)

[CHƯƠNG 3: CÁCH PHÒNG CHỐNG CUỘC TẤN CÔNG DDOS 12](#_Toc128551199)

[3.1 Giai đoạn phát hiện và ngăn ngừa 12](#_Toc128551200)

[3.1.1 Ngăn ngừa một cuộc tấn công DDoS 12](#_Toc128551201)

[3.1.2 Phát hiện một cuộc tấn công DDoS 12](#_Toc128551202)

[3.2 Giai đoạn đối đầu và sau một cuộc tấn công 12](#_Toc128551203)

[3.2.1 Làm suy giảm hay dừng cuộc tấn công 12](#_Toc128551204)

[3.2.2 Giai đoạn sau một cuộc tấn công 13](#_Toc128551205)

[3.3 Giai đoạn đánh giá mức độ thiệt hại 13](#_Toc128551206)

[3.3.1 Throughput 13](#_Toc128551207)

[3.3.2 Round-trip Time 13](#_Toc128551208)

[3.3.3 Packet Loss 13](#_Toc128551209)

[3.3.4 CPU Utilization 13](#_Toc128551210)

[3.3.5 Jitter 13](#_Toc128551211)

[3.4 Các giải pháp đơn giản phòng chống một cuộc tấn công 14](#_Toc128551212)

[3.4.1 Cài đặt bản bảo mật mới nhất 14](#_Toc128551213)

[3.4.2 Vô hiệu hóa IP broadcast 14](#_Toc128551214)

[3.4.3 Firewall 14](#_Toc128551215)

[3.5 Một số công cụ phòng chống tấn công DDoS phổ biến 15](#_Toc128551216)

[3.5.1 CloudFlare 15](#_Toc128551217)

[3.5.2 Vietnix Firewall 15](#_Toc128551218)

[3.5.3 SolarWinds Security Event Manager 16](#_Toc128551219)

[CHƯƠNG 4: THỰC NGHIỆM TẤN CÔNG DDOS 17](#_Toc128551220)

[4.1 Mô hình thực nghiệm 17](#_Toc128551221)

[4.2 Kịch bản 17](#_Toc128551222)

[4.2.1 SYN-Flood Attack 17](#_Toc128551223)

[4.2.2 ICMP Flood Attack 22](#_Toc128551224)

[4.2.3 HTTP Flood Attack 24](#_Toc128551225)

[4.3 Kết luận chung: 26](#_Toc128551226)

[KẾT LUẬN 27](#_Toc128551227)

[TÀI LIỆU THAM KHẢO 28](#_Toc128551228)

[PHỤ LỤC 29](#_Toc128551229)

# **DANH MỤC VIẾT TẮT**

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Từ viết tắt** | **Tên đầy đủ** | **Giải thích** |
| **1** | IP | Internet Protocol | Giao thức trên Internet. |
| **2** | OSI | Open Systems Interconnection Reference Model | Mô hình tham chiếu kết nối các hệ thống mở. |
| **3** | TCP | Transmission Control Protocol | Giao thức điều khiển truyền vận, là một trong các giao thức cốt lõi của bộ giao thức TCP/IP, thuộc tầng 4 - vận chuyển. |
| **4** | HTTP | HyperText Transfer Protocol | Giao thức truyền tải siêu văn bản, là một giao thức thuộc tầng 7 - ứng dụng cho các hệ thống thông tin phân tán, công tác. |
| **5** | CPU | Central Processing Unit | Bộ xử lý trung tâm. |
| **6** | UDP | User Datagram Protocol | Là giao thức giao tiếp thay thế cho TCP, được sử dụng chủ yếu để thiết lập các kết nối có độ trễ thấp và không chịu lỗi giữa các ứng dụng. |
| **7** | SYN | Synchoronize | Là một trong các gói dự liệu trong quá trình bắt tay ba bước. |
| **8** | ACK | Acknowledgement | Là một trong các gói dự liệu trong quá trình bắt tay ba bước. |
| **9** | ICMP | Internet Control Message Protocol | Là một giao thức thuộc tầng 3 – Network, được sử dụng để truyền các thông điệp điều khiển giữa máy chủ và bộ định tuyến. |
| **10** | FTP | File Transfer Protocol | Là giao thức truyền tải tập tin, được dùng trong việc trao dổi dữ liệu trong các mạng, thuộc tầng 7 - ứng dụng. |
| **11** | PoP | Post Office Protocol | Giao thức tiêu chuẩn được sử dụng bởi các mail client để truy xuất email từ xa từ mail server qua kết nối TCP/IP. |

# **DANH MỤC HÌNH ẢNH**

[Hình 1.1: Mô hình tấn công DDoS 1](#_Toc128551296)

[Hình 1.2: Mô hình mạng lưới Botnet 2](#_Toc128551297)

[Hình 1.3: Mô hình IRC Botnet 3](#_Toc128551298)

[Hình 1.4: Sở đồ phân loại DDoS attack theo mục đích tấn công 4](#_Toc128551299)

[Hình 2.1: Mô hình Bắt tay ba bước (Three-way Handshake) 6](#_Toc128551300)

[Hình 2.2: Mô hình Tấn công SYN Flood 7](#_Toc128551301)

[Hình 2.3: Mô hình Tấn công UDP Flood 8](#_Toc128551302)

[Hình 2.4: Mô hình Smurf Attack 9](#_Toc128551303)

[Hình 2.5: Mô hình Tấn công HTTP Flood 10](#_Toc128551304)

[Hình 2.6: Mô hình Slowloris Attack 11](#_Toc128551305)

[Hình 3.1: Mô hình Firewall 14](#_Toc128551306)

[Hình 3.2: Mô hình phóng chống DDoS của CloudFlare 15](#_Toc128551307)

[Hình 3.3: Mô hình Vietnix Firewall 16](#_Toc128551308)

[Hình 3.4: Giao diện SolarWinds Security Event Manager 16](#_Toc128551309)

[Hình 4.1: Mô hình thực nghiệm 17](#_Toc128551310)

[Hình 4.2: Địa chỉ IP máy tấn công 17](#_Toc128551311)

[Hình 4.3: Địa chỉ IP máy chủ 17](#_Toc128551312)

[Hình 4.4: Câu lệnh Nmap và kết quả 18](#_Toc128551313)

[Hình 4.5: Câu lệnh tấn công SYN-Flood 19](#_Toc128551314)

[Hình 4.6: Công cụ Wireshark chụp lại gói tin (1) 19](#_Toc128551315)

[Hình 4.7: Công cụ Wireshark chụp lại gói tin (2) 19](#_Toc128551316)

[Hình 4.8: Công cụ Wireshark chụp lại gói tin (3) 20](#_Toc128551317)

[Hình 4.9: Thông số Sử dụng CPU khi bị tấn công 21](#_Toc128551318)

[Hình 4.10: Thông số lưu lượng mạng khi bị tấn công 21](#_Toc128551319)

[Hình 4.11: Câu lệnh Nmap và kết quả 22](#_Toc128551320)

[Hình 4.12: Câu lệnh tấn công ICMP-Flood 23](#_Toc128551321)

[Hình 4.13: Công cụ Wireshark trên máy tấn công ICMP Flood 23](#_Toc128551322)

[Hình 4.14: Thống số lưu lượng mạng khi bị tấn công 24](#_Toc128551323)

[Hình 4.15: Trang web trước khi bị tấn công 24](#_Toc128551324)

[Hình 4.16: Công cụ đang khởi chạy trên máy tấn công 25](#_Toc128551325)

[Hình 4.17: Công cụ Wireshark đang chụp lại các gói tin 25](#_Toc128551326)

[Hình 4.18: Website đã bị sập khi truy cập bằng máy tấn công 26](#_Toc128551327)

# **TÓM TẮT NỘI DUNG ĐỀ TÀI**

* Giới thiệu tổng quát về DDoS và các thành phần tham gia, tóm tắt các giai đoạn của một cuộc tấn công DDoS, phân loại các cuộc tấn công DDoS.
* Giới thiệu và phân tích cụ thể một số loại DDoS phổ biến.
* Phân tích các giai đoạn khi bị tấn cống và các cách để nhận biết cũng như phòng chống DDoS, giới thiệu một số công cụ phóng chống DDoS phổ biến.
* Triển khai thực nghiệm tấn công DDoS bằng 3 phương pháp phổ biến là SYN-Flood Attack, ICMP Flood Attack và HTTP Flood Attack vào máy chủ ảo và đánh giá.

# **LỜI NÓI ĐẦU**

Ngày nay với sự phát triển của mạng Internet, mọi người được kết nối với nhau dễ dàng hơn. Công việc cũng như nhiều hoạt động mua bán, trao đổi thông tin, giao dịch đa số đều thực hiện trên mạng Internet. Cùng sự phát triển đó là các sự số của các cuộc tấn công trực tuyến cũng tăng lên đáng kể và ngày càng phức tạp, tinh vi hơn nhiều so với các cuộc tấn công trong quá khứ Vì vậy nên các cuộc tấn công mạng ngày càng phổ biến và các kiểu tấn công cũng đa dạng nguy hiểm gây thiệt hại lớn qua mạng. Một trong những cuộc tấn cống trực tuyến có mức độ gây thiệt hại lớn là cuộc tấn công từ chối dịch vụ phân tán (DDoS - viết tắt của Distributed Denial of Service).

Vì vậy, để nhận biết được một cuột tấn công DDoS, cũng như phòng chống và giảm thiểu thiệt hại đến mức độ nhỏ nhất có thể. Chúng ta cần hiểu biết được tấn công DDoS là gì và cách chúng hoạt động như thế nào. Từ đó chung ta có thể tìm được cách biện pháp và công cụ để phòng chống cũng như giảm thiểu thiệt hại mà cuộc tấn công DDoS gây ra. Để giải quyết các vấn đề này, chúng em chọn đề tài “Tấn công DDoS và cách phòng chống” để có thể giới thiệu mọi người hiểu biết thêm về DDoS và các cách hạn chế và phòng chống một cuộc tấn công DDoS.

Trong đề tài này, chúng em sẽ tìm hiểu về tấn công DDoS, các thành phần tham gia và cách thức thực hiện của chúng. Tìm hiểu về các loại tấn công DDoS và cách phòng chống, bao gồm cách phát hiện và ngăn chặn tấn công trước khi nó gây ra tổn thất nghiêm trọng. Ngoài ra, chúng ta cũng sẽ tìm hiểu về những công cụ và kỹ thuật mới nhất được sử dụng để đối phó với tấn công DDoS.

# **CHƯƠNG 1: TỔNG QUAN VỀ TẤN CÔNG TỪ CHỐI DỊCH VỤ PHÂN TÁN (DDOS)**

* 1. **Định nghĩa cuộc tấn công DDoS**

Tấn công từ chối dịch vụ (Denial of Service Attack) là một loại tấn công mạng được sử dụng để tối đa hóa số lượng các yêu cầu gởi đến một máy chủ. Điều này có thể dẫn đến việc hệ thống bị tắc nghẽn bởi vì bị tận dụng tới mức tối đa khiến cho người dùng hợp pháp không thể truy cập vào tài nguyên và dịch vụ của máy chủ. Mục đích chính của cuộc tấn công là vô hiệu hóa việc sử dụng dịch vụ trên Internet hoặc một mạng nào đó đã được kẻ tấn công nhắm tới. Thông thường, cuộc tấn công này có thể được phát hiện từ xa.

Tấn công từ chối dịch vụ phân tán (Distributed Denial of Service Attack - DDoS) là một cải tiến của cuộc tấn công DoS, cả hai loại tấn công đều có mục đích làm cạn kiệt tài nguyên của mạng bị tấn công khiến hệ thống trì trệ và có thể dẫn đến ngưng hoạt động. Hacker sử dụng một số lượng khổng lồ các gói tin từ nhiều máy phân tán (điểm khác nhau giữa DDoS và DoS) với các địa chỉ IP khác nhau để gửi tới máy cần tấn công.

Diagram

Description automatically generated

#### **Hình 1.1: Mô hình tấn công DDoS**

Thông thường có 4 thành phần trong một cuộc tấn công DDoS:

* Real Attacker: kẻ tấn công
* Host Computer/Victim: máy nạn nhân
* Master Control Program: chương trình điều khiển các Zombies
* Zombies: các máy đã bị Attacker chiếm dụng để thực hiện tấn công**.**
  1. **Đặc trưng của cuộc tấn công DDoS**

Một số đặc trưng của cuộc tấn công DDoS:

* Sử dụng một số lượng hàng trăm hàng ngàn máy tính để tấn công hay còn thường được gọi là Botnet.
* Có 2 dạng nạn nhân “Primary Victim” và “Secondary Victim”:
  + Primary Victim: nạn nhân chịu ảnh hưởng của cuộc tấn công.
  + Secondary Victim: những máy tính bị sử dụng để phát động những cuộc tấn công vào chính nó.
* Tấn công DDoS có thể rất khó để truy ngược kẻ tấn công bởi có rất nhiều máy tính tham gia, và kẻ tấn công có thể giả mạo địa chỉ IP để lẩn trốn.
* Phòng chống tấn công là rất khó bởi số lượng các máy tấn công tham gia. Cấu hình tường lửa để chặn một vài IP là có thể nhưng với số lượng lớn các địa chỉ IP độc hại được tạo ra bởi hàng ngàn Zombies thì gần như không thể xác định và ngăn chặn.
* Sự ảnh hưởng của tấn công DDoS là lớn hơn nhiều so với tấn công DoS.
  1. **Tìm hiểu về mạng Botnet**
     1. **Khái niệm về mạng Botnet**

Botnet là một mạng gồm từ hàng trăm tới hàng triệu máy tính hoàn toàn mất quyền kiểm soát. Các máy tính này vẫn hoạt động bình thường, nhưng chúng không hề biết rằng đã bị các hacker kiểm soát và điều khiển. Các máy tính này có thể bị hacker lợi dụng để tải về các chương trình quảng cáo, hay cùng đồng loạt tấn công một trang web nào đó mà ta gọi là DDoS. Hầu hết chủ của những máy tính này không hề biết rằng hệ thống của họ đang được sử dụng theo cách này. Khi đã chiếm được quyền điều khiển, hacker sẽ xâm nhập vào các hệ thống này, ấn định thời điểm và phát động tấn công từ chối dịch vụ. Với hàng triệu các máy tính cùng tấn công vào một thời điểm, nạn nhân sẽ bị ngốn hết băng thông trong nháy mắt, dẫn tới không thể đáp ứng các yêu cầu hợp lệ và bị loại khỏi internet.

Diagram

Description automatically generated

#### **Hình 1.2: Mô hình mạng lưới Botnet**

* + 1. **Quy trình hoạt động của Botnet**

Đánh vào những lỗ hổng an ninh, những bản vá cũ hay những server đã lỗi thời, các Bot ẩn mình trong các máy tính của khách hàng – kết nối sẵn với Botmaster, chỉ đợi lệnh và điều khiển từ Bot Master để tiến hành hoạt động của mình. Sau khi nhận lệnh từ Hacker, mỗi Bot có một hoạt động riêng tùy theo sự điều khiển từ phía ngoài. Nó có thể tấn công theo nhiều cách như là: Tạo Spam, tấn công DDoS, chiếm giữ hệ thống, lừa đảo ăn cắp thông tin. Dù cách tấn công như nào thì mục đích cuối cùng của nó cũng chỉ là điều khiển hoạt động của máy tính bị nhiễm, bắt buộc người dùng phải làm theo mệnh lệnh của nó.

Nếu ta tấn công ngược lại Botnet thì cũng không thể đánh sập lại hệ thống máy chủ, mà đôi khi lại gặp những nạn nhân bị nhiễm khác, giống như hoạt động lặp lại pear – to – pear. Các máy tính bị nhiễm liên kết với nhau lại tạo thành mạng Botnet và càng khó khăn hơn trong việc tìm ra mạng điều hành phía sau.

* + 1. **Mạng IRC botnet**

Internet Relay Chat (IRC) là một hệ thống online chat nhiều người. IRC cho phép người sử dụng tạo một kết nối đến nhiều điểm khác với nhiều người sử dụng khác nhau 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 user tạo ba loại channel: Public, Private và Secret. Trong đó:

* Public channel: cho phép user của channel đó thấy IRC name và nhận được message của mọi user khác trên cùng một channel.
* Private channel: Được thiết kế để giao tiếp với các đối tượng cho phép. Không cho phép các user không cùng một 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.
* Secret channel: Tương tự như private channel nhưng không thể xác định bằng channel locator.

Diagram

Description automatically generated

#### **Hình 1.3: Mô hình IRC Botnet**

Các bot IRC được coi như một người dùng thông thường. Chúng có thể chạy tự động một số thao tác. Quá trình điều khiển các bot này thông thường dựa trên việc gửi lệnh để thiết lập kênh liên lạc do hacker thực hiện, với mục đích chính là phá hoại. Tất nhiên, việc quản trị bot cũng đòi hỏi cơ chế thẩm định và cấp phép. Vì thế, chỉ có chủ sở hữu chúng mới có thể sử dụng.

Một thành phần quan trọng của các bot này là những sự kiện mà chúng có thể dùng để phát tán nhanh chóng tới máy tính khác. Xây dựng kế hoạch cần thận cho chương trình tấn công sẽ giúp thu được kết quả tốt hơn với thời gian ngắn hơn. Một số *n* bot kết nối vào một kênh đơn để chờ lệnh từ kẻ tấn công thì được gọi là một botnet.

* 1. **Các giai đoạn của một cuộc tấn công DDoS**
     1. **Giai đoạn chuẩn bị**

Hacker chuẩn bị bằng cách tự xây dựng công cụ phù hợp hoặc tìm kiếm chúng và tải về trên mạng Internet để phục vụ cho việc tấn công, các công cụ thường hoạt động theo mô hình Client – Server.

Tiếp theo, hacker sẽ tiến hành phát tán và ngầm cài đặt các phần mềm độc hại vào các máy tính trên mạng và chiếm quyền điều khiển chúng để xây dựng một mạng lưới tấn công (Attack – Network), một mạng lưới có thể lên tới hàng ngàn, hàng vạn máy. Để làm được việc nay, hacker sẽ lừa người dùng click vào một đường link có chứa Trojan hoặc worm.

* + 1. **Giai đoạn xác định mục tiêu và thời điểm tấn công**

Hacker xác định mục tiêu cần tấn công và điều chỉnh mạng lưới Botnet của mình chuyển hướng tấn công vào mục tiêu đó.

Thời điểm thường là yếu tố quan trọng sẽ quyết định mức độ thiệt hại mà cuộc tấn công có thể gây ra.

* + 1. **Giai đoạn phát động tấn công và xóa dấu vết**

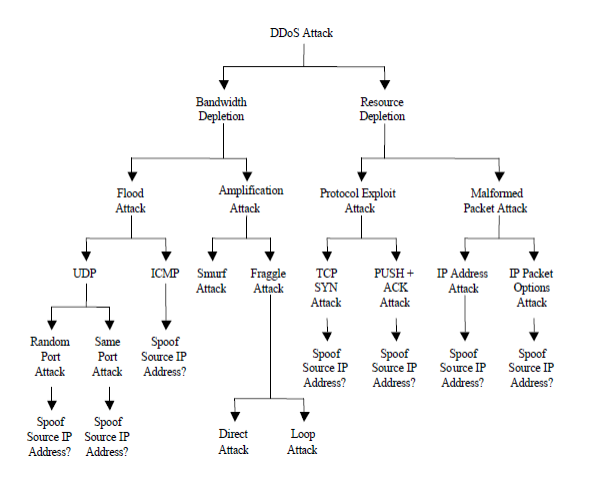
Khi đến thời điểm đã được định, hacker phát độc tấn công từ máy của mình để điều kiển mạng lưới Botnet cùng đồng loạt tấn công mục tiêu, mục tiêu sẽ nhanh chóng bị cạn kiệt băng thông và không thể tiếp tục hoạt động.

Sau khi tấn công xong, hacker sẽ tiến hành xóa dấu vết có thế truy ngược đến mình, nhưng việc này đòi hỏi hacker phải có trình độ cao.

* 1. **Phân loại tấn công DDoS**

Không phải tất cả các cuộc tấn công DDoS đều giống nhau. Tấn công DDoS có thể chia ra làm 2 loại, nó phụ thuộc vào cách thức thực hiện của hacker:

* Chiếm băng thông (Consumption of Bandwith)
* Chiếm tài nguyên của hệ thống (Consumption of Resources)



#### **Hình 1.4: Sở đồ phân loại DDoS attack theo mục đích tấn công**

Cũng có thể phân loại tấn công DDoS dựa trên mô hình OSI 7 tầng. Xu hướng các cuộc tấn công DDoS cho thấy thủ phạm thường biến đổi các cuộc tấn công theo mô hình OSI. Các cuộc tấn công được phân loại như sau:

* 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.

Ngày nay, hệ thống phòng thủ DDoS liên tục được hoàn thiện và đa dạng, nhưng thường tập trung ở tầng thấp trong mô hình OSI. Do đó các cuộc tấn công vào lớp ứng dụng (Lớp 7) đang ngày càng phổ biến.

* + 1. **Tấn công chiếm băng thông**

Chiếm băng thông là một trong những tấn công DDoS phổ biến nhất. Mục đích của loại tấn công này là làm cạn kiệt băng thông ra và vào của máy chủ bị tấn công khiến cho người dùng không thể truy cập tài nguyên hoặc gây ra sự khó chịu cho người dùng bởi sự chậm tễ. Các hình thức tấn công nổi tiếng của cuộc tấn công chiếm băng thông:

* Smurf Attack
* Flood Attack
  + 1. **Chiếm tài nguyên**

Loại tấn công này giống với tấn công chiếm băng thông. Mục đích là sử dụng những tài nguyên này của máy chủ mục tiêu như là CPU và Ram. Hacker tập trung vào tài nguyên trên hệ thống, khiến cho dịch vụ hoặc toàn bộ hệ thống trở nên quá tải. Các cuộc tấn công phổ biến của loại này:

* TCP/UDP Flood Attack
* Smurf Attack
* Ping Flood Attack

**CHƯƠNG 2: CÁC KỸ THUẬT TẤN CÔNG DDOS PHỔ BIẾN**

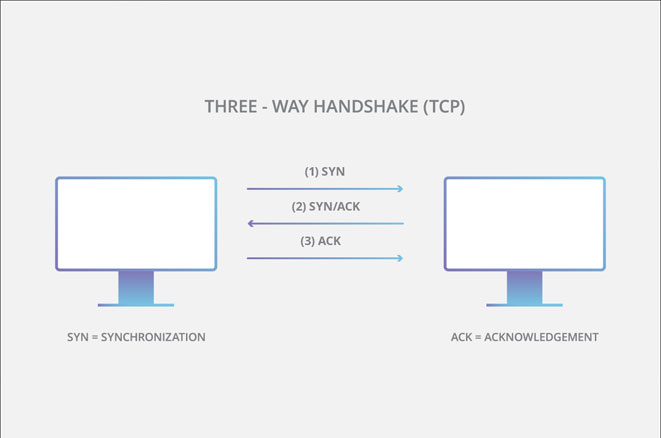
* 1. **Tấn công làm tràn băng thông (Flood Attack)**
     1. **SYN Flood Attack**

“SYN Flood Attack” khai thác lỗ hổng trong quá trình TCP bắt tay ba bước (Three-way Handshake). Trong cuộc tấn công, kẻ tấn công gửi các gói SYN với địa chỉ IP nguồn giả tới máy chủ mục tiêu. Khi đó máy chủ thực hiện lưu trữ các yêu cầu trong bộ nhớ Stack, nó sẽ chờ xác nhận từ Client đã gửi yêu cầu đó. Trong khi yêu cầu đang được chờ để xác nhận, nó sẽ vẫn ở trong bộ nhớ Stack của máy chủ.

Bởi vì địa chỉ nguồn là giả, nên máy chủ sẽ không thể nhận những gói tin xác nhận. Cuối cùng, các yêu cầu sẽ lấp đầy toàn bộ bộ nhớ của máy chủ.

Trong điều kiện bình thường, kết nối TCP được thể hiện quy trình 3 bước riêng biệt để tạo được sự kết nối như sau:

* **Bước 1:** Đầu tiên, máy tấn công gửi 1 gói tin SYN đến Server để yêu cầu kết nối.
* **Bước 2:** Sau khi tiếp nhận gói tin SYN, Server phản hồi lại máy khách bằng một gói tin SYN/ACK, để xác nhận thông tin từ Client.
* **Bước 3:** Cuối cùng, Client nhận được gói tin SYN/ACK thì sẽ trả lời Server bằng gói tin ACK báo với Server biết rằng nó đã nhận được gói tin SYN/ACK, kết nối đã được thiết lập và sẵn sàng trao đổi dữ liệu.

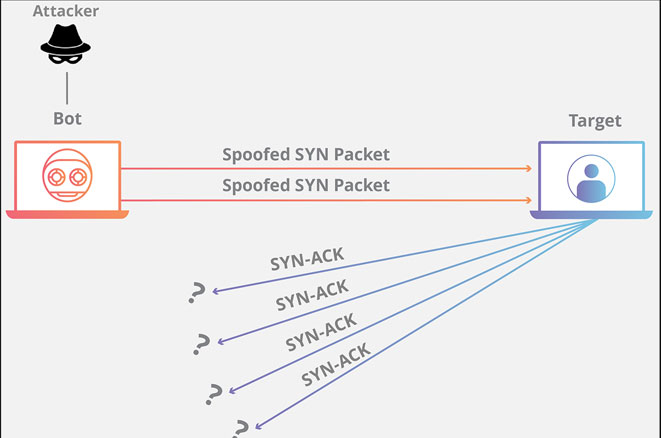


**Hình 2.1: Mô hình Bắt tay ba bước (Three-way Handshake)**

Để tạo từ chối dịch vụ (DoS), thực tế kẻ tấn công sẽ khai thác sau khi nhận được gói tin SYN ban đầu từ Client. Server sẽ phản hồi lại 1 hoặc nhiều gói tin SYN/ACK và chờ đến bước cuối cùng trong quá trình Handshake. Ở đây, cách thức thực hiện của nó như sau:

* **Bước 1:** Kẻ tấn công sẽ gửi một khối lượng lớn các gói tin SYN đến Server. Được nhắm là mục tiêu và thường là các địa chỉ IP giả mạo.
* **Bước 2:** Sau đó Server sẽ phản hồi lại từng yêu cầu kết nối. Để lại 1 cổng mở sẵn sàng tiếp nhận và phản hồi.
* **Bước 3:** Trong khi Server chờ gói tin ACK ở bước cuối cùng từ Client, gói tin mà không bao giờ đến. Kẻ tấn công tiếp tục gửi thêm các gói tin SYN. Sự xuất hiện các gói tin SYN mới khiến [máy chủ](https://vnso.vn/thue-may-chu-rieng/) tạm thời duy trì kết nối cổng mở mới trong một thời gian nhất định. Một khi các cổng có sẵn được sử dụng thì Server không thể hoạt động như bình thường.

Trong kết nối mạng, khi Server bên này kết nối mở nhưng máy bên kia không kết nối thì được coi là Half-open. Trong kiểu tấn công DDoS, sau khi server gửi gói tin SYN/ACK nó sẽ phải đợi cho đến khi Client trả lời. Đến khi các port trở lại bình thường. Kết quả của kiểu tấn công này được coi là cuộc tấn công Half-open.



#### **Hình 2.2: Mô hình Tấn công SYN Flood**

1. **Giả mạo địa chỉ IP trong SYN Flood Attack**

Giả mạo IP được sử dụng để che dấu địa chỉ IP thật của kẻ tấn công. Kỹ thuật này cho phép kẻ tấn công thực hiện những truy cập trái phép vào mạng bằng cách thay đổi IP thành IP của máy được cho phép truy cập. Một cuộc tấn công SYN Flood cũng có thể thực hiện từ một máy zombie sử dụng địa chỉ IP giả mạo, nguồn địa chỉ xác thực, khi mà các máy zombie bị từ chối các gói SYN/ACK.

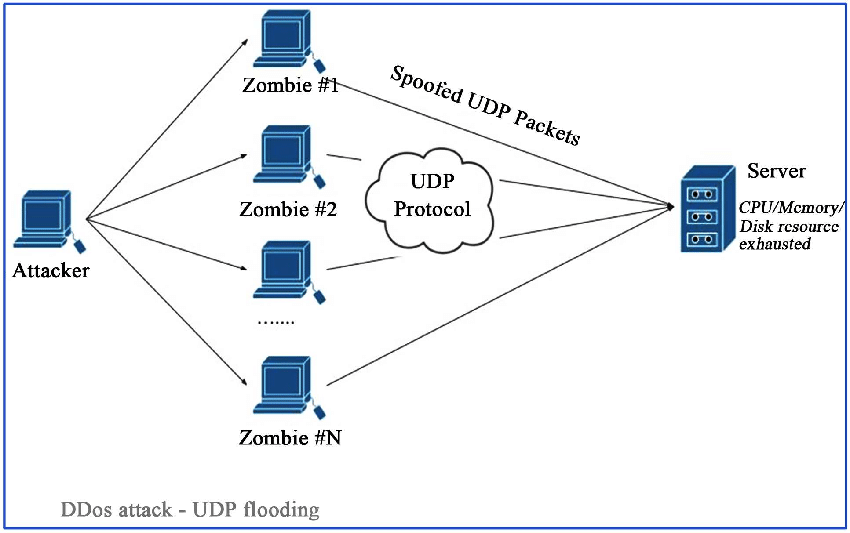
1. **Kỹ thuật giảm nhẹ thiệt hại cho SYN Flood Attack**

Tấn công SYN Flood có thể ngăn chặn bằng cách sử dụng máy chủ để phát hiện tấn công. Để phát hiện được tấn công, SYN requests được gửi bởi client sẽ được lưu trữ trong Database và sẽ đợi tới khi client gửi ACK tới máy chủ.Thông tin về client được lưu trữ trong máy chủ bao gồm: địa chỉ IP và số lượng gói tin SYN. Nếu như số các SYN request vượt quá ngưỡng cho phép, máy chủ sẽ loại bỏ các gói tin từ địa chỉ IP đó.

Quản trị viên cũng có thể sử dụng SYN cookies để phòng chống các cuộc tấn công SYN Flood dựa trên các địa chỉ IP giả mạo. SYN cookies sẽ không được cấp phát cho tới khi quá trình bắt tay 3 bước được hoàn thành. Nhưng hạn chế của kỹ thuật này là sử dụng tài nguyên quá lớn như CPU và Ram của server.

* + 1. **UDP Flood Attack**

Tấn công UDP Flood là một kỹ thuật tấn công từ chối dịch vụ sử dụng các gói tin UDP. Trong tấn công UDP Flood, các cuộc tấn công được khởi chạy với việc gửi một số lượng lớn các gói tin UDP đến các port ngẫu nhiên hoặc được chỉ định trên hệ thống của nạn nhân. Để xác định ứng dụng được yêu cầu, hệ thống nạn nhân phải xử lý dữ liệu vào. Trong trường hợp thiếu ứng dụng trên port được yêu cầu, hệ thống nạn nhân sẽ gửi thông điệp ICMP với nội dung “Đích không thể đến được” cho người gửi (kẻ tấn công). Với số lượng lớn các gói tin UDP, hệ thống nạn nhân sẽ bị ép buộc phải gửi các gói tin ICMP, cuối cùng dẫn đến không thể nhận yêu cầu từ các người dùng hợp lệ do bão hòa về băng thông. Nếu các gói UDP được kẻ tấn công phân phối đến tất cả các port của hệ thống, hệ thống đó sẽ bị treo ngay lập tức.



#### **Hình 2.3: Mô hình Tấn công UDP Flood**

Để thực hiện, hacker sẽ làm cho hệ thống đi vào một vòng lặp trao đổi dữ liệu vô ích qua giao thức UDP một cách vô tận bằng cách:

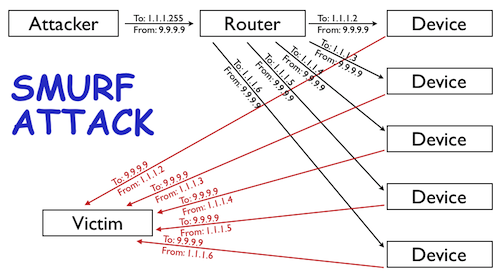
* **Bước 1:** Hacker giả mạo địa chỉ IP của một gói tin tấn công là địa chỉ loopback (127.0.0.1), sau đó gửi những gói tin này tới hệ thống của nạn nhân trên cổng UDP ECHO (cổng số 7).
* **Bước 2:** Hệ thống nạn nhân sẽ “echo” hồi đáp lại các thồng điệp do 127.0.0.1 (chính nó) gửi đến và kết quả là nó sẽ thực hiện một vòng lặp echo vô tận.

Việc sử dụng cổng UDP ECHO và tạo vòng lặp này khiến mục tiêu dần sử dụng hết băng thông của mình và cản trở hoạt động chia sẻ tài nguyên của các máy tính khác trong mạng.

* 1. **Smurf Attack**

Smurf Attack là dạng tấn công DDoS được thiết kế để làm cạn kiệt nguồn tài nguyên máy tính và băng thông mạng. Trong giao thức ICMP, khi một thiết bị trên mạng nhận được một “ping” request, thiết bị đó sẽ trả lời lại địa chỉ IP nguồn bằng một thông điệp “pong”, nhằm thăm dò xem tình trạng máy gửi “ping” request. Smurf attack khai thác lỗ hổng của ICMP và TCP/IP. Trong suốt cuộc tấn công, kẻ tấn công gửi lượng lớn các gói tin ICMP tới địa chỉ nguồn là địa chỉ của máy nạn nhân, và broadcast vào mạng máy tính.

Mọi thiết bị trong mạng nhận được thông điệp broadcast sẽ đáp trả thông điệp “pong” trở lại nạn nhân. Điều này khiến cạn kiệt tài nguyên tính toán của máy nạn nhân. Bên cạnh đó, mức độ của cuộc tấn công phụ thuộc vào số máy tính có trong mạng (những máy nhận được thông điệp broadcast) và tần suất gửi gói tin của kẻ tấn công.



#### **Hình 2.4: Mô hình Smurf Attack**

Các cuộc tấn công sử dụng phương pháp này không còn hiệu quả và dùng phổ biến nữa. Tuy nhiên vẫn có các hệ thống cũ sử dụng thiết bị quá cũ và không còn được cập nhật nữa. Đồng nghĩa sẽ có khả năng là nạn nhân của các vụ tấn công bằng phương thức này. Smurf attack có thể được ngăn chặn bằng việc sử dụng một tường lửa hoặc router để lọc các gói ICMP, có 3 thành phần tham gia trong một cuộc Smurf Attack:

* Mạng tấn công
* Mạng trung gian
* Mạng nạn nhân

Để phòng chống Smurf Attack, tất cả 3 thành phần phải có nhiệm vụ không cho kẻ tấn công xâm nhập. Đầu tiên, mạng tấn công không được cho phép User trong mạng tạo ra các địa chỉ IP giả mạo. Để làm được điều này, tường lửa cần cơ chế ngăn chặn không cho kẻ tấn công khuếch đại các lưu lượng độc hại.

Một cách khác để bảo vệ mạng trước một cuộc tấn công Smurf Attack là vô hiệu hóa IP Directed Broadcast. Bên cạnh đó, có rất nhiều hệ điều hành có thể được cấu hình để ngăn việc trả lời các gói tin ICMP.

* 1. **Application Layer Attack**

Thông thường, một cuộc tấn công DDoS Attack thực hiện tấn công vào tầng Network. VD: TCP Flood Attack, UDP Flood Attack. Mục đích của kiểu tấn công này là chiếm lượng lớn băng thông mạng và khiến cho người dùng hợp pháp không thể truy cập đến các dịch vụ. Tuy nhiên, khi cuộc tấn công kiểu này thất bại, kẻ tấn công sẽ chuyển sang tấn công vào tầng Ứng dụng (được gọi chung là App-DDoS Attacks).

App-DDoS Attacks thực hiện tấn công nhằm tiêu hao các tài nguyên của máy chủ như CPU, memory, băng thông, bộ nhớ,v.v. Kẻ tấn công có thể gửi lượng lớn request tới Database khiến cho máy chủ quá tải, hoặc gửi một lượng khổng lồ các HTTP Get request để tấn công Webserver. Cuộc tấn công này tương tự như việc nhiều người dùng hợp pháp truy cập vào một website cùng lúc. Và kết quả là rất khó để phân biệt đâu là lưu lượng hợp pháp và tấn công.

* + 1. **HTTP Flood Attack**

Khi một HTTP client như web browser giao tiếp với một ứng dụng hay server, nó gửi một HTTP request-GET hoặc POST. Một GET request được dùng để nhận các nội dung tĩnh như hình ảnh, trong khi POST request được dùng truy cập các tài nguyên tự động tạo ra.

Cuộc tấn công hiệu quả nhất khi server hoặc ứng dụng bị lừa để sử dụng nguồn tài nguyên lớn nhất có thể để respone một request. HTTP flood attack sử dụng POST request thằng là nguồn tài nguyên tấn công hiệu quả của kẻ tấn công, bởi POST request bao gồm các thông số kích hoạt phức tạp khi máy chủ xử lý. Mặt khác, các cuộc tấn công dựa trên GET response thì đơn giản hơn để tạ và có thể hiệu quả hơn trong một cuộc tấn công có mạng lưới tấn công (Attack – Network).

Diagram

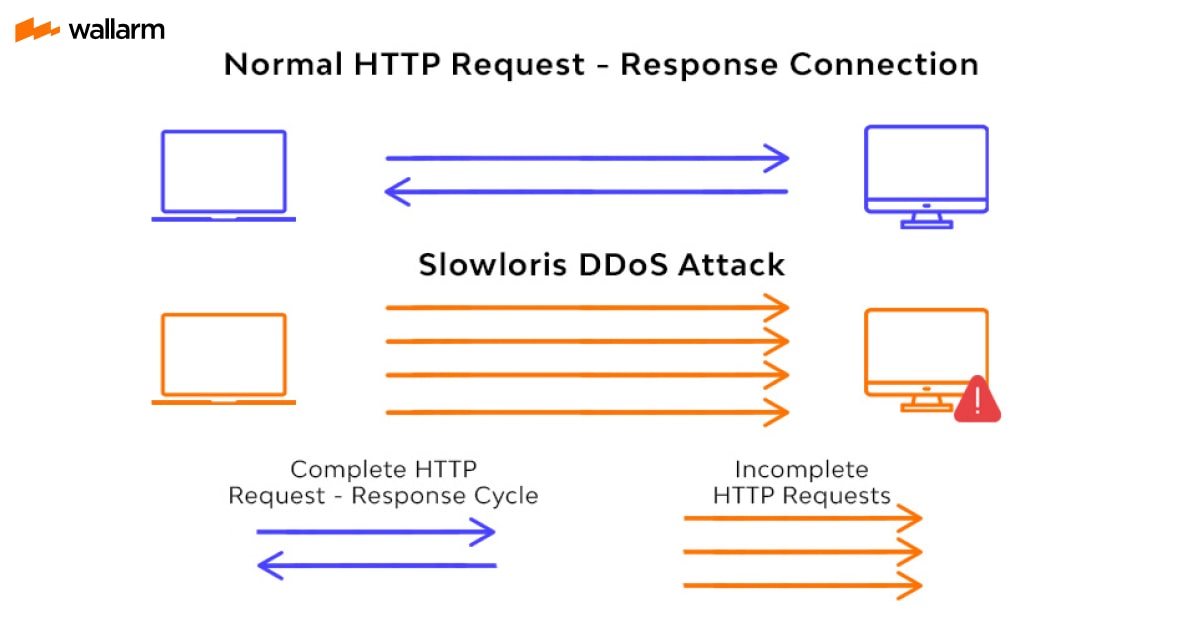
Description automatically generated

#### **Hình 2.5: Mô hình Tấn công HTTP Flood**

* + 1. **Slowloris Attack**

Slowloris thực hiện mở rất nhiều kết nối tới máy chủ web nạn nhân và giữ chúng mở càng lâu càng tốt. Để đạt được điều này, kẻ tấn công lợi dụng lỗ hổng của webserver mà ở đó máy chủ đợi nhận được toàn bộ HTTP header trước khi đóng kết nối. Một số server như Apache sử dụng thời gian chờ các gói HTTP chưa hoàn thiện là 300 giây theo mặc định, và thời gian này sẽ được tái thiết lập khi client gửi dữ liệu bổ sung.

Điều này tạo điều kiện cho kẻ tấn công mở một loạt các kết nối bằng cách khởi tạo HTTP request và không đóng nó. Bằng cách giữ các HTTP request mở và khiến server nhận các data không có thật trước khi đạt tới thời gian timeout, kết nối HTTP sẽ mở cho tới khi kẻ tấn công đóng nó lại. Đương nhiên, nếu kẻ tấn công chiếm hết các kết nối HTTP trên máy chủ web, người sử dụng hợp pháp sẽ không thể sử dụng các dịch vụ.

****

#### **Hình 2.6: Mô hình Slowloris Attack**

**HiH**

# **CHƯƠNG 3: CÁCH PHÒNG CHỐNG CUỘC TẤN CÔNG DDOS**

Để có thể phòng chống một cuộc tấn công DDoS, ta có thể chia thành 3 giai đoạn chính:

1. Giai đoạn phát hiện và ngăn ngừa.
2. Giai đoạn đối đầu và sau một cuộc tấn công.
3. Giai đoạn đánh giá mức độ thiệt hại.
   1. **Giai đoạn phát hiện và ngăn ngừa**
      1. **Ngăn ngừa một cuộc tấn công DDoS**

Phương pháp hiệu quả để ngăn ngừa các cuộc tấn công DDoS là từng người sử dụng Inrternet phải tự đề phòng, không để bị lợi dụng tấn công các hệ thống, máy chủ khác. Để làm được vậy, ý thức và các kỹ thuật phòng chống phải được chia sẻ phổ biến rỗng rãi cho người sử dụng mạng lưới Internet. Các cuộc tấn công DDoS sẽ khó hình thành hoặc bị hạn chế nếu không có hoặc ít người dùng nào bị lợi dụng để trở thành Zombie. Người dùng phải liên tục tiến hành bảo vệ các thiết bị truy cập mạng của mình bằng cách thường xuyên kiểm tra và cập nhập hệ thống, không nhấn vào đường link lạ, chưa rõ nguồn gốc.

Một số giải pháp:

* Đối với nhà cung cấp thiết bị có thế tích hợp khả năng ngăn ngừa tấn công qua phần mềm và phần cứng của hệ thống trước khi cung cấp cho người dùng.
* Đối với người dùng Internet, nên cài đặt và cập nhật liên tục các phần mềm bảo mật và hệ thống.
  + 1. **Phát hiện một cuộc tấn công DDoS**

Có nhiều kỹ thuật được áp dụng để phát hiện một cuộc tấn công DDoS, nhưng phổ biến nhất gồm có 02 kỹ thuật:

* **Agress Filtering:** Kỹ thuật này dùng để kiểm tra xem một gói tin có đủ tiêu chuẩn ra khỏi một subnet hay không dựa trên cơ sở gateway của một server subnet luôn biết được địa chỉ IP của các máy thuộc subnet. Các gói tin từ bên trong của subnet gửi ra bên ngoài với địa chỉ nguồn không hợp lệ sẽ bị giữ lại để điều tra nguyên nhân. Nếu kỹ thuật này được áp dụng trên tất cả các subnet của mạng lười Internet thì khái niệm IP giả mạo sẽ không tồn tại. Việc kiểm tra như vậy có thể thực hiện bằng các lưu lại các địa chỉ IP thường xuyên truy cập vào server trong một cơ sở dữ liệu. Khi có một cuộc tấn công xảy ra thì ta sẽ tiến hành so sánh với các địa chỉ IP trong thời gian tấn công với các địa chỉ IP trong cở sở dữ liệu (IP Address Darabase) để phát hiện các IP mới.
* **MIB statistics**: trong Management Information Base (SNMP – Simple Network Management Protocol) của router luôn có thông tin thống kê về sự biến thiện trạng thái của mạng. Nếu ta giám sát chặt chẽ các thống kê của Protocol ICMP, UDP và TCP ta sẽ có khả năng phát hiện được thời điểm bắt đầu của một cuộc tấn công để tạo “quỹ thời gian vàng” cho việc sử lý tình huống.
  1. **Giai đoạn đối đầu và sau một cuộc tấn công**
     1. **Làm suy giảm hay dừng cuộc tấn công**
* **Load balancing**: Thiết lập kiến trúc cân bằng lượng công việc cho tất cả các máy chủ trong thời gian trọng điểm sẽ giúp làm gia tăng thời gian chống chọi của hệ thống với cuộc tấn công DDoS. Tuy nhiên, điều này không có ý nghĩa lắm về mặt thực tiễn vì quy mô của cuộc tấn công có thể coi là không có giới hạn.
* **Throttling:** Thiết lập cơ chế điều tiết trên router, giới hạn tốc độ hoặc lượng truy cập hợp lý mà server bên trong có thể xử lý được.
* **Drop request:** Thiết lập cơ chế drop request (loại bỏ địa chỉ IP nghi ngờ là nguồn của cuộc tấn công) nếu nó vi phạm một số quy định như: thời gian delay kéo dài, tốn nhiều tài nguyên để xử lý, gây deadlock. Tuy nhiên nó cũng giới hạn một số hoạt động thông thường của hệ thống, cần cân nhắc trước khi sử dụng.
  + 1. **Giai đoạn sau một cuộc tấn công**
* **Traffic Pattern Analysis:** Phân tích, thống kê các dữ liệu lưu lượng truy cập mạng. Quá trình phân tích này rất có ích cho việc tinh chỉnh lại các hệ thống Load Balancing và Throttling, Ngoài ra các dữ liệu này còn giúp quản trị mạng điều chỉnh lại quy tắc kiểm soát traffic ra vào mạng của mình.
* **Packet Traceback:** Kỹ thuật Traceback thống kê danh sách tất cả thông tin liên quan đến lỗi trong một hệ thống, từ đó ta có thế truy ngược vị trí của kẻ tấn công. Tuy nhiên haker trình độ cao cũng đã phát triển thêm khả năng Block Traceback.
* **Event Logs:** Bằng cách phân tích file log sau cuộc tấn công, quản trị mạng có thể tìm ra nhiều manh mối và chứng cứ quan trọng.
  1. **Giai đoạn đánh giá mức độ thiệt hại**

Có 5 thông số thường được dùng để đánh giá mức độ thiệt hại, ảnh hưởng của một cuộc tấn công DDoS:

* + Thông lượng (Throughput)
  + Thời gian trễ trọn vòng (Round-trip Time)
  + Mất gói tin (Packet Loss)
  + Sử dụng CPU (CPU Utilization)
  + Jitter
    1. **Throughput**

Throughput được định nghĩa là số lượng byte được truyền tải trong khoảng thời gian nhất định (byte/s).

* + 1. **Round-trip Time**

Round-trip Time được định nghĩa là khoảng thời gian khi một request được tạo ra tới khi máy đích nhận được một response hoàn chỉnh. Thông số này dùng để đánh giá mức độ ảnh hưởng của tấn công DDoS khi nó chỉ ra thời gian trễ một gói tin được gửi đi và khi nó nhận được phản hồi từ đích.

* + 1. **Packet Loss**

Packet Loss là số gói tin hoặc byte bị mất bởi cuộc tấn công. Thông số này chủ yếu để đánh giá mức độ tắc nghẽn trong mạng do các cuộc tấn công Flooding gây ra.

* + 1. **CPU Utilization**

CPU Utilization là phần trăm CPU sử dụng trong khi thực thi của một chương trình hay tác vụ. Một vài loại tấn công DDoS như TCP Flood Attack… sẽ làm cho các dịch vụ mạng của máy chủ làm việc hết công suất và chúng chiếm hết công suất của CPU khiến cho thông số này tăng lên rất cao hoặc có thể đạt tối đa.

* + 1. **Jitter**

Jitter là một thông số quan trọng được sử dụng để đo lường độ trễ do máy tính bị tấn công DDoS. Nó đại diện cho thời gian phản hồi của một máy chủ đến yêu cầu từ người dùng. Trong một tấn công DDoS, thông số Jitter sẽ giảm đáng kể bởi vì có quá nhiều yêu cầu đã được gởi đến máy chủ và không thể được phục vụ một cách thích hợp.

* 1. **Các giải pháp đơn giản phòng chống một cuộc tấn công**
     1. **Cài đặt bản bảo mật mới nhất**

Trước khi tấn công, kẻ tấn công cần phải tìm những lỗ hổng của máy mục tiêu. Những lỗ hổng này có thể từ các thiết kế mạng, thiếu các yếu tố bảo mật, hoặc ứng dụng đang được sử dụng có lỗ hổng bảo mật. Vì vậy, việc cập nhật các bản vá bảo mật là vô cùng quan trọng.

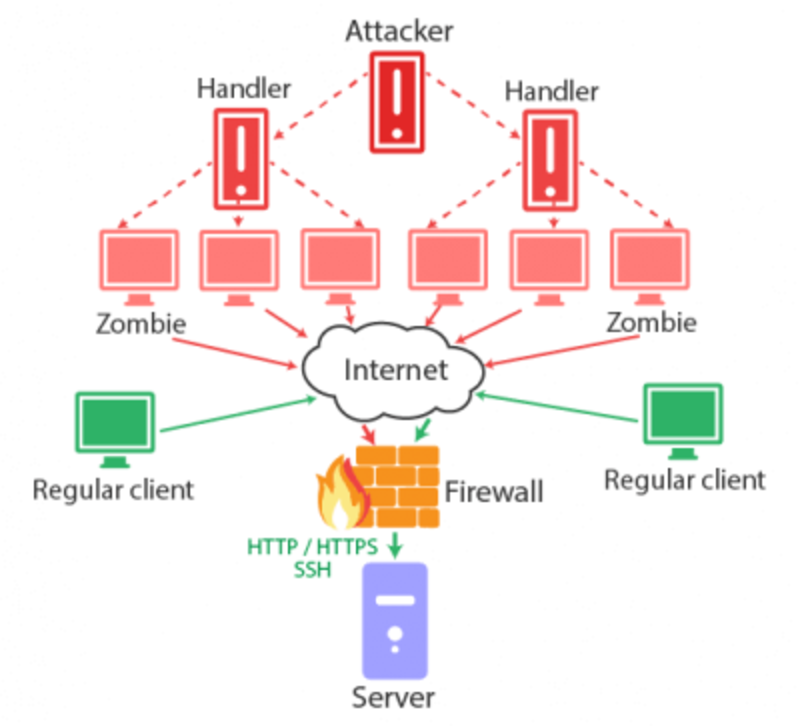
* + 1. **Vô hiệu hóa IP broadcast**

Để ngăn chặn một cuộc tấn công như Smurf Attack, quản trị viên có thể sử dụng các giải pháp như cấu hình thiết bị từ chối chuyển tiếp các gói tin với địa chỉ là IP Broadcast đến các thiết bị trong mạng.

* + 1. **Firewall**

Firewall có thể được sử dụng chặn các gói tin độc hại từ bên ngoài đi vào máy tính. Nó có thể giới hạn số lượng kết nối đến hệ thống, thiết lập chặn các IP đã biết là nguồn của cuộc tấn công DDoS từ trước. Firewall cũng cung cấp thông tin và cảnh báo về một cuộc DDoS.

Tuy nhiên những cuộc tấn công tinh vi vãn sẽ có thể vượt qua Firewall để tấn công hệ thống.



#### **Hình 3.1: Mô hình Firewall**

* + 1. **IP Hopping**

IP hopping là kỹ thuật che dấu địa chỉ IP của người dùng, giúp giảm thiểu tác động của các cuộc tấn công DDoS bằng cách che dấu địa chỉ thật và giảm bớt lưu lượng tấn công. Tuy nhiên cách này không đủ hiệu quả khi hacker sử dụng kỹ thuật phức tạp hơn.

* 1. **Một số công cụ phòng chống tấn công DDoS phổ biến**
     1. **CloudFlare**

Diagram

Description automatically generated

**Hình 3.2: Mô hình phóng chống DDoS của CloudFlare**

Cloudflare là một dịch vụ CDN (Content Delivery Network) và bảo mật web được cung cấp bởi công ty Cloudflare, Inc. Cloudflare được thiết kế để tăng tốc độ tải trang web và bảo vệ chúng khỏi các cuộc tấn công trên mạng như DDoS, SQL injection, cross-site scripting (XSS) và các cuộc tấn công khác.

Cloudflare hoạt động bằng cách đưa dữ liệu từ máy chủ gốc đến các máy chủ CDN trên toàn cầu, giúp tăng tốc độ tải trang web và giảm thiểu thời gian phản hồi. Cloudflare cũng cung cấp các công cụ bảo mật như bộ lọc gói tin, tường lửa ứng dụng web (WAF), và phát hiện các cuộc tấn công DDoS.

### **Vietnix Firewall**

Vietnix Firewall là tường lửa gồm nhiều lớp đứng giữa người dùng và server. Nó có nhiệm vụ phân tích và vô hiệu hóa các kết nối đang tấn công server. Tường lửa của Vietnix có khả năng bảo vệ toàn diện, nâng cao tính ổn định. Đồng thời giúp hệ thống đứng vững trước các cuộc tấn công DDoS.

**Diagram

Description automatically generated**

#### **Hình 3.3: Mô hình Vietnix Firewall**

* + 1. **SolarWinds Security Event Manager**

Đây là một phần mềm chống DDoS có khả năng giám sát nhật ký các sự kiện (Event log). Event log là một tài nguyên chính để kiểm tra nếu phát các yếu tố độc hại đang cố gắng phá vỡ mạng.

Để bảo vệ server khỏi DDoS, SolarWinds Security Event Manager duy trì một danh sách các yếu tố độc hại. Từ đó chương trình có thể tự động chặn IP tương tác với mạng. Dựa vào danh sách này, ta cũng có thể phòng chống các mối nguy hại gần đây.

Trong một cuộc tấn công, các cảnh báo cũng có thể được cấu hình để thông báo khi có nguồn đáng ngờ đang gửi các lưu lượng đến. Bên cạnh đó, các bản ghi cũng có thể được sử dụng để phân tích. Từ đó giúp tìm ra hướng để giảm thiểu các cuộc tấn công DDoS. Các kết quả ghi chép này có thể được lọc ra theo tài khoản, IP, thời gian…

**Graphical user interface

Description automatically generated**

#### **Hình 3.4: Giao diện SolarWinds Security Event Manager**

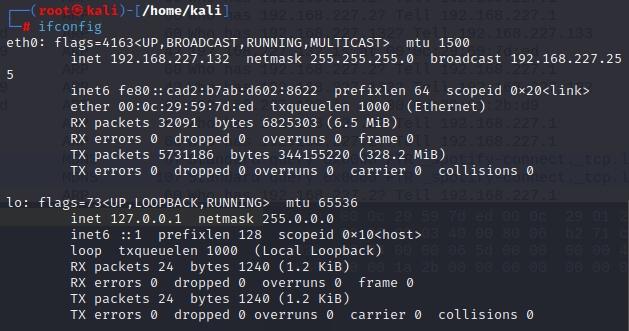
# **CHƯƠNG 4: THỰC NGHIỆM TẤN CÔNG DDOS**

* 1. **Mô hình thực nghiệm**

**Graphical user interface

Description automatically generated**

**Hình 4.1: Mô hình thực nghiệm**

****

**Hình 4.2: Địa chỉ IP máy tấn công**

**Text

Description automatically generated with medium confidence**

**Hình 4.3: Địa chỉ IP máy chủ**

* 1. **Kịch bản**
     1. **SYN-Flood Attack**
        1. **Mục tiêu**

Ở phương pháp này, máy tấn công sẽ sử dụng công cụ Hping3 được tích hợp sẵn trong hệ điều hành Kali Linux. Máy tấn công sẽ gửi một lượng lớn các gói tin SYN đến máy chủ sử dụng Windows Server 2022. Và máy chủ sẽ phản hồi lại yêu cầu, đồng thời mở một cổng chờ tiếp nhận các gói tin ACK. Máy tấn công sẽ không bao giờ gửi các gói tin ACK và vẫn tiếp tục gửi gói tin SYN để mục tiêu khiến máy chủ duy trì kết nối và mở tất cả các cổng có sẵn. Từ đó sẽ làm cho hệ thống máy chủ sẽ không thể hoạt động bình thường và gây ra tình trạng delay hoặc bị treo.

* + - 1. **Thực hiện**
* **Bước 1: Quét Port của máy chủ mục tiêu**

Sử dụng công cụ nmap được tích hợp sẵn trong hệ điều hành Kali Linux để thực hiện truy quét các port của máy mục tiêu nhằm mục đích tìm ra cổng mở để gửi gói tin.

Tại máy tấn công ta sử dụng dòng lệnh:

***nmap -F 192.168.227.140***

Trong đó:

* + Nmap: tên tool được dùng.
  + -F: tùy chọn quét nhanh các port.
  + 192.168.227.140: IP máy đích.

Hình ảnh chạy lệnh:

**Text

Description automatically generated**

**Hình 4.4: Câu lệnh Nmap và kết quả**

Theo hình, công cụ nmap đã quét được các cổng đang có trạng thái (STATE) open là đang mở, ta có thể sử dụng các cổng đó để tiến hành tấn công DDoS

* **Bước 2: Tiến hành tấn công**

Sau khi tiến hành quét, ta chọn một trong số các cổng mở thích hợp để tiến hành thực nghiệm tấn công SYN-Flood.

Tại máy tấn công, thực hiện gửi liên tục các gói tin SYN bằng dòng lệnh sau:

***sudo hping3 -S –flood -p 135 192.168.227.140***

Trong đó:

* + hping3: tên của tool được dùng.
  + -S: gói tin SYN.
  + --flood: tùy chọn gửi liên tục các gói tin với tốc độ nhanh nhất có thể.
  + -p: chỉ định cổng địa chỉ của IP dích.
  + 135: cổng được chỉ định.
  + 192.168.227.140: địa chỉ IP đích.

Hình ảnh chạy lệnh tấn công:

**Text

Description automatically generated**

#### **Hình 4.5: Câu lệnh tấn công SYN-Flood**

Ta mở Terminal và nhập lệnh sau, sau đó chọn eth0 để xem công cụ Wireshark chụp gói tin:

***sudo wireshark***

**Graphical user interface, application, table

Description automatically generated**

#### **Hình 4.6: Công cụ Wireshark chụp lại gói tin (1)**

Ngay khi thực hiện tấn công, công cụ Wireshark đã và đang chụp hàng loạt các gói SYN do máy tấn công (192.168.227.132) đang liên tục gửi đến từ nhiều port tới một port duy nhất của máy chủ mục tiêu (192.168.227.140) là port 135.

Graphical user interface

Description automatically generated

**Hình 4.7: Công cụ Wireshark chụp lại gói tin (2)**

Sau khi nhận được được gói SYN từ máy gửi (máy tấn công), máy chủ mục tiêu đã phản hồi lại bằng cách gửi lại gói tin SYN/ACK từ port 135 tới từng port của máy gửi (máy tấn công) để yêu cầu bên gửi xác nhận lại bằng cách phản hồi lại bằng gói ACK là đã nhận được gói tin.

Graphical user interface

Description automatically generated with medium confidence

#### **Hình 4.8: Công cụ Wireshark chụp lại gói tin (3)**

Tuy nhiên máy tấn công sẽ không bao giờ gửi lại các gói tin phản hồi ACK, vì vậy công cụ Wireshark đã chụp được liên tiếp các gói tin có thông báo “TCP Retrasmission”, thông báo này chỉ ra rằng máy chủ không nhận được gói ACK phản hồi từ máy gửi nên máy chủ sẽ đóng cổng. Tuy nhiên trong cuộc tấn công này, vì nhận được liên tiếp các gói SYN nên máy chủ phải duy trì port 135 để tiếp nhận và phản hồi lại các gói tin.

* + - 1. **Kết quả và đánh giá**

Tại máy chủ, thông số sử dụng CPU (CPU Utilization) và lưu lượng dữ liệu truyền tải (Ethernet) cho thấy tăng bất thường: thông số sử dụng CPU luôn đạt trên 50%.

**Chart

Description automatically generated**

#### **Hình 4.9: Thông số Sử dụng CPU khi bị tấn công**

**Chart

Description automatically generated**

#### **Hình 4.10: Thông số lưu lượng mạng khi bị tấn công**

Ta có thể thấy đây là một cuộc tấn công đơn giản để thực hiện, nhưng khi máy chủ bị tấn công sẽ bị quá tải và khó có thể phục vụ yêu cầu kết nối từ máy khác. Nó thường được sử dụng để che giấu các cuộc tấn công khác. Vì vậy, Syn-Flood là cuộc tấn công nguy hiển và có thể gây ra nhiều tổn hại cho hệ thống mạng.

* + 1. **ICMP Flood Attack**
       1. **Mục tiêu**

Ở phương pháp này, máy tấn công sẽ sử dụng Hping3 để cổ gắng áp đảo máy chủ, gây tắc nghẽn đường truyền và từ đó không thể đáp ứng những yêu câu hợp lệ bằng cách gửi nhiều các gói tin echo-request ICMP đến máy chủ mục tiêu bằng nhiều thiết bị. Sau đó máy chủ sẽ phải gửi echo-reply ICMP lại đến từng địa chỉ IP.

* + - 1. **Thực hiện**
* **Bước 1: Quét Port của máy chủ mục tiêu**

Sử dụng công cụ nmap được tích hợp sẵn trong hệ điều hành Kali Linux để thực hiện truy quét các port của máy mục tiêu nhằm mục đích tìm ra cổng mở để gửi gói tin.

Tại máy tấn công ta sử dụng dòng lệnh:

***nmap -p1-65535 192.168.227.140***

Trong đó:

* + Nmap: tên tool được dùng.
  + -p: tùy chọn quét port.
  + 1-65535: tất cả các port từ 1 đến 65535.
  + 192.168.227.140: IP máy đích.

Hình ảnh chạy lệnh:

**Text

Description automatically generated**

**Hình 4.11: Câu lệnh Nmap và kết quả**

Theo hình, công cụ nmap đã quét được các cổng đang có trạng thái (STATE) open là đang mở, ta có thể sử dụng các cổng đó để tiến hành tấn công DDoS

* **Bước 2: Tiến hành tấn công**

Tại máy tấn công, thực hiện câu lệnh:

***sudo hping3 -l --flood -p 135 192.168.227.140***

Trong đó: .

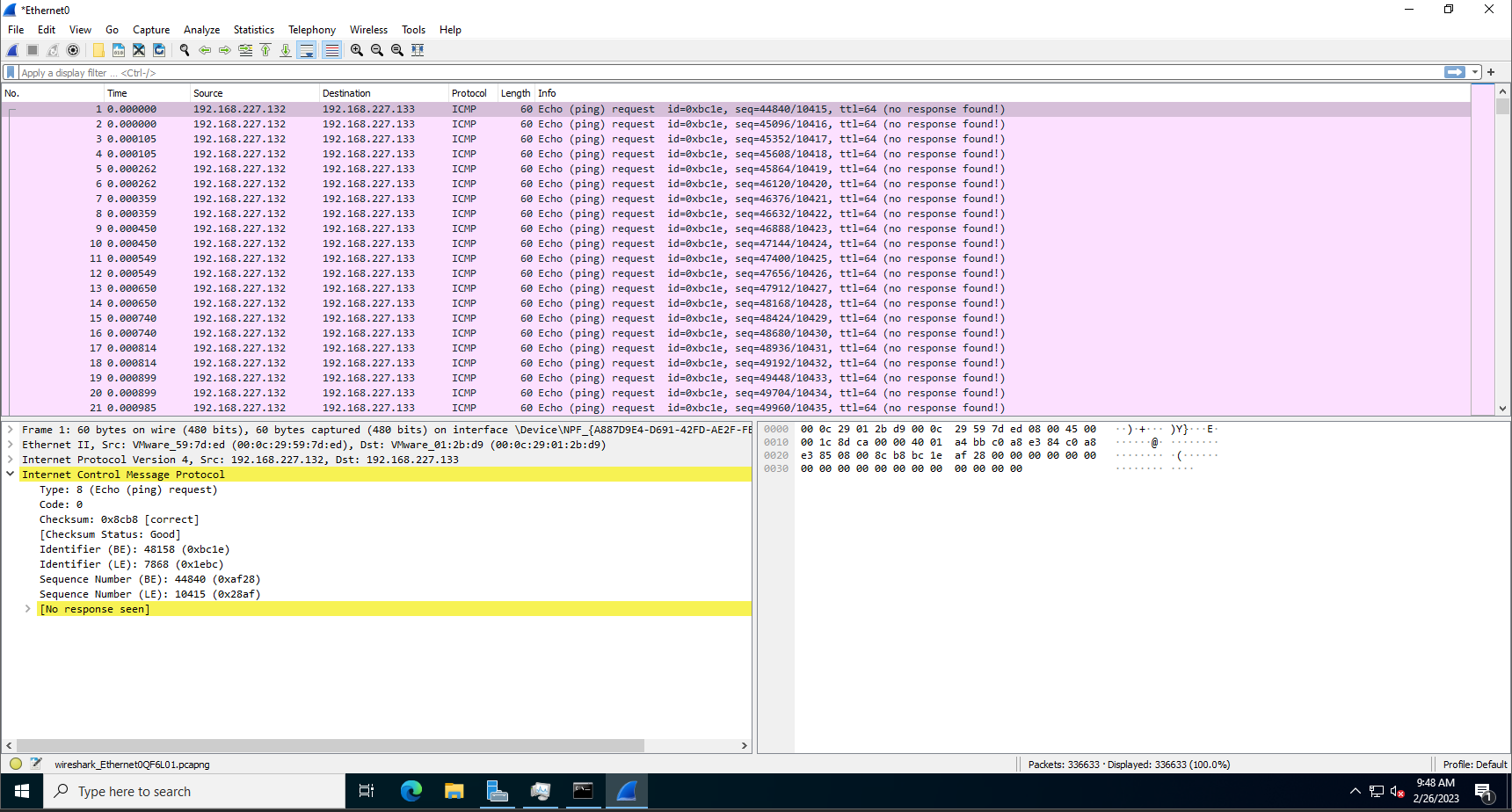
* + hping3: tên của tool được dùng.
  + -1: tùy chọn ICMP
  + --flood: tùy chọn gửi liên tục các gói tin với tốc độ nhanh nhất có thể.
  + -p: chỉ định cổng địa chỉ của IP dích.
  + 135: cổng được chỉ định.
  + 192.168.227.140: địa chỉ IP đích.

Hình ảnh chạy lệnh tấn công:

***Text

Description automatically generated***

#### **Hình 4.12: Câu lệnh tấn công ICMP-Flood**

****

#### **Hình 4.13: Công cụ Wireshark trên máy tấn công ICMP Flood**

Khi đang tiến hành tấn công ICMP Flood vào máy chủ mục tiêu, Wireshark đã và đang chụp được hàng loạt các gói tin ICMP do máy tấn công (192.168.106.132) đang liên tục gửi tới máy chủ mục tiêu.

Các gói tin khi được chụp từ máy chủ mục liên tục hiện thị thông báo “ no response found”, điều này cho thấy máy chủ không nhận lại được các ping reply trong khoảng thời gian chờ đợi. Nguyên nhân là do khi máy chủ bị tấn công sẽ khiến cho đường truyền mạng tới máy chủ bị tắc nghẽn nên làm cho gói ping reply bị mất hoặc trì hoãn.

* + - 1. **Kết quả và đánh giá:**

Tại máy chủ, thông số lưu lượng dữ liệu truyền tải (Ethernet) cho thấy tăng bất thường.

Chart, line chart

Description automatically generated

#### **Hình 4.14: Thống số lưu lượng mạng khi bị tấn công**

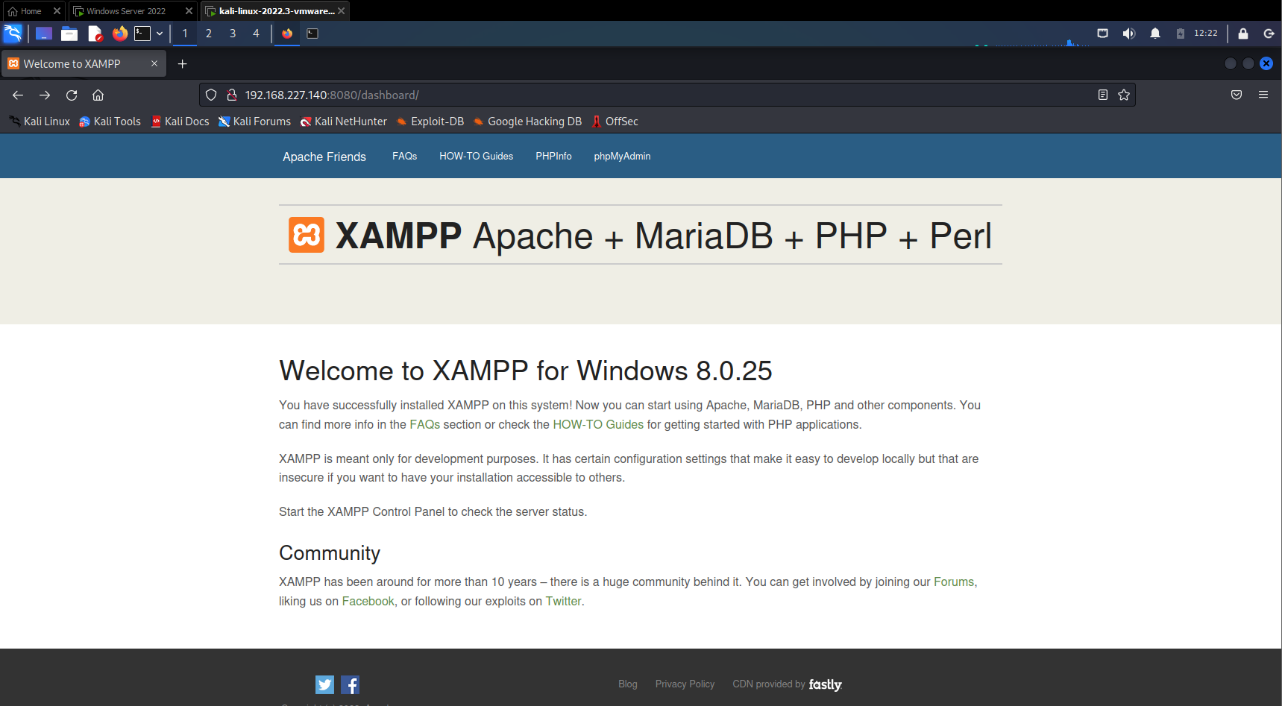
Tấn công ICMP flood có thể gây ra các sự cố mạng nghiêm trọng và làm giảm hiệu suất của hệ thống mạng, từ đó đường truyền mạng sẽ bị tắc nghẽn và hệ thống sẽ không đáp ứng được các yêu cầu hợp lý.

* + 1. **HTTP Flood Attack**
       1. **Mục tiêu:**

Máy tấn công sẽ gửi một lượng lớn yêu cầu HTTP tới máy chủ mục tiêu với tốc độ và tần suất cao hơn tốc độ xử lý của server. Mục tiêu của việc làm này là khiến cho trang web bị chậm trễ hoặc có thể ngừng hoạt động và khiến cho người dùng khác không thể nào truy cập được vào trang web.

* + - 1. **Thực hiện:**

Ban đầu, trang web của máy chủ mục tiêu có địa chỉ <http://192.168.227.140:8080/dashboard/> đang chạy ổn định và máy người dùng vẫn có thể truy cập vào và thao tác với website bình thường.



#### **Hình 4.15: Trang web trước khi bị tấn công**

Để thực hiện tấn công, máy tấn công thực hiện theo các bước sau:

* + **Bước 1:** Sử dụng câu lệnh sau và nhập mật khẩu “kali” để khởi chạy RavenStorm

***sudo rst***

* + **Bước 2:** Nhập ***l7*** để lựa chọn module layer 7.
  + **Bước 3:** Nhập ***target*** để chọn tùy chọn target .
  + **Bước 4:** Nhập URL: <http://192.168.227.140:8080/dashboard/>.
  + **Bước 5:** Nhập ***threads*** để chọn tùy chọn thread.
  + **Bước 6:** Nhập 1000.
  + **Bước 7:** Nhập ***run*** và nhấn ***y*** để khởi chạy.

Hình ảnh khởi chạy công cụ trên máy tấn công:

Text

Description automatically generated

#### **Hình 4.16: Công cụ đang khởi chạy trên máy tấn công**

Hình ảnh công cụ Wireshark đang chụp các gói tin trong máy chủ:

Graphical user interface, text, application

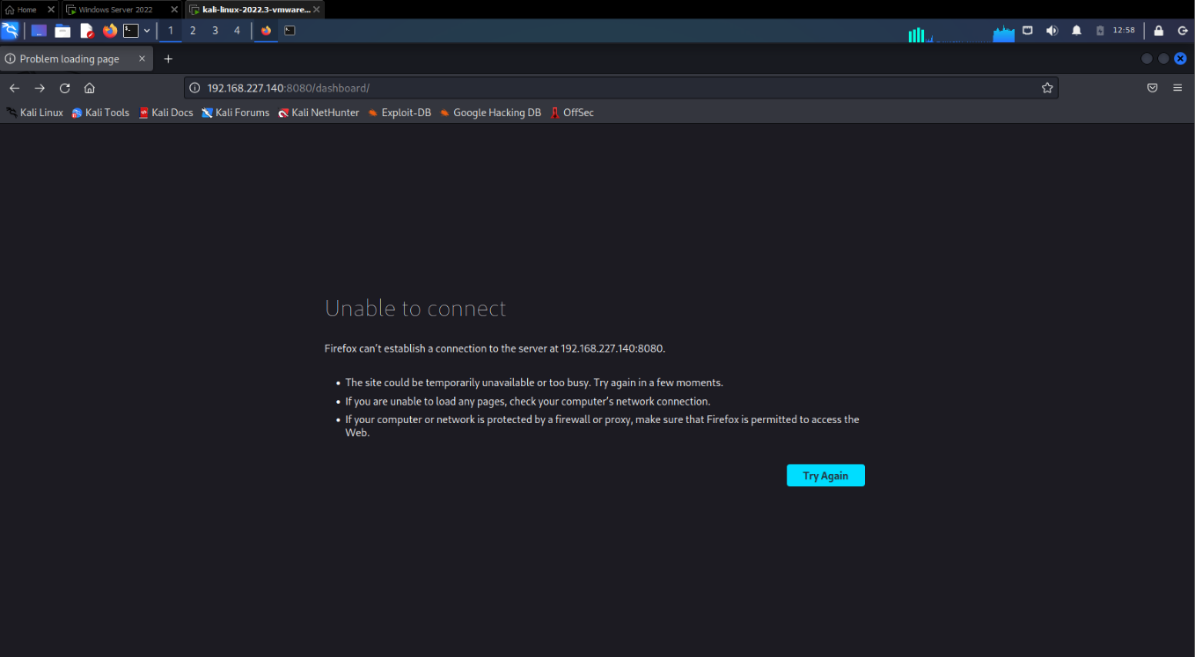
Description automatically generated

#### **Hình 4.17: Công cụ Wireshark đang chụp lại các gói tin**

Khi trong quá trình tấn công, Wireshark đã chụp được các gói tin HTTP requets do máy tấn công liên tiếp gửi tới máy chủ mục tiêu với tốc độ và tần số nhanh. Nó khiến cho máy chủ bị quá tải và không thể phục vụ được các yêu cầu hợp lệ khác.

* + - 1. **Kết quả và đánh giá:**

Khi máy tấn công đang tấn công HTTP Flood vào địa chỉ của WebServer. Website của Server sẽ bị sập, người dùng không thể nào có thể truy cập và tương tác với website được cho đến khi cuộc tấn công kết thúc.



#### **Hình 4.18: Website đã bị sập khi truy cập bằng máy tấn công**

HTTP Flood Attack là một hình thức tấn công đơn giản và dễ triển khai. Nhưng nó có thể gây ra hậu quả rất lớn như làm sập hệ thống website của máy chủ và thậm chỉ có thể khiến cho thông tin cá nhân của người dùng bị lộ ra ngoài.

* 1. **Kết luận chung:**

Qua các lần thử nghiệm trên, ta có thể thấy tuy các phương pháp tấn công đều rất đơn giản, dễ thực hiện được, nhưng hậu quả của chúng để có thể rất nghiêm trọng như có thể làm tắc nghẽn kết nối mạng dẫn đến làm sập hệ thống, chúng cũng có thể làm lộ các thông tin cá nhân của những người sử dụng dịch vụ của các máy chủ đó. Các cuộc tấn công như vậy có thể diễn ra liên tục trong thời gian dài và ảnh hưởng đáng kể đến các máy chủ và hệ thống mạng.

# **KẾT LUẬN**

DDoS là một loại tấn công từ chối dịch vụ mạng mà kẻ tấn công sử dụng nhiều thiết bị để gửi lưu lượng truy cập đến một mục tiêu nhất định, gây hậu quả là làm cho hế thống mục tiêu quá tải và không thể phục vụ các yêu cầu hợp lệ của người dùng. DDoS có thể gây ra những tổn thất nghiêm trọng cho các doanh nghiệp và tổ chức, bao gồm mất dữ liệu, thời gian chết máy chủ, từ đó sẽ ảnh hướng đến mặc uy tín, khả năng hoạt động và tài chính của họ.

Vì vậy, để phòng chống được các cuộc tấn công DDoS, các tổ chức cần thực hiện các biện pháp bảo mật như luôn đảm bảo và cập nhật sớm nhất các bản vá lỗ hổng, sử dụng biện pháp bảo mật: tường lửa, hệ thống phòng thủ chống DDoS, và thường xuyên thực hiện kiểm tra bảo mật của hệ thống và nhanh chóng giải quyết chung một cách sớm nhất và tốt nhất.

# **TÀI LIỆU THAM KHẢO**

* <https://mona.media/ddos-la-gi-tan-cong-tu-choi-dich-vu-tren-internet/>
* <https://vietnix.vn/phan-mem-chong-ddos-tot-nhat/>
* <https://vietnix.vn/botnet-la-gi/>
* <https://github.com/Tmpertor/Raven-Storm>
* <https://topdev.vn/blog/cai-dat-xampp/>
* <https://wiki.matbao.net/ddos-la-gi-phan-biet-tan-cong-tu-choi-dich-vu-dos-va-ddos/>
* <https://vnso.vn/syn-flood-attack-ddos-la-gi-cach-thuc-phong-chong/>
* <https://vnso.vn/ping-icmp-flood-attack-tan-cong-ddos-bang-ping-flood-la-gi/>
* <https://vnso.vn/tan-cong-http-flood-http-flood-co-the-ap-dao-server-mot-cach-nhanh-chong/>

# **PHỤ LỤC**

1. **Hướng dẫn cài đặt mô hình thực nghiệm**

**VMware**: là phần mềm máy chủ ảo, đây là một môi trường ảo có chức năng như một hệ thống máy tính ảo với CPU, bộ nhớ, mạng và bộ lưu trữ riêng. Chúng được tạo trên một hệ thống phần cứng vật lý.

Thực hiện cài đặt VMware theo hương dẫn trong video sau: <https://youtu.be/mvG5lT3moto>.

* 1. **Xây dựng các máy ảo**

1. **Xây dựng máy tấn công:**

**Kali Linux**: là một bản phân phối của hệ điều hành mã nguồn mở Linux, được sử dụng nhiều trong lĩnh vực bảo mật. Nó tập hợp nhiều công cụ kiểm tra bảo mật và thâm nhập tốt nhất có thể trong một môi trường hệ điều hành.

Cấu hình yêu cầu tối thiểu:

* + Dung lượng ổ đĩa: 20GB.
  + RAM: 1GB.

Các bước cài đặt:

* **Bước 1:** Truy cập đường dẫn:<https://cdimage.kali.org/kali-2022.4/kali-linux-2022.4-vmware-amd64.7z> để tiền hành tải về.
* **Bước 2:** Sau khi tải về xong, tiến hành giải file nén vào thư mục bất kỳ.
* **Bước 3:** Mở phần mền VMware. Sau đó nhấn vào **File**, chọn **Open…**, rồi tìm dẫn đến file vừa giải nén, chọn file có tên **kali-linux-2022.4-vmware-amd64.vmx** rồi chọn **Open**.
* **Bước 4:** Chọn **Power on this virtual machine** để tiến hành mở máy ảo.
* **Bước 5:** Khi đến màn hình đăng nhập, nhập kali ở cả 2 ô để tiền hành đăng nhập.
* **Bước 6:** Mở **Terminal** và nhập lệnh sau để tiến hành cập nhật.

***sudo apt update***

Hoặc ta cũng có thể làm theo hướng dẫn trong video : <https://youtu.be/FsSqXhebWXI>.

1. **Xây dựng máy chủ:**

**Windows Server 2022**: là một phiên bản của hệ điều hành máy chủ Windows Server, được phát triển dựa trên Windows 10 phiên bản 21H1.

Cấu hình yêu cầu tối thiểu:

* + CPU: 1.4 GHz (bản 64-bit).
  + RAM: 512 MB có tích hợp ECC.
  + Dung lượng ổ đĩa: 32 GB.
  + Tích hợp TPM: 2.0.

Các bước cài đặt:

* **Bước 1:** Tải xuống tệp ISO của Windows Server 2022 Standard theo đường dẫn:

<https://go.microsoft.com/fwlink/p/?LinkID=2195280&clcid=0x409&culture=en-us&country=US>.

* **Bước 2:** Mở VMware Workstation Pro 17 và chọn "Create a New Virtual Machine" để tạo máy ảo mới.
* **Bước 3:** Trong hộp thoại New Virtual Machine Wizard, chọn "Typical" và nhấp vào "Next".
* **Bước 4**: Chọn đường dẫn đến tệp ISO của Windows Server 2022 Standard đã tải xuống ở bước 1 và nhấp vào "Next".
* **Bước 5:** Đặt tên cho máy ảo của bạn và chọn đường dẫn để lưu trữ tệp máy ảo và nhấp vào "Next".
* **Bước 6:** Chọn dung lượng bộ nhớ RAM cho máy ảo của bạn và nhấp vào "Next".
* **Bước 7:** Chọn "Use bridged networking" để cho phép máy ảo truy cập vào mạng và nhấp vào "Next".
* **Bước 8:** Chọn "Create a new virtual disk" và nhấp vào "Next".
* **Bước 9:** Chọn định dạng ổ đĩa (VDI hoặc VMware Workstation virtual disk) và nhấp vào "Next".
* **Bước 10:** Chọn kích thước ổ đĩa và nhấp vào "Next".
* **Bước 11:** Nhấp vào "Finish" để tạo máy ảo của bạn.
* **Bước 12:** Bật máy ảo và chọn tệp ISO của Windows Server 2022 Standard để boot vào máy ảo.
* **Bước 13:** Thực hiện quá trình cài đặt trên máy ảo theo các hướng dẫn trên màn hình.
* **Bước 14:** Sau khi cài đặt xong, khởi động lại máy ảo và bắt đầu sử dụng.

Hoặc ta cũng có thể làm theo hướng dẫn trong video: <https://youtu.be/lBpp9wax-hw>.

* 1. **Cài đặt các công cụ**

1. **Hướng dẫn cài đặt WebServer thử nghiệm trên máy chủ**

**XAMPP** là một phần mềm nguồn mở và miễn phí dùng để tạo web server trên máy tính cá nhân (Localhost).

Các bước cài đặt:

* + **Bước 1:** Truy cập đường dẫn và chọn phiên bản phù hợp để tải về:

<https://www.apachefriends.org/download.html>

* + **Bước 2:** Sau khi đã tải về xong, mở file lên và liên tục nhấn Next và cuối cùng nhấn Finish.
  + **Bước 3:** Khởi động file **Xampp Control Panel** để mở bảng điều khiển.
  + **Bước 4:** Nhập vào ô **Config** trong dòng Apache và tiếp tục nhấn dòng có **httpd.conf**.
  + **Bước 5:** Tìm đến dòng Listen và sửa địa chỉ IP thành địa chỉ IP của máy chủ và port muốn mở rồi lưu.

1. **Hướng dẫn cài đặt công cụ Raven Storm (DoS Layer 7)**

**Raven Storm** là một công cụ mã nguồn mở được sử dụng để thực nghiệm tấn công DoS/DDoS

Cách cài đặt: mở Terminal trên máy tấn công và nhập lệnh:

***curl -s https://raw.githubusercontent.com/Taguar258/Raven-Storm/master/install.sh | sudo bash -s***

Hướng dẫn sử dụng RavenStorm: <https://github.com/Tmpertor/Raven-Storm>

1. **Bảng phân công công việc**

|  |  |
| --- | --- |
| **Họ và tên - MSV** | **Công việc** |
| Tạ Xuân Cường – AT170107 | Chương 1: Tổng quan về từ chối dịch vụ phân tán.  Tìm hiểu và tiến hành thực nghiệm HTTP Flood Attack |
| Đỗ Công Minh – AT170634 | Chương 2: Phân tích một số loại DDoS.  Tìm hiểu và tiến hành thực nghiệm SYN Flood Attack |
| Thái Hoàng Long – AT170130 | Chương 3: Cách phòng chống DDoS.  Tìm hiểu và tiến hành thực nghiệm HTTP Flood Attack |
| Cao Đắc Quân – AT170640 | Chương 3: Cách phòng chống DDoS.  Tìm hiểu và tiến hành thực nghiệm ICMP Flood Attack |