|  |  |
| --- | --- |
|  | BỘ GIÁO DỤC VÀ ĐÀO TẠO  **TRƯỜNG ĐẠI HỌC CÔNG NGHỆ TP. HCM** |

**ĐỒ ÁN BẢO MẬT THÔNG TIN**

**Đề tài : SYN FLOODING**

Ngành: **Công Nghệ Thông Tin**

Giảng viên hướng dẫn: ThS. Phan Đình Duy Thông

Sinh viên thực hiện Lớp MSSV

Trần Quang Thiện 22DTHH2 2280603066

Nguyễn Đại Kim Cương 22DTHH2 2280605169

Đỗ Văn Đạt 22DTHH2 2280606052

Nguyễn Tiến Vương 22DTHH2 2280603772

TP. Hồ Chí Minh, 2024

MỤC LỤC

[LỜI CẢM ƠN 2](#_Toc186735574)

[TÓM TẮT 3](#_Toc186735575)

[DANH MỤC CÁC KÝ HIỆU VÀ CHỮ VIẾT TẮT 4](#_Toc186735576)

[DANH MỤC CÁC HÌNH VÀ ĐỒ THỊ 5](#_Toc186735577)

[LỜI MỞ ĐẦU 6](#_Toc186735578)

[CHƯƠNG 1: TỔNG QUAN VỀ TẤN CÔNG SYN FLOOD 8](#_Toc186735579)

[1.1. Giới thiệu về tấn công SYN FLOOD 8](#_Toc186735580)

[1.2. Tầm quan trọng của nghiên cứu SYN Flooding 11](#_Toc186735581)

[1.3. Mối nguy hiểm và tác động của SYN Flooding 12](#_Toc186735582)

[1.4. Lộ trình thực hiện nghiên cứu 13](#_Toc186735583)

[CHƯƠNG 2: HIỆN TRẠNG VÀ DẤU HIỆU NHẬN DIỆN TẤN CÔNG SYN FLOOD 15](#_Toc186735584)

[2.1. Hiện trạng tấn công SYN Flood 15](#_Toc186735586)

[2.1.1. Thực trạng trên toàn cầu 15](#_Toc186735587)

[2.1.2. Thực trạng tại Việt Nam 15](#_Toc186735588)

[2.2. Dấu hiệu nhận diện tấn công SYN Flood 16](#_Toc186735589)

[2.2.1. Lưu lượng mạng bất thường 16](#_Toc186735590)

[2.2.2. Hiệu suất hệ thống suy giảm 16](#_Toc186735591)

[2.2.3. Bất thường trong log hệ thống 17](#_Toc186735592)

[2.3. Các công cụ giám sát và phân tích lưu lượng mạng 17](#_Toc186735593)

[CHƯƠNG 3: BIỆN PHÁP PHÒNG CHỐNG TẤN CÔNG SYN FLOOD 19](#_Toc186735594)

[3.1. Sử dụng tường lửa và bộ cân bằng tải 19](#_Toc186735596)

[3.2. Giới hạn tỷ lệ kết nối (Connection Rate Limiting) 19](#_Toc186735597)

[3.3. Sử dụng SYN Cookies 20](#_Toc186735598)

[3.4. Biện pháp phi kỹ thuật: Đào tạo và nâng cao nhận thức 20](#_Toc186735599)

[CHƯƠNG 4: KẾT QUẢ NGHIÊN CỨU 21](#_Toc186735600)

[4.1. Mô hình mô phỏng tấn công SYN Flooding 21](#_Toc186735605)

[4.1.1. Thiết lập mô hình mô phỏng 21](#_Toc186735606)

[4.1.2. Thực hiện Tấn công SYN Flood trực tiếp 25](#_Toc186735607)

[4.1.3. Thực hiệntấn công SYN Flood có giả mạo IP: 28](#_Toc186735608)

[CHƯƠNG 5: KẾT LUẬN 30](#_Toc186735609)

[NGUỒN THAM KHẢO 31](#_Toc186735610)

# LỜI CẢM ƠN

Để có thể hoàn thành tốt báo cáo đồ án học phần Bảo Mật Thông Tin: “SYN FLOODING”. Nhóm chúng em xin chân thành cảm ơn sự trợ giúp của thầy: ThS.Phan Đình Duy Thông, đã tận tình hướng dẫn chúng em về phương hướng cũng như cách thức, cung cấp nền tảng kiến thức vững chắc để chúng em có thể vận dụng, thực hiện tốt bài báo cáo của dự án lần này. Bên cạnh, nhóm cũng xin cảm ơn mỗi thành viên trong nhóm đã cố gắng hoàn thành tốt nhiệm vụ được giao và tận tình hỗ trợ lẫn nhau trong quá trình thực hiện và hoàn thành đề tài báo cáo trong môn học Bảo Mật Thông Tin.

# TÓM TẮT

Tấn công SYN Flood là một dạng tấn công từ chối dịch vụ (DoS), trong đó kẻ tấn công lợi dụng cơ chế “Bắt tay ba bước” (Three-Way Handshake) của giao thức TCP để gửi lượng lớn gói SYN giả mạo đến máy chủ. Điều này khiến máy chủ giữ các kết nối bán hoàn chỉnh, chiếm dụng tài nguyên và làm gián đoạn dịch vụ. Tấn công SYN Flood có thể thực hiện dưới dạng cơ bản (từ một nguồn) hoặc phân tán (DDoS), gây khó khăn trong việc phát hiện và ứng phó. Đây là một trong các loại tấn công phổ biến của DDoS, cùng với tấn công lượng lớn làm nghẽn mạng, chiếm dụng tài nguyên hệ thống, và khai thác lỗ hổng ứng dụng. Tấn công SYN Flood gây hậu quả nghiêm trọng, bao gồm giảm hiệu suất, gián đoạn dịch vụ, tổn thất tài chính và làm giảm uy tín của tổ chức bị tấn công.

# 

# DANH MỤC CÁC KÝ HIỆU VÀ CHỮ VIẾT TẮT

|  |  |
| --- | --- |
| **Ký hiệu/Chữ viết tắt** | **Ý nghĩa** |
| ACK | Cờ trong giao thức TCP dùng để xác nhận một kết nối |
| backlog | Danh sách các kết nối đang chờ xử lý trên máy chủ |
| Client | Máy khách, thiết bị yêu cầu tài nguyên hoặc dịch vụ từ máy chủ |
| DDoS | Tấn công từ chối dịch vụ phân tán |
| DoS | Tấn công từ chối dịch vụ |
| half-open | Kết nối chưa hoàn tất trong giao thức TCP |
| IDS | Hệ thống phát hiện xâm nhập |
| IPS | Hệ thống ngăn ngừa xâm nhập |
| outbound traffic | Lưu lượng dữ liệu được gửi ra ngoài từ một hệ thống mạng |
| Package | Gói dữ liệu được truyền trong mạng |
| Server | Máy chủ, cung cấp tài nguyên hoặc dịch vụ cho các thiết bị khác |
| SMEs | Doanh nghiệp vừa và nhỏ (Small and Medium-sized Enterprises) |
| SSH | Giao thức Secure Shell, dùng để truy cập và quản lý máy từ xa |
| SYN | Cờ trong giao thức TCP dùng để bắt đầu một kết nối |
| SYN Flood | Một loại tấn công từ chối dịch vụ (DoS) dựa trên giao thức TCP |
| SYN Flooding | Hiện tượng tấn công SYN Flood diễn ra liên tục và ở quy mô lớn |
| SYN\_RECEIVED | Trạng thái của một kết nối trong giao thức TCP khi chờ xác nhận (ACK) |
| TCP | Giao thức điều khiển truyền tải |

# DANH MỤC CÁC HÌNH VÀ ĐỒ THỊ

[BẢNG PHÂN CÔNG CÁC THÀNH VIÊN 7](#_Toc187023347)

[Bảng 1. Sự khác biệt giữa DoS và DdoS 11](#_Toc187023350)

[Hình 1: Quy trình bắt tay 3 bước TCP 9](#_Toc187023348)

[Hình 2: Cơ chế hoạt động SYN Flood 10](#_Toc187023349)

[Hình 3: Tấn công DoS và DdoS 12](#_Toc187023351)

[Hình 4: Biểu đồ thống kê tấn công DDoS tại một số quốc gia 17](#_Toc187023352)

[Hình 5: Phòng chống tấn công SYN Flood 18](#_Toc187023353)

[Hình 6: Top 10 Network Security Tools in 2022 20](#_Toc187023354)

[Hình 7: Khởi chạy SimpleDDoS trên Kali chờ máy mục tiêu kết nối. 25](#_Toc187023355)

[Hình 8: Chạy File WindowsUpdateTools.exe trên Windows Server 26](#_Toc187023356)

[Hình 9: Giao diện Fake Windows Update 26](#_Toc187023357)

[Hình 10: Thông tin mục tiêu hiển thị khi kết nối thành công. 27](#_Toc187023358)

[Hình 11: Giao diện Script 28](#_Toc187023359)

[Hình 12: Thực hiện tấn công trực tiếp 29](#_Toc187023360)

[Hình 13: Tác động của tấn công SYN Flood lên máy mục tiêu 29](#_Toc187023361)

[Hình 14: Thông tin kết nối SYN Flood hiển thị trong Wireshark 30](#_Toc187023362)

[Hình 15: Biểu đồ thống kê IO Graphs cho thấy đỉnh cao bất thường trong lưu lượng SYN 31](#_Toc187023363)

[Hình 16: Thông tin kết nối SYN FLood với hình thức tấn công có giả mạo hiển thị trong Wireshark 32](#_Toc187023364)

# LỜI MỞ ĐẦU

Với sự phát triển nhanh chóng của Internet hiện nay, công nghệ mạng đóng vai trò hết sức quan trọng. Đặc biệt trong thời kỳ Cách mạng Công nghiệp 4.0, Internet không chỉ mang lại những lợi ích to lớn mà còn đi kèm với nhiều thách thức tiềm tàng. Trong lĩnh vực công nghệ mạng, an ninh mạng đã trở thành ưu tiên hàng đầu của bất kỳ tổ chức hay doanh nghiệp nào, bất kể quy mô lớn hay nhỏ.

Hiện nay, các hacker luôn tìm mọi cách để tấn công và xâm nhập vào hệ thống nhằm đánh cắp thông tin nhạy cảm, gây ảnh hưởng nghiêm trọng đến hoạt động và sự tồn vong của doanh nghiệp. Theo số liệu thống kê từ nhiều tổ chức an ninh mạng, Việt Nam thường xuyên nằm trong nhóm các quốc gia bị tấn công mạng nhiều nhất, với các hình thức ngày càng tinh vi và nguy hiểm.

Một trong những hình thức tấn công điển hình, gây thiệt hại lớn nhưng vẫn duy trì mối đe dọa đáng kể trong môi trường mạng hiện nay là tấn công SYN Flooding. Đây là loại tấn công thuộc nhóm từ chối dịch vụ (DoS/DDoS), nhắm đến việc làm cạn kiệt tài nguyên của hệ thống máy chủ thông qua việc khai thác các lỗ hổng trong quá trình thiết lập kết nối TCP.

Nhận thấy tính cấp thiết và tầm quan trọng của việc hiểu rõ và phòng chống loại tấn công này, nhóm chúng em đã chọn nghiên cứu đề tài "SYN FLOODING". Qua nghiên cứu này, chúng em mong muốn làm rõ cơ chế tấn công, những nguy cơ tiềm ẩn cũng như đề xuất các biện pháp nhằm tăng cường bảo mật hệ thống, đóng góp một phần nhỏ vào việc bảo vệ an toàn thông tin trong môi trường mạng hiện nay.

Đề tài nghiên cứu 6 chương:

**Chương 1: Tổng quan về Tấn công SYN FLOOD**

**Chương 2: Hiện trạng và dấu hiệu nhận diện tấn công SYN Flood**

**Chương 3: Biện pháp phòng chống tấn công SYN Flood**

**Chương 4: Kết quả nghiên cứu**

**Chương 5: Kết luận**

**BẢNG PHÂN CÔNG CÁC THÀNH VIÊN**

|  |  |  |  |
| --- | --- | --- | --- |
| **TT** | **Họ và tên** | **Công việc phụ trách** | **Mức độ hoàn thành** |
|  | Trần Quang Thiện | Code, Word | 100% |
|  | Nguyễn Đại Kim Cương | Code, PowerPoint | 100% |
|  | Nguyễn Tiến Vương | Code, Word | 100% |
|  | Đỗ Văn Đạt | Code, PowerPoint | 100% |

# CHƯƠNG 1: TỔNG QUAN VỀ TẤN CÔNG SYN FLOOD

## 

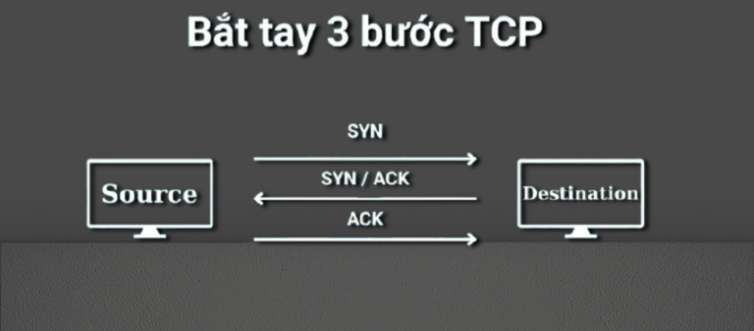
## Giới thiệu về tấn công SYN FLOOD

Tấn công SYN Flood là một trong những hình thức tấn công phổ biến và nguy hiểm đối với các hệ thống mạng, đặc biệt là các máy chủ cung cấp dịch vụ trực tuyến. Tấn công này lợi dụng cơ chế thiết lập kết nối của giao thức TCP, gây tê liệt các máy chủ và làm gián đoạn hoạt động của các dịch vụ trực tuyến.

Giao thức TCP (Transmission Control Protocol) là một giao thức quan trọng trong việc truyền tải dữ liệu giữa các máy tính trong mạng. Khi một máy tính muốn thiết lập một kết nối với máy chủ qua giao thức TCP, quá trình này thường được thực hiện thông qua một cơ chế gọi là “Bắt tay ba bước” (Three-Way Handshake). Quá trình này bao gồm ba bước:

**Bước 1**: Client gửi SYN packet (gói tin SYN) đến bên phía server để yêu cầu thiết lập kết nối.

**Bước 2**: Server nhận gói SYN, phản hồi lại bằng gói SYN-ACK để xác nhận yêu cầu kết nối.

**Bước 3**: Client nhận gói SYN-ACK và gửi lại một gói ACK để thông báo nhận thành công packet. Lúc này kết nối TCP mở và máy có thể gửi và nhận dữ liệu.

Hình 1: Quy trình bắt tay 3 bước TCP

Đối với hình thức tấn công [DDoS](https://vietnix.vn/ddos-la-gi/) SYN Flood, quá trình này sẽ bị thay đổi như sau:

1. Gửi SYN packet cho phía server thông báo mở kết nối.
2. Server phản hồi yêu cầu bằng SYN ACK packet để xác nhận.
3. Phía tấn công không gửi ACK packet hiện lại mà tiếp tục gửi SYN packet mới cho phía server.
4. Server nhận được SYN packet mới và không nhận được ACK packet của yêu cầu trước đó, buộc duy trì kết nối cũ và đồng thời mở kết nối mới.
5. Quá trình liên tục lặp lại và tài nguyên hệ thống mục tiêu bị tiêu bao ngày càng nhiều hơn, hiệu suất giảm rõ rệt.

Cuối cùng hệ thống quá tải cho tràn cache kết nối, Hiện tượng từ chối dịch vụ xảy ra và các truy cập hợp lệ sau đó sẽ không thể xử lý.

Trong kết nối mạng, khi 1 bên để kết nối mở trong khi phía còn lại thì không, đây được gọi là kết nối “half-open”. Hình thức này khi áp dụng vào tấn công [DDoS](https://vietnix.vn/ddos-la-gi/) sẽ gọi là tấn công “half-open”.

Có ba phương thức tấn công SYN Flood thường gặp bao gồm:A diagram of a computer

Description automatically generated

Hình 2: Cơ chế hoạt động SYN Flood

* Tấn công trực tiếp: Kẻ tấn công sử dụng địa chỉ IP thật mà không che giấu hoặc giả mạo. Do vậy, hình thức này dễ dàng bị phát hiện và đối phó. Các biện pháp thường áp dụng là thiết lập tường lửa để chặn các gói tin không hợp lệ hoặc lọc các gói SYN ACK trước khi chúng quay về phía kẻ tấn công. Tuy nhiên, vì sự đơn giản trong cách phòng thủ, loại tấn công này hiện ít được sử dụng.
* Tấn công có giả mạo: Bằng cách giả mạo địa chỉ IP trên các gói SYN, kẻ tấn công có thể che đậy danh tính và làm cho việc truy vết trở nên khó khăn hơn. Dù vậy, việc lần ra nguồn gốc của các gói tin vẫn khả thi nếu có sự hợp tác chặt chẽ giữa các bên liên quan, bao gồm cả các nhà cung cấp dịch vụ mạng.
* Tấn công DDoS: Ở phương thức này, kẻ tấn công tận dụng một mạng lưới botnet để thực hiện các cuộc tấn công quy mô lớn từ nhiều thiết bị khác nhau. Địa chỉ IP của mỗi gói tin gửi đi có thể được giả mạo, khiến việc xác định nguồn gốc trở nên cực kỳ phức tạp. Đặc biệt, trong các cuộc tấn công sử dụng botnet nổi tiếng như Mirai, việc che giấu địa chỉ IP của các thiết bị bot không còn là vấn đề lớn vì mức độ phá hoại đã đủ cao để gây ra hậu quả nghiêm trọng.

|  |  |
| --- | --- |
| DoS | DDoS |
| Là viết tắt của Denial of Service. | Là viết tắt của Distributed Denial of Service. |
| Chỉ một hệ thống nhắm mục tiêu vào hệ thống nạn nhân. | Nhiều hệ thống tấn công hệ thống nạn nhân. |
| Tấn công DoS chậm hơn so với DDoS. | Tấn công DDoS nhanh hơn tấn công DoS. |
| Có thể bị chặn dễ dàng vì chỉ sử dụng một hệ thống. | Rất khó để ngăn chặn cuộc tấn công này vì nhiều thiết bị đang gửi gói tin và tấn công từ nhiều vị trí. |
| Các cuộc tấn công DoS rất dễ theo dõi. | Các cuộc tấn công DDoS rất khó theo dõi. |
| Lưu lượng truy cập trong cuộc tấn công DoS ít hơn so với DDoS. | Các cuộc tấn công DDoS cho phép kẻ tấn công gửi một lượng lớn lưu lượng truy cập đến mạng nạn nhân. |
| Các loại tấn công DoS là:  1. Tấn công tràn bộ đệm 2. Tấn công Ping of Death hoặc ICMP flood 3. Tấn công Teardrop Attack | Các loại tấn công DDoS là:  1. [Tấn công Volumetric](https://quantrimang.com/volumetric-ddos-attack-la-gi-177778) (tấn công băng thông).  2. Tấn công Volumetric (tấn công băng thông). 3. Application Layer Attack (khai thác lỗ hổng trong các ứng dụng). |

Bảng 1. Sự khác biệt giữa DoS và DdoS

A diagram of a computer server

Description automatically generated

Hình 3: Tấn công DoS và DdoS

Khác với các cuộc tấn công làm ngập băng thông bằng lượng lớn lưu lượng truy cập, tấn công SYN Flood tập trung vào việc làm quá tải backlog của hệ điều hành mục tiêu. Khi kẻ tấn công nắm được dung lượng backlog và thời gian chờ của từng kết nối, chúng có thể thiết kế các gói tin tấn công với mức độ tối thiểu nhưng vẫn gây ra sự gián đoạn nghiêm trọng. Phương pháp này không chỉ hiệu quả mà còn giúp tiết kiệm tài nguyên tấn công, đồng thời tạo ra hậu quả nghiêm trọng cho hệ thống mục tiêu.

## Tầm quan trọng của nghiên cứu SYN Flooding

Việc nghiên cứu SYN Flooding là vô cùng quan trọng vì các cuộc tấn công này có thể gây ra thiệt hại nghiêm trọng đối với các hệ thống mạng. SYN Flooding không chỉ ảnh hưởng đến tính ổn định của hệ thống mà còn có thể gây thiệt hại tài chính cho các tổ chức khi hệ thống không thể phục vụ người dùng hợp pháp. Ngoài ra, các tấn công này có thể dễ dàng được thực hiện mà không cần nhiều tài nguyên, khiến cho chúng trở thành mối đe dọa lớn đối với các dịch vụ trực tuyến và hạ tầng mạng.

Một trong những lý do cần nghiên cứu SYN Flooding là để phát triển các biện pháp phòng chống và giảm thiểu tác động của loại tấn công này. Việc hiểu rõ cách thức hoạt động và các phương pháp bảo vệ sẽ giúp tăng cường khả năng bảo vệ hệ thống mạng khỏi những tấn công này. Hơn nữa, với sự gia tăng các mối đe dọa mạng hiện nay, việc nghiên cứu các phương thức tấn công như SYN Flooding trở nên cần thiết để bảo vệ các dịch vụ trực tuyến và dữ liệu quan trọng.

## Mối nguy hiểm và tác động của SYN Flooding

Tấn công SYN Flood gây ra những mối nguy hiểm và tác động nghiêm trọng đến hệ thống mục tiêu và doanh nghiệp:

* **Mối nguy hiểm**
* **Quá tải hệ thống:**
  + Tấn công SYN Flood khiến backlog của hệ thống bị đầy do phải duy trì nhiều kết nối “half-open” (kết nối không hoàn chỉnh).
  + Khi backlog đầy, hệ thống không thể xử lý thêm kết nối hợp lệ nào khác, dẫn đến tình trạng từ chối dịch vụ.
* **Khó phát hiện:**
  + Tấn công có giả mạo hoặc DDoS khiến việc truy vết nguồn gốc trở nên khó khăn, làm tăng thách thức trong việc ứng phó và khắc phục.
* **Lợi dụng botnet:**
  + Các botnet khổng lồ có thể tạo ra lưu lượng tấn công lớn mà không cần hacker trực tiếp tham gia, khiến việc kiểm soát và phòng thủ phức tạp hơn.
* **Tác động**
* **Mất dịch vụ:**
  + Các dịch vụ trực tuyến bị gián đoạn, ảnh hưởng đến hoạt động của doanh nghiệp và người dùng.
  + Gây thiệt hại về tài chính, đặc biệt đối với các dịch vụ thương mại điện tử hoặc ngân hàng trực tuyến.
* **Giảm uy tín doanh nghiệp:**
  + Một cuộc tấn công thành công có thể làm giảm niềm tin của khách hàng và đối tác vào doanh nghiệp.
  + Đối với các tổ chức lớn, việc bị tấn công có thể ảnh hưởng đến hình ảnh và thương hiệu.
* **Chi phí khắc phục cao:**
  + Doanh nghiệp phải đầu tư lớn vào việc nâng cấp cơ sở hạ tầng, triển khai các giải pháp bảo mật và xử lý hậu quả.
  + Tốn nhiều thời gian để phục hồi hoạt động bình thường.

## Lộ trình thực hiện nghiên cứu

* **Giai đoạn chuẩn bị (Tuần 1)**
* **Xác định mục tiêu nghiên cứu:**
  + Hiểu rõ khái niệm, cơ chế và hậu quả của tấn công SYN Flood.
  + Đánh giá hiệu quả của các biện pháp phòng chống hiện nay.
* **Tìm kiếm tài liệu:**
  + Thu thập tài liệu từ sách, báo cáo nghiên cứu, và các bài báo khoa học uy tín.
  + Tìm hiểu các tài liệu thực tiễn về an ninh mạng.
* **Phân công công việc:**
  + Chia công việc cụ thể cho từng thành viên (tìm tài liệu, viết báo cáo, thực nghiệm, thuyết trình).
* **Giai đoạn nghiên cứu lý thuyết (Tuần 2)**
* **Tìm hiểu về SYN Flood:**
  + Khám phá các kỹ thuật tấn công SYN Flood và cách chúng được triển khai.
  + Phân loại các hình thức tấn công: tấn công trực tiếp, giả mạo IP, và tấn công DDoS.
* **Khám phá cơ chế phòng thủ:**
  + Phân tích cách các hệ điều hành quản lý backlog và cơ chế timeout.
  + Tìm hiểu các công cụ bảo mật như tường lửa, IDS/IPS và các giải pháp hạn chế lưu lượng.
* **Tóm tắt và phân tích:**
  + Tổng hợp nội dung lý thuyết.
  + Xây dựng bảng so sánh giữa các phương pháp tấn công và phòng thủ.
* **Giai đoạn thực nghiệm (Tuần 3)**
* **Mô phỏng tấn công:**
  + Sử dụng các công cụ mạng như Wireshark hoặc Kali Linux để mô phỏng cuộc tấn công SYN Flood trong môi trường an toàn (máy ảo).
  + Quan sát các gói tin SYN, SYN-ACK và trạng thái "half-open" trên hệ thống mục tiêu.
* **Triển khai biện pháp phòng thủ:**
  + Thử nghiệm các biện pháp phòng thủ, ví dụ: cấu hình backlog, sử dụng tường lửa hoặc công cụ bảo mật khác.
  + Đánh giá hiệu quả của từng biện pháp dựa trên thời gian phản hồi và mức độ tiêu thụ tài nguyên.
* **Giai đoạn tổng hợp kết quả (Tuần 4)**
* **Phân tích và so sánh:**
  + Tổng hợp kết quả thực nghiệm và so sánh với lý thuyết.
  + Đánh giá những ưu và nhược điểm của các biện pháp phòng chống.
* **Viết báo cáo:**
  + Xây dựng báo cáo hoàn chỉnh gồm các phần: mục tiêu, phương pháp, kết quả, và đề xuất.
  + Chỉnh sửa báo cáo dựa trên góp ý của các thành viên.
* **Giai đoạn hoàn thiện và trình bày (Tuần 5)**
* **Chuẩn bị thuyết trình:**
  + Xây dựng bài thuyết trình ngắn gọn, tập trung vào các điểm nổi bật của nghiên cứu.
  + Thực hành thuyết trình để đảm bảo thời gian và khả năng tương tác.
* **Đóng góp ý tưởng:**
  + Đề xuất các biện pháp cải thiện hoặc hướng đi mới cho nghiên cứu trong tương lai.
* **Đánh giá và rút kinh nghiệm (Tuần 6)**
* **Tổng kết:**
  + Ghi nhận những bài học kinh nghiệm trong quá trình thực hiện.
  + Đánh giá hiệu quả làm việc nhóm.

# CHƯƠNG 2: HIỆN TRẠNG VÀ DẤU HIỆU NHẬN DIỆN TẤN CÔNG SYN FLOOD

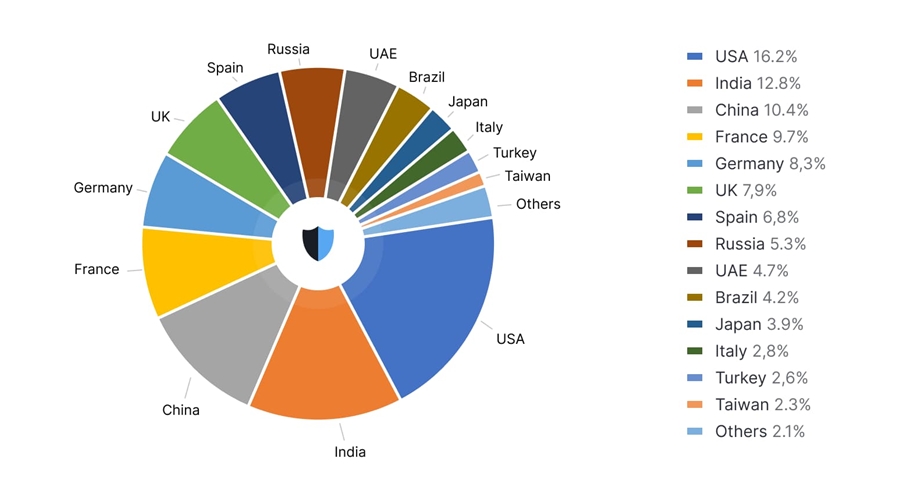


## Hiện trạng tấn công SYN Flood

Với sự phát triển nhanh chóng của công nghệ và Internet, các cuộc tấn công mạng, bao gồm SYN Flooding, ngày càng trở nên phổ biến và phức tạp. Hiện nay, SYN Flooding không chỉ là mối đe dọa đối với các doanh nghiệp mà còn ảnh hưởng đến các tổ chức chính phủ, cơ sở hạ tầng quan trọng và người dùng cá nhân.

### Thực trạng trên toàn cầu

* **Gia tăng số lượng tấn công:**
* Theo các báo cáo an ninh mạng, số lượng các cuộc tấn công từ chối dịch vụ (DoS) và phân tán từ chối dịch vụ (DDoS) đã tăng đều qua từng năm.
* SYN Flooding chiếm một tỷ lệ đáng kể trong các dạng tấn công DoS, nhắm vào các hệ thống có lỗ hổng hoặc khả năng bảo vệ yếu.
* **Sử dụng mạng botnet:**
* Hacker tận dụng các botnet khổng lồ như Mirai hoặc các thiết bị IoT không được bảo mật chặt chẽ để thực hiện các cuộc tấn công DDoS dựa trên SYN Flood.
* Những cuộc tấn công này có thể đạt lưu lượng hàng chục triệu gói dữ liệu mỗi giây, khiến hệ thống mục tiêu bị tê liệt.
* **Mục tiêu phổ biến:**
* Các tổ chức tài chính, dịch vụ thương mại điện tử, cơ sở hạ tầng viễn thông và các nhà cung cấp dịch vụ đám mây là những mục tiêu chính.
* Hệ thống của các doanh nghiệp vừa và nhỏ (SMEs) cũng dễ bị tấn công do hạn chế về ngân sách và nguồn lực bảo mật.



Hình 4: Biểu đồ thống kê tấn công DDoS tại một số quốc gia

Báo cáo Quý I/2023 của StormWall, được phát hành vào tháng 4/2023 cũng liệt kê Ấn Độ, Trung Quốc và Mỹ là ba quốc gia hàng đầu hứng chịu các cuộc tấn công DDoS. Người sáng lập và Giám đốc điều hành của StormWall, Ramil Khantimirov, đã bày tỏ mối lo ngại về xu hướng leo thang của các cuộc tấn công DDoS trong một số ngành công nghiệp. Ông nhấn mạnh sự cần thiết đối với các công ty, đặc biệt là những công ty về các dịch vụ thiết yếu, cần tăng cường các biện pháp bảo vệ DDoS.

### Thực trạng tại Việt Nam

* **Mức độ tấn công cao:**
* Việt Nam nằm trong nhóm các quốc gia có nguy cơ bị tấn công mạng cao, đặc biệt là các cuộc tấn công SYN Flood.
* Theo thống kê, các tổ chức tại Việt Nam thường thiếu hệ thống giám sát an ninh mạng chủ động, dẫn đến khó phát hiện và ứng phó kịp thời với các cuộc tấn công.
* **Thiếu nhận thức và giải pháp:**
* Nhiều doanh nghiệp nhỏ chưa nhận thức được mức độ nghiêm trọng của SYN Flooding và chưa đầu tư vào các giải pháp bảo mật tiên tiến.
* Hệ thống mạng cũ hoặc cấu hình bảo mật yếu cũng tạo điều kiện thuận lợi cho các cuộc tấn công xảy ra.

## Dấu hiệu nhận diện tấn công SYN Flood

Việc nhận diện sớm một cuộc tấn công SYN Flood là yếu tố quan trọng để giảm thiểu thiệt hại. A person holding a shield

Description automatically generated

Hình 5: Phòng chống tấn công SYN Flood

### Lưu lượng mạng bất thường

* **Tăng đột biến các gói SYN:**
* Số lượng gói SYN gửi đến máy chủ tăng cao đột ngột mà không có các gói ACK phản hồi tương ứng.
* Thường thấy sự gia tăng bất thường tại các cổng dịch vụ phổ biến như 80 (HTTP), 443 (HTTPS), hoặc 22 (SSH).
* **Tải trọng mạng không cân xứng:**
* Hệ thống ghi nhận lưu lượng lớn từ một hoặc nhiều địa chỉ IP trong khi không có lưu lượng phản hồi (outbound traffic) đáng kể.

### Hiệu suất hệ thống suy giảm

* **Server phản hồi chậm:**
* Thời gian phản hồi của server tăng lên đáng kể do backlog bị lấp đầy bởi các kết nối “half-open.”
* Các dịch vụ quan trọng như website, cơ sở dữ liệu, hoặc ứng dụng bị gián đoạn hoặc ngừng hoạt động.
* **Tăng sử dụng tài nguyên:**
* CPU, bộ nhớ, và băng thông của server bị sử dụng ở mức tối đa.
* Các kết nối hợp lệ bị từ chối do không còn tài nguyên để xử lý.

### Bất thường trong log hệ thống

* **Lượng lớn kết nối không hoàn chỉnh:**
* Các log của hệ điều hành hoặc thiết bị mạng cho thấy lượng lớn các kết nối TCP không hoàn chỉnh, chỉ dừng lại ở trạng thái SYN\_RECEIVED.
* **Địa chỉ IP bất thường:**
* Xuất hiện nhiều kết nối từ các địa chỉ IP không hợp lệ hoặc không tồn tại.
* Trong trường hợp tấn công giả mạo hoặc DDoS, các địa chỉ IP có thể thay đổi liên tục và không tuân theo bất kỳ quy luật nào.

Tấn công SYN Flood là một trong những hình thức tấn công mạng nguy hiểm và phổ biến, gây ra nhiều hậu quả nghiêm trọng cho hệ thống mục tiêu. Hiện trạng thực tế tại Việt Nam cho thấy mức độ tổn thương của các doanh nghiệp trước loại tấn công này vẫn còn cao, do thiếu hụt về giải pháp bảo mật và nhận thức. Nhận diện kịp thời các dấu hiệu tấn công SYN Flood là bước đầu tiên và quan trọng trong việc giảm thiểu rủi ro và bảo vệ hệ thống.

### Các công cụ giám sát và phân tích lưu lượng mạng

Để nhận diện và ngăn chặn kịp thời các cuộc tấn công SYN Flood, việc sử dụng các công cụ giám sát và phân tích lưu lượng mạng là rất cần thiết. Những công cụ này giúp quản trị viên phát hiện các hành vi bất thường, phân tích nguyên nhân và đưa ra biện pháp phòng ngừa hiệu quả.

****

Hình 6: Top 10 Network Security Tools in 2022

**Wireshark:** phân tích gói tin mạnh mẽ, Wireshark cho phép ghi lại và kiểm tra các gói tin TCP/IP để phát hiện lưu lượng SYN bất thường. Cung cấp thông tin chi tiết về các gói SYN gửi đến, địa chỉ IP nguồn, và trạng thái của các kết nối TCP.

**Nagios:** Giám sát trạng thái của các thiết bị mạng, server, và dịch vụ. Cảnh báo khi phát hiện lưu lượng SYN bất thường hoặc server hoạt động vượt mức tải. Tùy chỉnh cao và hỗ trợ nhiều plugin.

**Snort:** Là một hệ thống phát hiện xâm nhập (IDS) và ngăn chặn xâm nhập (IPS), Snort có khả năng phát hiện các cuộc tấn công SYN Flood dựa trên các quy tắc xác định trước. Miễn phí và mạnh mẽ, được sử dụng rộng rãi trong cộng đồng an ninh mạng. Dễ dàng tích hợp với các công cụ giám sát khác.

**Splunk:** Thu thập và phân tích log từ hệ thống mạng, giúp nhận diện các bất thường liên quan đến SYN Flood. Cung cấp biểu đồ trực quan và báo cáo chi tiết. Có khả năng mở rộng và tích hợp với các hệ thống khác. Cảnh báo tự động khi phát hiện lưu lượng bất thường.

**ELK Stack (Elasticsearch, Logstash, Kibana):** là một bộ công cụ mã nguồn mở dùng để thu thập, phân tích và trực quan hóa dữ liệu log mạng. Hỗ trợ giám sát lưu lượng SYN để phát hiện các dấu hiệu tấn công. Miễn phí, mã nguồn mở và tùy chỉnh linh hoạt. Giao diện trực quan và dễ sử dụng với Kibana.

# CHƯƠNG 3: BIỆN PHÁP PHÒNG CHỐNG TẤN CÔNG SYN FLOOD

Các cuộc tấn công SYN Flood có thể gây ảnh hưởng nghiêm trọng đến tính sẵn sàng và hiệu suất của hệ thống mạng. Do đó, việc triển khai các biện pháp phòng chống hiệu quả là rất cần thiết. Chương này sẽ trình bày những biện pháp phòng chống kỹ thuật và phi kỹ thuật nhằm giảm thiểu tác động của các cuộc tấn công SYN Flood.



## Sử dụng tường lửa và bộ cân bằng tải

* **Tường lửa (Firewall):** là tuyến phòng thủ đầu tiên để bảo vệ hệ thống mạng khỏi các mối đe dọa. Các tường lửa hiện đại có khả năng phát hiện và ngăn chặn các gói SYN bất thường trước khi chúng đến máy chủ mục tiêu.
* **Cách triển khai:**
* Lọc gói (Packet Filtering): Chặn các gói SYN từ những nguồn đáng ngờ hoặc giới hạn số lượng kết nối mới từ một IP cụ thể.
* Deep Packet Inspection (DPI): Phân tích sâu vào từng gói tin để phát hiện các mẫu lưu lượng bất thường.
* **Ưu điểm:**
* Hiệu quả trong việc chặn các cuộc tấn công trực tiếp hoặc quy mô nhỏ.
* **Nhược điểm:**
* Có thể không đủ mạnh để chống lại các cuộc tấn công DDoS lớn.
* **Bộ cân bằng tải (Load Balancer):** Phân phối lưu lượng mạng đến nhiều máy chủ, giảm tải cho một máy chủ đơn lẻ. Khi xảy ra tấn công SYN Flood, bộ cân bằng tải giúp phân tán lưu lượng, ngăn chặn việc quá tải cho một nút mạng duy nhất.
* **Ưu điểm:**
* Tăng khả năng chịu tải và giảm nguy cơ từ chối dịch vụ.
* **Nhược điểm:**
* Chi phí triển khai cao và yêu cầu kiến thức chuyên sâu để cấu hình.

## Giới hạn tỷ lệ kết nối (Connection Rate Limiting)

Giới hạn tỷ lệ kết nối là một kỹ thuật thiết lập giới hạn số lượng kết nối mới mà mỗi IP có thể tạo trong một khoảng thời gian nhất định. Điều này ngăn chặn các nguồn không xác định gửi quá nhiều yêu cầu SYN liên tiếp đến hệ thống.

**Cách triển khai:**

* Cấu hình trên tường lửa hoặc router để giới hạn kết nối từ mỗi địa chỉ IP.
* Sử dụng các công cụ như iptables (trên Linux) để giới hạn số lượng gói SYN.

**Ưu điểm:** Hiệu quả đối với các cuộc tấn công sử dụng số lượng lớn SYN từ một số nguồn nhất định.

**Nhược điểm:** Có thể gây ra hiện tượng từ chối dịch vụ đối với các IP hợp lệ nếu giới hạn quá chặt.

## Sử dụng SYN Cookies

SYN Cookies là một cơ chế bảo mật được sử dụng trong giao thức TCP nhằm giảm thiểu tác động của các cuộc tấn công SYN Flood. Khi hệ thống nhận được gói SYN, thay vì lưu thông tin kết nối trong backlog, nó sẽ mã hóa thông tin này thành một cookie và gửi lại cho máy khách trong gói SYN-ACK. Máy chủ chỉ tạo kết nối đầy đủ khi nhận được phản hồi ACK hợp lệ.

**Cách triển khai:**

* Kích hoạt SYN Cookies trên hệ điều hành. Ví dụ, trong Linux:

echo 1 > /proc/sys/net/ipv4/tcp\_syncookies

**Ưu điểm:** Giảm thiểu yêu cầu tài nguyên trên hệ thống, bảo vệ backlog khỏi bị đầy.

**Nhược điểm:** Không hỗ trợ đầy đủ các tùy chọn TCP, gây ảnh hưởng đến một số ứng dụng mạng phức tạp.

## Biện pháp phi kỹ thuật: Đào tạo và nâng cao nhận thức

* **Đào tạo nhân sự:**
  + Đảm bảo rằng đội ngũ quản trị mạng và nhân viên IT hiểu rõ về các mối đe dọa từ tấn công SYN Flood cũng như các biện pháp phòng chống hiệu quả.
  + Tổ chức các khóa đào tạo định kỳ về an ninh mạng, tập trung vào phát hiện và ứng phó với các cuộc tấn công.
* **Nâng cao nhận thức:**
  + Tuyên truyền cho toàn bộ nhân viên trong tổ chức về tầm quan trọng của bảo mật thông tin, giúp họ nhận diện các dấu hiệu bất thường trong hệ thống mạng.
  + Áp dụng chính sách bảo mật nội bộ, bao gồm quản lý mật khẩu và hạn chế truy cập không cần thiết.
* **Phối hợp với nhà cung cấp dịch vụ (ISP):**
  + Liên hệ và hợp tác chặt chẽ với các ISP để truy vết nguồn gốc tấn công và triển khai các biện pháp ngăn chặn từ phía nhà cung cấp dịch vụ.

# CHƯƠNG 4: KẾT QUẢ NGHIÊN CỨU



## Mô hình mô phỏng tấn công SYN Flooding

Để hiểu rõ hơn về cách thức hoạt động của tấn công SYN Flooding, một mô hình mô phỏng đã được xây dựng. Mô phỏng này giúp quan sát được hành vi của các gói SYN khi tấn công vào một hệ thống mạng và ảnh hưởng của chúng đối với khả năng xử lý của máy chủ.

### Thiết lập mô hình mô phỏng

* **Hai máy Linux (Máy tấn công) (IP: 192.168.182.128):** thực hiện tấn công vào máy server. Đồng thời sử dụng công cụ **Wireshark** để theo dõi và ghi lại các gói SYN được gửi đi, cũng như theo dõi các thay đổi về hiệu suất và trạng thái của máy server.
* **Máy Windows Server (Máy mục tiêu) (IP: 192.168.182.132):** Chịu trách nhiệm tiếp nhận các kết nối từ hai máy Linux. Máy Windows Server sẽ được cấu hình để có thể phản hồi các yêu cầu kết nối TCP thông qua các gói SYN, SYN-ACK, ACK. Tuy nhiên, khi bị tấn công, máy sẽ không thể xử lý tất cả các kết nối hợp lệ và sẽ gặp tình trạng đầy backlog.

**Bước 1: Cấu hình môi trường và chuẩn bị công cụ:**

* **Windows Server:** Chuẩn bị file WindowsUpdateTools từ <http://github.com/NTVuong23/BMTT.git>.
* **Kali:** Tải công cụ về máy.

┌──(kali㉿kali)-[~]

└─$ git clone https://github.com/NTVuong23/BMTT.git

**Bước 2: Chạy công cụ thiết lập chờ máy mục tiêu “cắn câu”:**

**A screenshot of a computer

Description automatically generated**Hình 7: Khởi chạy SimpleDDoS trên Kali chờ máy mục tiêu kết nối.

* Trong trường hợp này chúng ta giả sử máy mục tiêu (Windows Server) người dùng (hoặc mục tiêu) khởi chạy file **WindowsUpdateTools.exe**. Đây là file giả mạo, khi được thực thi sẽ:
  + Hiển thị giao diện giả lập cập nhật Windows.
  + Vô hiệu hóa tường lửa trên máy mục tiêu.
  + Kích hoạt kết nối với máy tấn công qua địa chỉ IP 192.168.182.128 (máy Kali Linux) thông qua cổng 80.

**A screenshot of a computer

Description automatically generated**

Hình 8: Chạy File WindowsUpdateTools.exe trên Windows Server

* Khi mục tiêu nhấn vào button **Download and install** máy của mục tiêu sẽ tự động tắt tường lửa và ping tới IP: 192.168.182.128 của máy Linux có và hiện Form thông báo.

**A screenshot of a computer

Description automatically generated**

Hình 9: Giao diện Fake Windows Update

**Bước 3: Thiết lập tấn công trên máy Kali Linux**

* **Quan sát kết nối:**
* Sau khi mục tiêu kích hoạt mã độc, kiểm tra thông tin kết nối trên máy Kali:
  + - Máy mục tiêu đã kết nối tới IP: 192.168.182.132.
    - Sử dụng cổng: 80.

A screenshot of a computer

Description automatically generated

Hình 10: Thông tin mục tiêu hiển thị khi kết nối thành công.

* Chạy lệnh sau để cấp quyền thực thi cho script và mở công cụ tấn công dưới quyền root:

┌──(kali㉿kali)-[~/…/Tools/SimpleDDoS/build/classes]

└─$ sudo su

[sudo] password for kali:

┌──(root㉿kali)-[/home/…/Tools/SimpleDDoS/build/classes]

└─# cd /home/kali/BMTT/Tools

┌──(root㉿kali)-[/home/kali/BMTT/Tools]

└─# chmod +x synflood.sh

┌──(root㉿kali)-[/home/kali/BMTT/Tools]

└─# ./synflood.sh

A screenshot of a computer

Description automatically generated  
Hình 11: Giao diện Script

### Thực hiện Tấn công SYN Flood trực tiếp

* **Bắt đầu tấn công:**
  + Script bắt đầu gửi các gói SYN đến máy Windows Server. Chúng ta thực hiện tấn công trực tiếp đầu tiên để dễ dàng quan sát hơn trong lúc tấn công.
  + Các gói SYN được gửi liên tục, làm đầy hàng đợi kết nối (backlog) trên máy mục tiêu.

A screenshot of a computer

Description automatically generated

Hình 12: Thực hiện tấn công trực tiếp

* **Quan sát trên máy mục tiêu:**
* Máy Windows Server bắt đầu gặp khó khăn trong việc xử lý các kết nối mới:
  + CPU tăng đột biến.
  + Bộ nhớ hệ thống bị tiêu tốn nhanh chóng.
  + Các kết nối hợp lệ từ máy khách không được xử lý do backlog đã đầy.

A screenshot of a computer

Description automatically generated  
Hình 13: Tác động của tấn công SYN Flood lên máy mục tiêu

* **Theo dõi bằng công cụ giám sát:** Trên máy Kali, tiến hành mở công cụ Wireshark để ghi lại toàn bộ lưu lượng mạng trong thời gian thực. Quá trình theo dõi diễn ra như sau:
* **Bắt đầu ghi lại lưu lượng mạng:**
  + Khởi chạy Wireshark và chọn giao diện mạng phù hợp (ví dụ: eth0 hoặc wlan0) để theo dõi lưu lượng đi qua mạng nội bộ.
  + Sử dụng bộ lọc tcp.flags.syn == 1 && tcp.flags.ack == 0 để chỉ tập trung vào các gói SYN đang gửi đi.
* **Quan sát lưu lượng bất thường:**
  + Trong danh sách các gói tin, nhận thấy một lượng lớn gói SYN được gửi từ địa chỉ IP nguồn **192.168.182.128** (máy Kali) đến địa chỉ IP đích **192.168.182.132** (Windows Server).
  + A screenshot of a computer

    Description automatically generatedCác gói tin SYN này xuất hiện liên tục với tần suất cao, không có gói ACK phản hồi từ máy đích, cho thấy sự bất thường trong giao tiếp mạng.

Hình 14: Thông tin kết nối SYN Flood hiển thị trong Wireshark

* **Phân tích chi tiết:**
  + Thời gian giữa các gói SYN được gửi rất ngắn, điều này xác nhận hành vi tấn công SYN Flooding, vì máy Kali cố tình mở nhiều kết nối đồng thời mà không hoàn tất bắt tay 3 bước.
  + Truy cập vào chi tiết của từng gói tin, thông tin bao gồm:
    - **Source Port:** Cổng nguồn trên máy Kali (được thay đổi liên tục).
    - **Destination Port:** Cổng đích trên Windows Server (80).
    - **Flags:** Chỉ có cờ SYN được bật.
* **Biểu đồ thống kê lưu lượng mạng:**
  + Sử dụng tính năng **Statistics > IO Graphs** của Wireshark để hiển thị số lượng gói SYN gửi đi theo thời gian.
  + Biểu đồ hiển thị một đỉnh lớn, cho thấy sự gia tăng đột ngột của gói SYN trong khoảng thời gian ngắn, khớp với thời điểm thực hiện tấn công.

A screenshot of a computer

Description automatically generatedHình 15: Biểu đồ thống kê IO Graphs cho thấy đỉnh cao bất thường trong lưu lượng SYN

### Thực hiệntấn công SYN Flood có giả mạo IP:

* **Địa chỉ IP giả mạo**: Địa chỉ IP nguồn (random) không phải của máy tấn công thực sự, nhằm mục đích làm sai lệch thông tin nguồn gốc.
* **Khó truy vết**: Việc truy vết địa chỉ nguồn trở nên phức tạp hơn do kẻ tấn công liên tục thay đổi địa chỉ IP giả mạo. Điều này đòi hỏi sự phối hợp giữa nhiều bên liên quan, bao gồm cả nhà cung cấp dịch vụ Internet (ISP).
* **Hậu quả**: Máy đích sẽ bị tắc nghẽn backlog bởi các gói SYN giả mạo, dẫn đến tình trạng không thể đáp ứng các yêu cầu kết nối hợp lệ từ người dùng thực sự.

A screenshot of a computer

Description automatically generated

Hình 16: Thông tin kết nối SYN FLood với hình thức tấn công có giả mạo hiển thị trong Wireshark

* **Đánh giá:** Dựa trên kết quả ghi nhận, tấn công SYN Flooding đã gây ra hiện tượng backlog trên Windows Server, dẫn đến việc từ chối dịch vụ tạm thời. Các thông số lưu lượng rõ ràng phản ánh dấu hiệu của cuộc tấn công DoS.

# CHƯƠNG 5: KẾT LUẬN

Tấn công SYN Flood thực sự là một mối đe dọa đáng lo ngại đối với các hệ thống mạng và dịch vụ trực tuyến. Qua quá trình tìm hiểu và thực hành, chúng em đã có cái nhìn rõ hơn về cách thức hoạt động của loại tấn công này, khi kẻ xấu lợi dụng giao thức TCP để tạo ra các kết nối chưa hoàn tất, làm tiêu hao tài nguyên của máy chủ mục tiêu và khiến hệ thống bị quá tải, không thể phục vụ các yêu cầu hợp lệ.

Thông qua việc mô phỏng tấn công SYN Flood trong môi trường Kali Linux, chúng em nhận thấy rằng việc phát hiện kịp thời và áp dụng các biện pháp phòng ngừa như sử dụng tường lửa, bộ cân bằng tải, hay kỹ thuật SYN Cookies có thể làm giảm đáng kể thiệt hại mà tấn công này gây ra. Tuy nhiên, đây chỉ là những biện pháp trong ngắn hạn, và thực tế bảo mật mạng đòi hỏi sự phối hợp đồng bộ của nhiều giải pháp khác nhau.

Chúng em cũng hiểu rằng, dù các biện pháp được đề xuất chưa thể đảm bảo ngăn chặn hoàn toàn mọi cuộc tấn công, nhưng việc không ngừng nâng cao nhận thức và kiến thức về các loại mối đe dọa như SYN Flooding là yếu tố tiên quyết. Điều này giúp cho các nhà quản trị hệ thống có sự chuẩn bị tốt hơn, chủ động đối phó khi sự cố xảy ra.

Nhìn chung, SYN Flooding là một thách thức lớn nhưng cũng là bài học quý giá cho chúng em trong hành trình tìm hiểu về an ninh mạng. Những nghiên cứu và trải nghiệm thực tế này giúp chúng em nhận thức rõ rằng bảo mật mạng không phải là một công việc nhất thời mà là một quá trình bền bỉ, đòi hỏi sự cẩn trọng và sáng tạo trong mọi chiến lược bảo vệ hệ thống.

# NGUỒN THAM KHẢO

* 1. https://antoanthongtin.vn/hacker-malware/tan-cong-ddos-tang-168-tren-dich-vu-cua-chinh-phu-nhieu-nuoc-tren-the-gioi-109148
  2. <https://luanvan.net.vn/luan-van/do-an-tan-cong-ddos-28478/>
  3. <https://www.studocu.vn/vn/document/truong-dai-hoc-duy-tan/thi-giac-may/do-an-an-ninh-mang/63435716>
  4. <https://quantrimang.com/cong-nghe/tim-hieu-ve-tan-cong-tu-choi-dich-vu-dos-34926>
  5. <https://vietnix.vn/syn-flood/>