

TRƯỜNG ĐẠI HỌC: CÔNG NGHỆ TP.HCM

**KHOA: CÔNG NGHỆ THÔNG TIN**

**BÁO CÁO TIỂU LUẬN**

**Học phần: Bảo mật thông tin**

***Chuyên đề:* DOS/DDOS**

**Thành viên:**

Đặng Lâm Thế Nhân - 2280612138

Trần Quốc Đại - 2280600549

Đinh Quốc Cường - 2280618437

Vũ Dương Hoàng Phước - 2280602515

Lớp: **22DTHB2**

Giáo viên hướng dẫn: **Nguyễn Thị Yến**

**TP.HCM, tháng 09/2024**

**DANH SÁCH THÀNH VIÊN**

| **Họ và tên** | **MSSV** | **Tỷ lệ đóng góp** |
| --- | --- | --- |
| **Đặng Lâm Thế Nhân** | **2280612138** | **100%** |
| **Trần Quốc Đại** | **2280600549** | **100%** |
| **Đinh Quốc Cường** | **2280618437** | **100%** |
| **Vũ Dương Hoàng Phước** | **2280602515** | **100%** |

**MỤC LỤC**

# 

[**1.1. Tính cấp thiết của đề tài**](#_fb89cvtdx7of) **5**

[**1.2. Mục đích và nhiệm vụ nghiên cứu**](#_yy4axvabbl8) **5**

[**1.3. Đối tượng và phạm vi nghiên cứu**](#_3z0dl4wuqp9d) **6**

[**1.4. Câu hỏi nghiên cứu**](#_5hd23oikskzk) **6**

[**1.5. Ý nghĩa của tiểu luận**](#_t3w8xsolw3o5) **6**

[**1.6. Phương pháp nghiên cứu**](#_ooigo2x6b4ps) **6**

[**1.7. Kết của bài tiểu luận**](#_77man2l5x1kl) **6**

[**2.1. DoS**](#_fnuciwv5y4c9) **6**

[**2.2. DDoS**](#_sw9mltbboknt) **9**

[**2.3. Sự Khác Nhau và Điểm Giống Nhau Giữa DoS và DDoS**](#_yma3bfmqxrtl) **11**

[**2.4. Đặc điểm của tấn công DoS và DDoS**](#_lb9iwg5fs9hr) **12**

[**2.5. Các loại hình thức tấn công**](#_m0k4v3ke7tkf) **14**

[**2.6. Biện pháp phòng ngừa, ngăn chặn trước DOS và DDOS**](#_fnpiamvip6to) **16**

[**2.7 Case study**](#_vgvyiovnq2zt) **19**

[**So sánh sự khác nhau trong cách thức tấn công DoS và DDoS**](#_7kl7s3j9exnr) **21**

# 

**LỜI MỞ ĐẦU**

Trong thời đại kỹ thuật số, internet đã trở thành nền tảng không thể thiếu cho hoạt động của các tổ chức, doanh nghiệp và người dùng cá nhân. Tuy nhiên, cùng với sự phát triển này, các mối đe dọa về an ninh mạng cũng không ngừng gia tăng. Trong số đó, các cuộc tấn công từ chối dịch vụ (DoS) và tấn công từ chối dịch vụ phân tán (DDoS) đang trở thành một thách thức lớn đối với việc bảo vệ các hệ thống mạng. Những cuộc tấn công này không chỉ làm gián đoạn hoạt động của các tổ chức mà còn có thể gây ra tổn thất nghiêm trọng về kinh tế và uy tín.

Nhằm mục tiêu nâng cao hiểu biết và tìm ra những giải pháp hiệu quả để phòng chống các cuộc tấn công DoS và DDoS, tiểu luận này tập trung phân tích cơ chế, phương pháp tấn công và các biện pháp bảo vệ hiện nay. Thông qua nghiên cứu, chúng tôi hy vọng đóng góp một phần vào việc bảo vệ hệ thống mạng trong bối cảnh công nghệ đang phát triển nhanh chóng.

**DANH MỤC CÁC CHỮ VIẾT TẮT**

**DoS:** Denial of Service

**DDoS:** Distributed Denial of Service

**LOIC:** Low Orbit Ion Cannon

**HOIC:** High Orbit Ion Cannon

**IoT**: Internet of Things

**NỘI DUNG**

# **1.1 Tính cấp thiết của đề tài**

Với sự phát triển mạnh mẽ của công nghệ thông tin và sự phổ biến của internet, các mối đe dọa về an ninh mạng ngày càng trở nên nghiêm trọng hơn. Tấn công từ chối dịch vụ (DoS) và tấn công từ chối dịch vụ phân tán (DDoS) là hai trong những hình thức tấn công mạng phổ biến và nguy hiểm nhất hiện nay. Những cuộc tấn công này có thể làm gián đoạn hoạt động của các hệ thống, gây thiệt hại lớn về kinh tế và uy tín cho các tổ chức và doanh nghiệp. Việc nghiên cứu và hiểu rõ về DoS và DDoS là cấp thiết để nâng cao khả năng phòng chống và giảm thiểu tác động của các cuộc tấn công này.

**1.2 Mục đích và nhiệm vụ nghiên cứu**

**1.2.1 Mục đích**

Mục đích của nghiên cứu này là hiểu rõ cơ chế, phương pháp và hậu quả của các cuộc tấn công DoS và DDoS, từ đó đề xuất các giải pháp phòng chống hiệu quả để bảo vệ hệ thống thông tin.

**1.2.2 Nhiệm vụ**

Phân tích cơ bản về tấn công DoS và DDoS, bao gồm các loại hình và phương thức tấn công.

Đánh giá các hệ thống phòng chống hiện có và đưa ra nhận xét về hiệu quả của chúng.

Đề xuất các biện pháp và chiến lược mới để tăng cường bảo mật và giảm thiểu thiệt hại từ các cuộc tấn công DoS và DDoS.

**1.3 Đối tượng và phạm vi nghiên cứu**

**1.3.1 Đối tượng**

Nghiên cứu tập trung vào các cuộc tấn công DoS và DDoS trong môi trường mạng hiện nay, bao gồm cả hệ thống doanh nghiệp lớn và người dùng cá nhân. Phạm vi bao gồm cả các biện pháp phòng chống tại thời điểm hiện tại và những đề xuất cho tương lai.

**1.3.2 Phạm vi nghiên cứu**

Nghiên cứu tập trung vào các cuộc tấn công DoS và DDoS trong môi trường mạng hiện nay, bao gồm cả hệ thống doanh nghiệp lớn và người dùng cá nhân. Phạm vi bao gồm cả các biện pháp phòng chống tại thời điểm hiện tại và những đề xuất cho tương lai.

**1.4 Câu hỏi nghiên cứu**

Tấn công DoS và DDoS hoạt động như thế nào, và chúng ảnh hưởng đến các hệ thống mạng ra sao?

Những biện pháp nào đang được sử dụng để phòng chống tấn công DoS và DDoS?

Có những phương pháp mới nào có thể được áp dụng để tăng cường bảo mật chống lại các cuộc tấn công này?

**1.5 Ý nghĩa của tiểu luận**

Tiểu luận này có ý nghĩa quan trọng trong việc cung cấp một cái nhìn toàn diện về các mối đe dọa từ DoS và DDoS, từ đó nâng cao nhận thức và hiểu biết về vấn đề này cho các cá nhân và tổ chức. Kết quả nghiên cứu có thể giúp xây dựng các chiến lược bảo vệ hiệu quả hơn, góp phần vào việc đảm bảo an toàn cho hệ thống mạng và dữ liệu.

**1.6 Phương pháp nghiên cứu**

Phương pháp nghiên cứu chủ yếu bao gồm phân tích tài liệu, khảo sát các cuộc tấn công DoS và DDoS đã xảy ra, và đánh giá các công cụ, phương pháp phòng chống hiện có. Nghiên cứu cũng bao gồm việc mô phỏng một số cuộc tấn công để hiểu rõ cơ chế hoạt động và đánh giá hiệu quả của các biện pháp phòng chống.

**1.7 Kết của bài tiểu luận**

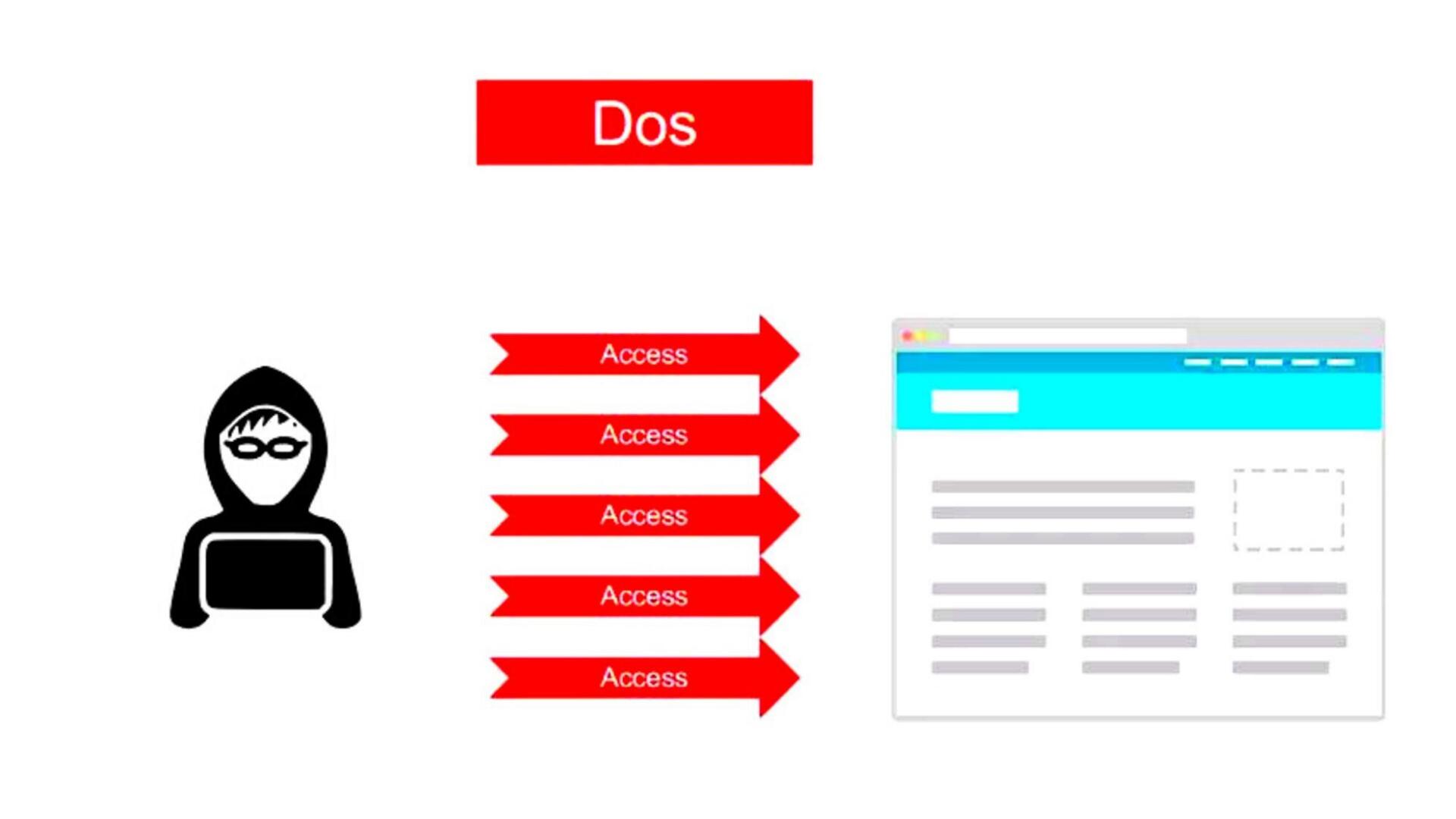
Bài tiểu luận sẽ cung cấp cái nhìn tổng quan về tấn công DoS và DDoS, đồng thời đề xuất những phương pháp phòng chống mới có thể áp dụng trong thực tế. Những kết quả này sẽ có thể giúp các tổ chức và cá nhân nâng cao khả năng đối phó với các mối đe dọa an ninh mạng.

# **2.1 DoS**

**DoS là gì?**

DoS viết tắt của cụm từ Denial of Service, là một kiểu tấn công từ chối dịch vụ khi đó máy tính của bạn sẽ bị tấn công bởi lưu lượng truy cập từ hệ thống của hacker. DoS là một cuộc tấn công trực tuyến thường nhắm vào một trang web hoặc máy chủ điển hình. Bằng cách làm quá tải tài nguyên hệ thống, tốc độ hệ thống của máy tính sẽ bị chậm lại đáng kể.

Cuộc tấn công này có thể khiến máy tính của bạn ngừng hoạt động hoặc tắt đột ngột. Khi hiện tượng này xảy ra sẽ ảnh hưởng nghiêm trọng đến hệ thống của máy tính và buộc máy tính phải tắt nguồn.



**2.1.1 Cách Thức Hoạt Động**

Xuất hiện một kẻ tấn công khiến cho tài nguyên của hệ thống dần trở nên cạn kiệt qua các mục tiêu như băng thông mạng, dung lượng bộ nhớ, hoặc khả năng xử lý của CPU. Hệ thống không thể tiếp tục hoạt động bình thường bởi khi các tài nguyên này bị quá tải sẽ dẫn đến việc các dịch vụ không thể phục vụ người dùng hợp pháp. Thường kẻ tấn công sẽ gửi một lượng lớn các yêu cầu giả mạo hoặc dữ liệu đến hệ thống mục tiêu, làm cho hệ thống bị ảnh hưởng nghiêm trọng và bị tắt nguồn tự động.

**2.1.2 Quy Mô và Nạn Nhân**

Tấn công DoS thường sẽ có quy mô nhỏ hơn so với tấn công DDoS vì chỉ có một nguồn duy nhất thực hiện cuộc tấn công. Tuy nhiên, tấn công DoS vẫn có thể gây ra những hậu quả nghiêm trọng cho hệ thống mục tiêu. Quy mô của một cuộc tấn công DoS phụ thuộc vào khả năng và công cụ mà kẻ tấn công sử dụng.

**2.1.3 Nền tảng tấn công: Application-based attack**

Là lớp thứ 7 trong mô hình OSI, chịu trách nhiệm giao tiếp giữa người dùng và các ứng dụng mạng Lớp ứng dụng là nơi các giao thức và chương trình hoạt động .Có vài giao thức phổ biến như HTTP, DNS, FTP, SMTP,... cho việc cung cấp dịch vụ trực tiếp cho người dùng.

Với DoS thì việc tấn công lớp ứng dụng là một hình thức phổ biến và nguy hiểm. Loại hình thức này nhằm mục đích làm quá tải các dịch vụ cụ thể trên lớp ứng dụng, buộc hệ thống phải xử lý khối lượng lớn yêu cầu và không còn khả năng phục vụ yêu cầu hợp pháp của người dùng.

Các cuộc tấn công vào lớp ứng dụng thường khó phát hiện hơn vì chúng bắt chước các yêu cầu hợp pháp, nhưng với số lượng lớn. Ví dụ, một cuộc tấn công HTTP Flood có thể yêu cầu tải các trang web phức tạp hoặc thực hiện các hành động tốn tài nguyên trên máy chủ web, gây ra quá tải cho máy chủ.

**2.1.4 Tools and Technologies**

Theo xu hướng phát triển hiện nay nên rất đa dạng và có thể thay theo nhiều hình thức mới. Sau đây sẽ là các công cụ và công nghệ được dùng phổ biến để tiến hành DoS:

**2.1.4.1 LOIC**

Là một ứng dụng kiểm tra căng thẳng mạng và tấn công từ chối dịch vụ (DoS) mã nguồn mở được viết bằng C#.

Được phát triển bởi Praetox Technologies và sau đó nó đã được phát hành vào miền công cộng với phiên bản cuối cùng vào ngày 13 tháng 12 năm 2014, hiện nay đang có sẵn trên một số nền tảng mã nguồn mở.

Có khả năng làm ngập máy chủ với các gói TCP, UDP hoặc HTTP nhằm mục đích làm gián đoạn dịch vụ của một máy chủ cụ thể để làm quá tải máy chủ. Giúp người dùng tham gia vào các botnet tình nguyện.

**2.1.4.2 Ping of Death**

Là một loại tấn công vào hệ thống máy tính liên quan đến việc gửi một ping bị biến dạng hoặc độc hại đến một máy tính nhằm cố gắng làm cho hệ thống mục tiêu ngừng hoạt động hoặc giữ cho nó bận rộn bằng cách phản hồi với các phản hồi ICMP Echo.

Một gói tin ping được định dạng chính xác thường có kích thước 56 byte, hoặc 64 byte khi tính đến tiêu đề Giao thức Tin nhắn Điều khiển Internet (ICMP), và 84 byte khi bao gồm tiêu đề Giao thức Internet (IP) IPv4. Tuy nhiên, bất kỳ gói tin IPv4 nào (bao gồm cả ping) có thể có kích thước lên đến 65.535 byte.

**2.1.5. Strategies**

Khai thác từ các điểm yếu của hệ thống để làm ngưng trệ, gián đoạn .Tùy thuộc vào mục tiêu và loại tấn công của DoS, chúng thường xoay quanh việc làm cạn kiệt tài nguyên hệ thống, gây quá tải cho dịch vụ hoặc làm hỏng khả năng phản hồi của hệ thống. Application-based Attack cũng là một trong những chiến thuật cua Dos và sau đây Ví Dụ Khác:

**Tấn Công vào Tài Nguyên Hệ Thống**

Tấn Công vào CPU và Bộ Nhớ.

Tấn Công vào Băng Thông.

**Chiến lược Tấn Công vào Hạ Tầng Mạng**

Tấn Công vào Router và Switch

Tấn Công vào Hệ Thống Cơ Sở Dữ Liệu

**Chiến Lược Tấn Công Phân Phối**

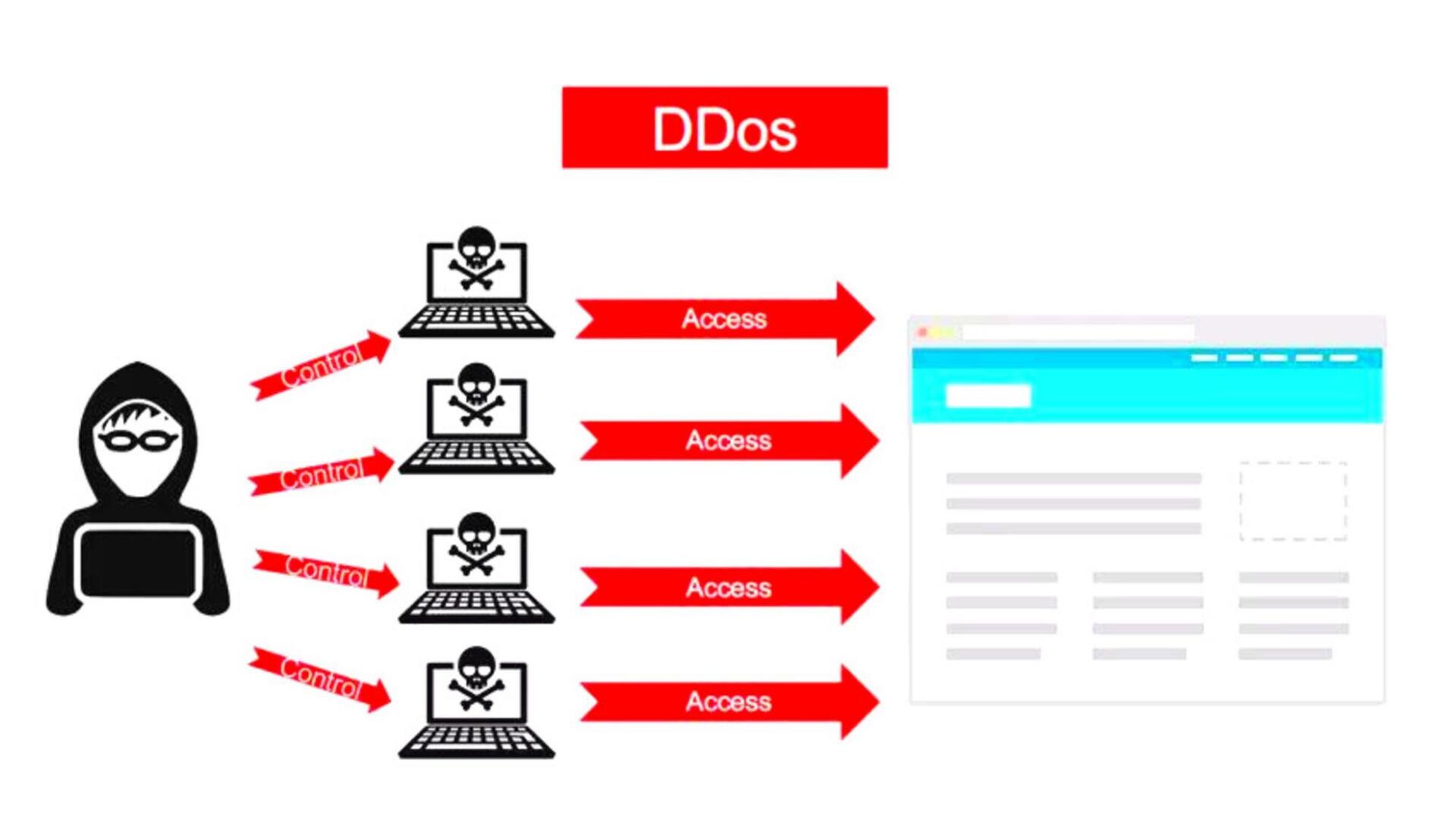
DDoS

# **2.2. DDoS**

**DDoS là gì?**

DDoS viết tắt của cụm từ Distributed Denial of Service, có nghĩa là từ chối dịch vụ phân tán, máy tính của bạn bị tấn công với lưu lượng truy cập từ nhiều hệ thống khác nhau thông qua nhiều nơi khác nhau.

Trọng tâm của việc này là máy tính hoặc server chắc chắn sẽ bị đánh sập hoặc ngừng hoạt động, gián đoạn dịch vụ. Những kẻ tấn công sau khi có được quyền kiểm soát máy tính sẽ lợi dụng điều đó để gửi các dữ liệu xấu, các yêu cầu đến các thiết bị khác thông qua trang web hoặc địa chỉ email.



**2.2.1. Cách Thức Hoạt Động**

Xuất hiện một kẻ tấn công có quyền kiểm soát botnet có thể là các điện thoại, máy tính, hơn nữa là các thiết bị IoT và tấn công vào hệ thống của mục tiêu bằng lượng lớn yêu cầu từ những thiết bị trong botnet. Việc ngăn chặn sẽ cực kỳ khó khăn vì các yêu cầu tới từ những địa chỉ IP khác nhau và khiến cho hệ thống khó phân biệt giữa yêu hợp pháp và yêu cầu tấn công.

**2.2.2. Quy Mô và Nạn Nhân**

Tấn công DDoS Distributed Denial of Service sẽ được chia thành 3 kiểu: Local Scale nhắm vào một máy chủ và hệ thống cụ thể, Medium Scale nhắm vào các tổ chức lớn hơn hoặc các dịch vụ trực tuyến quan trọng, Large Scale nhắm vào các dịch vụ trực tuyến toàn cầu, các nhà cung cấp dịch vụ Internet (ISP), hoặc các cơ sở hạ tầng mạng quan trọng như các trung tâm dữ liệu lớn.

**2.2.3. Nền tảng tấn công: Application-based attack**

Là lớp thứ 7 trong mô hình OSI, chịu trách nhiệm giao tiếp giữa người dùng và các ứng dụng mạng Lớp ứng dụng là nơi các giao thức và chương trình hoạt động .Có vài giao thức phổ biến như HTTP, DNS, FTP, SMTP,... cho việc cung cấp dịch vụ trực tiếp cho người dùng.

Tập trung vào việc làm gián đoạn lớp ứng dụng của một hệ thống bằng cách gửi các yêu cầu giả mạo hoặc yêu cầu phức tạp để làm quá tải tài nguyên ứng dụng. Các cuộc tấn công này bao gồm HTTP Flood, Slowloris, RUDY, và XML Bomb.

**2.2.4. Tools and Technologies**

**2.2.4.1. HOIC**

Là một ứng dụng kiểm tra căng thẳng mạng và DoS mã nguồn mở được thiết kế để tấn công tới 256 URL cùng một lúc.

Nó được thiết kế để thay thế Low Orbit Ion Cannon. Sau đó đã được phát hành vào miền công cộng. Được Prolexic Technologies phát hành vào tháng 2 năm 2012.

Có khả năng tương tự như LOIC và HOIC có thể tấn công đồng thời lên đến 256 miền, làm cho nó trở thành một trong những công cụ linh hoạt nhất cho các hacker đang cố gắng phối hợp các cuộc tấn công DDoS theo nhóm.

**2.2.4.2.RUDY**

Công cụ này lần đầu xuất hiện trên các diễn đàn hacking khoảng năm 2010. Được đặt tên theo một album của ban nhạc death metal người Phần Lan Children of Bodom..

Được biết đến là DDoS chậm và thấp. Mục tiêu là mở một số lượng kết nối tương đối nhỏ đến mục tiêu trong một khoảng thời gian dài và giữ các phiên đó mở càng lâu càng tốt.

Điều này cuối cùng tiêu tốn tất cả các kết nối và tài nguyên có sẵn trên máy chủ, khiến nó không thể truy cập được đối với người dùng hợp pháp.

**2.2.5. Strategies**

Khai thác từ các điểm yếu của hệ thống để làm ngưng trệ, gián đoạn .Tùy thuộc vào mục tiêu và loại tấn công của DoS, chúng thường xoay quanh việc làm cạn kiệt tài nguyên hệ thống, gây quá tải cho dịch vụ hoặc làm hỏng khả năng phản hồi của hệ thống. Application-based Attack cũng là một trong những chiến thuật cua Dos và sau đây Ví Dụ Khác:

**Flood Attacks**

Volume-Based Attacks.

Protocol-Based Attacks.

**Amplification Attacks**

DNS Amplification

NTP Amplification

# **2.3. Sự Khác Nhau và Điểm Giống Nhau Giữa DoS và DDoS**

Đều là các loại tấn công nhằm làm gián đoạn dịch vụ của hệ thống mục tiêu, nhưng chúng có những điểm khác biệt và giống nhau quan trọng.

**2.3.1. Khác Nhau**

**2.3.1.1. Nguồn Tấn Công**

DoS: Được thực hiện từ một nguồn đơn lẻ. Kẻ tấn công sử dụng một máy tính hoặc thiết bị duy nhất để thực hiện cuộc tấn công.

DDoS: Được thực hiện từ nhiều nguồn khác nhau, thường là từ một mạng lưới các thiết bị bị nhiễm malware (botnet).

**2.3.1.2. Quy Mô**

**DoS: Thường có quy mô nhỏ hơn so với DDoS vì chỉ có một nguồn tấn công.**

**DDoS: Thường có quy mô lớn hơn nhiều vì nhiều nguồn tấn công cùng gửi lưu lượng đến mục tiêu.**

**2.3.1.3. Phương Pháp**

DoS: Có thể sử dụng các công cụ và phương pháp đơn giản, như gửi một lượng lớn yêu cầu từ một máy tính để làm quá tải hệ thống.

DDoS: Có thể sử dụng các botnets và các công cụ tấn công tinh vi hơn để phối hợp nhiều thiết bị và nguồn để thực hiện tấn công.

**2.3.2. Giống Nhau**

Cả DoS và DDoS đều nhằm mục đích làm cho dịch vụ hoặc hệ thống mục tiêu trở nên không khả dụng hoặc không thể đáp ứng các yêu cầu hợp lệ.

Cả hai loại tấn công đều làm quá tải tài nguyên của hệ thống mục tiêu. Điều này có thể là băng thông, CPU, bộ nhớ, hoặc các tài nguyên khác cần thiết để duy trì dịch vụ.

Cả DoS và DDoS có thể thực hiện thông qua các loại tấn công khác nhau như flooding, protocol attacks, và application layer attacks.

# **2.4. Đặc điểm của tấn công DoS và DDoS**

**2.4.1. Lợi ích của kẻ tấn công**

Tấn công DoS (Denial of Service) và DDoS (Distributed Denial of Service) tuy đều có cùng một mục đích làm quá tải hệ thống nhưng có hình thức tấn công và quy mô khác nhau. Với những mục đích khác nhau từ việc tấn công từ chối dịch vụ DoS và DDoS, tội phạm tấn công đều có những lợi ích như sau:

**Lợi ích trực tiếp:**

**Làm gián đoạn:** Các cuộc tấn công này đều có mục đích chính là làm quá tải hệ thống của mục tiêu bị tấn công cụ thể như người dùng hoặc server, hệ thống công ty,... khiến dịch vụ trở nên chậm chạp hoặc không thể truy cập được. Điều này gây ra sự gián đoạn lớn cho các thiết bị phản hồi như máy tính cũng như là các doanh nghiệp, tổ chức dẫn đến ảnh hưởng đến hoạt động kinh doanh, quán lý thông tin, dịch vụ, chăm sóc khách hàng cũng như là tổn thất cho nhiều cá nhân sử dụng.

**Cạnh tranh không lành mạnh:** Kẻ tấn công có thể sử dụng các cuộc tấn công này để loại bỏ đối thủ cạnh tranh khỏi thị trường, hoặc gây áp lực để đạt được các mục tiêu khác. Ngoài các công ty và máy chủ bị ảnh hưởng, các nạn nhân của hình thức tấn công này thường bị hư hỏng các thiết bị do “overload” (quá tải) CPU dẫn đến sập nguồn và hư hỏng nặng.

**Che giấu các hoạt động bất hợp pháp khác:** Khác với các cuộc tấn công DoS, các cuộc tấn công DDoS có thể được sử dụng để che đậy các hoạt động bất hợp pháp khác, như tấn công vào các hệ thống khác hoặc đánh cắp dữ liệu do quy mô tấn công và tốc độ tấn công của DDoS nhanh hơn rất nhiều so với DoS, khiến cho việc tấn công DDoS trở nên khó phát hiện và ngăn chặn hơn.

**Lợi ích gián tiếp:**

**Thu thập thông tin:** Qua việc quan sát phản ứng của hệ thống mục tiêu trước các cuộc tấn công và các “thành quả” mà kẻ tấn công có được, kẻ tấn công có thể thu thập thông tin và có tiền đề để tạo ra các cuộc tấn công có quy mô lớn hơn về sau này.

**Kiểm tra khả năng của công cụ tấn công:** Kẻ tấn công có thể sử dụng các cuộc tấn công DDoS để kiểm tra hiệu quả của các công cụ tấn công mà chúng đã phát triển (Botnet…). Qua đó, kẻ tấn công có thể tìm ra các lỗ hổng và lỗi gặp phải trong quá trình phát triển để giúp cho việc tấn công sau này có hiệu quả hơn.

**Tạo tiếng vang:** Các cuộc tấn công DDoS có quy mô lớn thường thu hút sự chú ý của truyền thông và công chúng, giúp kẻ tấn công đạt được mục tiêu tuyên truyền hoặc gây ảnh hưởng và đe dọa rất lớn đặc biệt là các đối thủ cạnh tranh trên thị trường kinh doanh và lao động

**2.4.2. Thiệt hại cho người dùng**

Các cuộc tấn công DoS (Denial of Service) và DDoS (Distributed Denial of Service) gây ra những hậu quả nghiêm trọng cho các nạn nhân, bao gồm các doanh nghiệp, tổ chức và cá nhân. Dưới đây là một số thiệt hại tiêu biểu:

**Thiệt hại về tài chính:**

**Mất doanh thu:** Khi website hoặc hệ thống bị tấn công, khách hàng không thể truy cập, dẫn đến mất doanh thu trực tuyến, gây tổn hại lớn đến các công ty liên quan đến kinh doanh.

**Chi phí khắc phục:** Các doanh nghiệp phải chi trả chi phí để khắc phục hệ thống, thuê chuyên gia bảo mật, và có thể phải thay thế phần cứng bị hư hỏng do hậu quả mà DoS và DDoS gây ra.

**Thiệt hại về uy tín:**

**Mất lòng tin của khách hàng:** Khi dịch vụ bị gián đoạn, khách hàng sẽ mất niềm tin vào doanh nghiệp và có thể chuyển sang sử dụng dịch vụ của đối thủ cạnh tranh.

**Ảnh hưởng đến thương hiệu:** Các cuộc tấn công mạng có thể làm tổn hại đến hình ảnh của doanh nghiệp, khiến khách hàng nghi ngờ về khả năng bảo vệ thông tin của doanh nghiệp.

**Thiệt hại về hoạt động kinh doanh:**

**Cản trở hoạt động:** Các cuộc tấn công DDoS có thể làm gián đoạn nghiêm trọng các hoạt động kinh doanh, gây ra sự hỗn loạn và ảnh hưởng nghiêm trọng đến hiệu quả làm việc của nhân viên. Bên cạnh đó, các hoạt động liên quan đến chăm sóc khách hàng và quản lý thông tin trở nên khó khăn hơn.

**Mất dữ liệu:** Trong một số trường hợp, các cuộc tấn công DDoS có thể dẫn đến việc mất dữ liệu quan trọng của doanh nghiệp và nhiều cá nhân bị ảnh hưởng khác

**Thiệt hại khác:**

**Mất cơ hội kinh doanh:** Các cuộc tấn công DDoS có thể làm mất đi các cơ hội kinh doanh quan trọng, chẳng hạn như các hợp đồng mới hoặc các dự án hợp tác.

**Ảnh hưởng đến danh tiếng cá nhân:** Đối với các cá nhân, việc bị tấn công DDoS có thể gây ra những hậu quả nghiêm trọng về tinh thần và danh tiếng cũng như là các thông tin cá nhân.

**2.4.3. Động lực thực hiện**

Các cuộc tấn công DoS và DDoS, mặc dù gây ra nhiều thiệt hại, nhưng đằng sau đó thường có những động cơ nhất định. Dưới đây là một số động lực phổ biến:

**Vì lợi nhuận:**

**Cạnh tranh không lành mạnh:** Các doanh nghiệp đối thủ có thể thực hiện các cuộc tấn công để làm gián đoạn hoạt động của đối phương, giành lợi thế trên thị trường.

**Tống tiền:** Kẻ tấn công có thể đe dọa sẽ tiếp tục tấn công nếu nạn nhân không trả tiền chuộc.

**Bán các dịch vụ tấn công:** Một số nhóm tội phạm mạng cung cấp dịch vụ tấn công DDoS cho thuê, kiếm lợi từ việc này.

**Vì chính trị:**

**Biểu tình trực tuyến:** Các nhóm hoạt động vì một mục tiêu chính trị nào đó có thể sử dụng các cuộc tấn công để thể hiện sự bất mãn hoặc gây áp lực lên các tổ chức, chính phủ.

**Chiến tranh mạng:** Các quốc gia hoặc tổ chức chính phủ có thể sử dụng các cuộc tấn công DDoS như một công cụ để gây rối loạn hoặc phá hoại cơ sở hạ tầng của đối phương.

**Vì mục đích cá nhân:**

**Trả thù:** Kẻ tấn công có thể thực hiện các cuộc tấn công để trả thù cho một cá nhân hoặc tổ chức nào đó.

**Chứng tỏ khả năng:** Một số hacker thực hiện các cuộc tấn công để chứng tỏ kỹ năng và kiến thức của mình.

**Khác:**

**Thử nghiệm:** Một số hacker và tội phạm trẻ tuổi có thể thực hiện các cuộc tấn công chỉ để thử nghiệm các công cụ và kỹ thuật mà họ đã học được nhằm mục đích thử nghiệm và tạo tiền đề để thực hiện các cuộc tấn công có quy mô lớn hơn.

**Lỗ hổng bảo mật:** Khi phát hiện ra lỗ hổng bảo mật trong hệ thống, kẻ tấn công có thể lợi dụng để thực hiện các cuộc tấn công vì các mục đích cá nhân hoặc mục đích xấu khác.

**Dễ dàng tiếp cận các công cụ tấn công:** Trên mạng có rất nhiều công cụ và hướng dẫn thực hiện các cuộc tấn công DDoS, khiến việc thực hiện chúng trở nên dễ dàng hơn cũng như khiến các hacker và tội phạm muốn thực hiện tấn công mà không vì mục đích nào.

# **2.5. Các loại hình thức tấn công**

Các loại tấn công DoS/DDoS thành 3 nhóm chính:

**2.5.1. IPv4 và IPv6:**

Đây là hai phiên bản giao thức Internet. Các cuộc tấn công có thể nhắm

vào cả hai phiên bản này.

**2.5.2. Layer-4 (Transport layer) Attacks**

Layer-4 Attack (hay còn gọi là tấn công Lớp 4), được gọi là tấn công tầng vận chuyển, là một loại tấn công mạng nhắm vào lớp giao thức truyền tải (Transport Layer) trong mô hình OSI. Lớp này chịu trách nhiệm thiết lập, duy trì và kết thúc các kết nối giữa các thiết bị trên mạng. Các cuộc tấn công Lớp 4 thường tập trung vào việc làm quá tải các kết nối này, khiến cho hệ thống mục tiêu không thể xử lý được các yêu cầu hợp lệ.

**2.5.2.1. Cơ chế hoạt động**

Các cuộc tấn công Lớp 4 thường khai thác các lỗ hổng trong các giao thức truyền tải như TCP và UDP. Kẻ tấn công sẽ gửi một lượng lớn các gói tin giả mạo hoặc các gói tin yêu cầu kết nối quá mức đến máy chủ mục tiêu. Điều này làm cho máy chủ phải tiêu tốn quá nhiều tài nguyên để xử lý các kết nối giả mạo, dẫn đến việc các kết nối hợp lệ bị chậm hoặc bị từ chối.

**2.5.2.2. Các loại tấn công Lớp 4**

**Tấn công SYN flood:** Đây là một trong những loại tấn công Lớp 4 phổ biến nhất. Kẻ tấn công gửi một lượng lớn các gói tin SYN (synchronize) đến máy chủ, làm cho máy chủ phải duy trì một số lượng lớn các kết nối nửa mở. Khi số lượng các kết nối này quá lớn, máy chủ sẽ không thể xử lý được các kết nối hợp lệ khác.

**UDP flood:** Trong cuộc tấn công này, kẻ tấn công gửi một lượng lớn các gói tin UDP (User Datagram Protocol) đến máy chủ. UDP là một giao thức không đảm bảo, vì vậy máy chủ phải xử lý từng gói tin UDP một cách riêng biệt. Điều này làm tiêu tốn rất nhiều tài nguyên của máy chủ.

**2.5.3. Layer 7 (Application layer) Attacks**

Layer-7 Attack (hay còn gọi là tấn công Lớp 7), được gọi là tấn công tầng ứng dụng, là một loại tấn công mạng nhắm vào lớp ứng dụng (Application Layer) trong mô hình OSI. Các cuộc tấn công Lớp 7 thường tập trung vào việc làm quá tải các ứng dụng gần gũi với người dùng nhất như mail, web,... khiến cho chúng không thể đáp ứng được các yêu cầu hợp lệ.

**2.5.3.1. Cơ chế hoạt động**

Các cuộc tấn công Lớp 7 thường khai thác các lỗ hổng trong ứng dụng hoặc các yếu tố không an toàn. Kẻ tấn công sẽ gửi một lượng lớn các yêu cầu không hợp lệ hoặc các yêu cầu quá mức đến ứng dụng mục tiêu. Điều này làm cho ứng dụng phải tiêu tốn quá nhiều tài nguyên để xử lý các yêu cầu giả mạo, dẫn đến việc các yêu cầu hợp lệ bị chậm hoặc nặng nhất là bị từ chối.

**2.5.2.2. Các loại tấn công Lớp 7**

**HTTP Flood:** Gửi một lượng lớn các yêu cầu HTTP đến một website.

**SQL Injection:** Tiêm các đoạn mã SQL vào các trường nhập liệu của ứng dụng web để thực thi các lệnh SQL tùy ý.

**Cross-Site Scripting (XSS):** Tiêm mã độc vào các trang web để đánh cắp thông tin người dùng hoặc thực hiện các hành động độc hại khác.

**Session hijacking:** Cướp đoạt phiên làm việc của người dùng khác để truy cập vào tài khoản của họ.

**DDoS ứng dụng:** Sử dụng nhiều máy tính để thực hiện các cuộc tấn công Lớp 7 đồng thời.

**2.5.4. IPv6 Neighbor Discovery Protocol Attacks**

IPv6 Neighbor Discovery Protocol là giao thức được sử dụng trong mạng IPv6 để các thiết bị tìm thấy nhau.

Các cuộc tấn công nhắm vào giao thức này có thể làm gián đoạn quá trình giao tiếp giữa các thiết bị trong mạng IPv6.

# **2.6. Biện pháp phòng ngừa, ngăn chặn trước DOS và DDOS**

Mục tiêu của phòng ngừa,ngăn chặn là để nhầm đám bảo các chức năng của hệ thống phục vụ , hoạt động đúng mục đích và đối tượng,bảo vệ các dữ liệu

quan trọng. Việc mất dữ liệu. mất kiểm soát đem đến thiệt hại lớn cho người dùng, doanh nghiệp. Theo như \*KasperskyLab thì trong năm 2016, có đến

758 triệu cuộc tấn công mạng (https://www.kaspersky.com/about/press-releases/2016\_kaspersky-labs-threat-review-for-2016) 5 tỷ tỷ đô trong 2020.

Việc phòng thủ trong một hệ thống thông tin là một phần quan trọng và trọng yếu không thể thiếu.

\* KasperskyLab :Nền tảng cung cấp bảo mật mạng và phần mềm chống Virus.

**2.6.1 Tổng quan về sự tấn công DOS,DDOS**

Cuộc tấn công Dos và DDos không tấn công một mình mà tấn công sau hoặc cùng lúc với một hoặc nhiều cuộc tấn công khác. Khi đó DOs, DDOs có môi trường thích hợp để tấn công.Các cuộc tấn công trước hoặc cùng như Botnet Creation, Phishing Attacks, Vulnerability Exploitation (Exploit Attacks), DNS Hijacking or Poisoning, Privilege Escalation Attacks, Man-in-the Middle, Brute Force Attacks, SQL Injection, Service Misconfiguration Attacks, Social Engineering Attacks, DNS Amplification or Reflection Attacks Setup.

Ngoài ra còn nhiều cách tiếp cận và tấn công vào máy chủ (server) nhằm tạo môi trường cho một cuộc tấn công DOS,DDOS thành công. Môi trường hệ thống máy chủ bị suy yếu về an ninh, phòng vệ, gián đoạn quản lí và thao tác sẽ là các điểm yếu chí mạng cho DOS, DDOS Attack tấn công vào dễ dàng và khó khăn cho việc ngăn chặn.

Dưới đây sẽ mô tả các cách phòng thủ trước các cuộc tấn công DOS,DDOS.

**2.6.1 Chiến thuật phòng thủ**

Lĩnh vực phòng thủ ngày càng đa dạng và phát triển mạnh mẽ với các chiến thuật phức tạp để tránh thiệt hại mà tấn công mạng đem lại.

**2.6.1.1 Tăng cường tài nguyên, dung lượng lưu trữ**

Dos,DDOS tấn công vào tài nguyên của server làm cho hệ thống bị thiếu, hết tài nguyên gây chậm trễ, tê liệt hệ thống. Do đó, việc tăng cường tài nguyên, mở rộng dung lượng làm giảm thiểu, chống chịu lại các cuộc tấn công.

Chiến thuật xây dựng hệ thống có tài nguyên và dung lượng vô hạn (Infinite Capacity) hoặc gần với mô hình đấy là chiến thuật hiệu quả nhất, cho dù có bị tấn công thì với dung lượng và tài nguyên vô hạn thì hệ thống không phải chịu ảnh hưởng của cuộc tấn công. Tuy nhiên, việc đạt đến kiến trúc vô hạn cực kỳ đắt đỏ và gần như là không thể.

Tuy nhiên với chiến thuật Cloud-Based (Lưu trữ Đám mây) đem đến các cơ chế giúp tăng cường sự chống chịu và sức chứa dữ liệu. Cơ chế Cloud Based Strategies đem lại là Auto- Scaling,Distributed Infra

**2.6.1.1.1 Cloud infrastructure**

Tuy nhiên với chiến thuật Cloud-Based (Lưu trữ Đám mây) đem đến các cơ chế giúp tăng cường sự chống chịu và sức chứa dữ liệu. Cơ chế Cloud Based Strategies đem lại cho hệ thống máy

**2.6.1.1.1.1 Auto-Scaling**

Nền tảng đám mây tự động mở rộng hoặc thu hồi tài nguyên theo thời gian thực dựa vào lưu lượng tải .

Khi xảy ra cuộc tấn công DOS, DDOS thì đám mây có thể mở rộng tài nguyên hơn để xử lý lưu lượng mà không dẫn đến tình trạng thiếu tài nguyên, cạn kiệt tài nguyên.

**2.6.1.1.1.2 Distributed Infrastructure**

Kiến trúc đám mây thực tế có cơ sở hạ tầng dữ liệu (data center) khắp nơi trên thế giới. Luồng lưu lượng được phân bổ qua nhiều khu vực, phân tán luồng xử lí và ngăn ngừa đảm bảo không có bất kỳ máy chủ đơn lẻ nào bị quá tải.

**2.6.1.1.1.3 Traffic Absorption**

Đám mây có khả năng chứa và xử lý luồng lưu lượng lớn, khi tận dụng nguồn tài nguyên và sức chứa rộng.

Tiếp nhận các luồng dữ liệu quan trọng, ngay cả khi có cuộc tấn công thì hệ thống vẫn có thể xử lí được và không làm ảnh hưởng đến hiệu suất làm việc.

**2.6.1.1.1.4 Load Balancing**

Các luồng dữ liệu được cập nhật liên tục và thông qua các thủ thuật như cache, replication, sharding và đến nhiều máy chủ phụ để đảm bảo khi có máy chủ bị tấn công và tê liệt thì các bản sao dữ liệu vẫn không bị mất và có thể hồi phục lại dữ liệu một cách thuận tiện. Việc này đem lại sự an toàn ngay khi cả có cuộc tấn công xảy ra.

**2.6.1.1.1.5 CDN integration**

Các dữ liệu cache được truyền qua nhiều máy chủ trên thế giới và điều này làm giảm lưu lượng tải cho máy chủ chính. Ngoài ra, hiệu suất và thời gian thực thi được cải thiện bằng việc sẽ cung cấp dữ liệu từ các máy chủ gần nhất và ngay tức thời.

**2.6.1.2 Redundancy**

Nếu ta có một hệ thống máy chủ, thì nó sẽ là một điểm chí mạng khi bị tấn công , về hệ thống sẽ bị tê liệt. Tuy nhiên nếu chúng ta có nhiều máy chủ ví dụ hai máy chủ thì việc một máy chủ bị tê liệt khi đó ta còn máy máy chủ còn lại với 50% hiệu suất để có thể tiếp tục vận hành.

Việc chia hệ thống thành nhiều hệ thống có cùng cơ sở dữ liệu có thể sẽ khá đắt đỏ nhưng là điều cần thiết trong một hệ thống điều hành.

Nhìn với khía cạnh của lưu lượng tải thì ta có thể áp dụng việc đặt giới hạn lưu lượng tải vào hoặc ra khỏi máy chủ bao nhiêu trong một khoảng thời gian và từ đó hạn chế được việc quá tải của hệ thống . Việc đặt giới hạn cũng liên quan một phần đến lọc dữ liệu vào và ra ở mục tiếp theo.

**2.6.1.4 Filtering in/out data**

Trong một số trường hợp ta cần chọn lọc các lưu lượng từ một địa chỉ cục thể nào đó hoặc yêu cầu nào đó từ một địa chỉ IP cụ thể. Khi ta cảm thấy hệ thống chúng ta bị tấn công thì ta bật các bộ lọc này lên để ngăn chận.

Tuy nhiên với cuộc tấn công của DDOS đến từ nhiều điểm khác nhau việc dùng đến bộ lọc để ngăn chặn gần như là vô tác dụng. Với góc độ khác khi ta lọc các dữ liệu đi ra khỏi server của ta và ngăn chặn địa chỉ đó ngay tại nguồn.

ví dụ : ta nhận thấy rằng có một địa chỉ đang liên tục gửi các gói SYN trong việc thực hiện TCP ( bắt tay 3 bước) nhưng địa chỉ được đề cập đến lại khác với địa chỉ gửi và ta ngay lập tức ngăn chặn địa chỉ IP đó ngay tại nguồn

**2.6.1.5 Hardening the system**

Củng cố hệ thống liên quan đến các mặt như củng cố và bảo vệ và sửa chữa các lỗ hổng trong hệ thống, giảm bề mặt tấn công và tăng cường sức chống chịu của hệ thống.

Về mặt dịch vụ và chức năng : khi vận hành một máy chủ hệ thống của chúng ta cần tập trung vào các chức năng cần thiết để vận hành và bảo vệ hệ thống, các phần mềm khác ngoài mục đích chúng ta nên gỡ bỏ và

Về mặt bộ nhớ, tài nguyên : ta nên xóa các bản ghi tạm thời hoặc các bản sao,sau lưu IDs hoặc giải phóng tài nguyên lưu trữ sau khi đã xử lý dữ liệu được gửi đến nhầm tránh xung đột và tối ưu hóa tài nguyên, bộ nhớ.

Vì nếu để các lỗ hổng , các tài nguyên không dùng đến trong hệ thống chúng ta thì đó là một điểm mà sau này có thể bị tấn công vào.

**2.6.1.3 Patching**

Bất kỳ phần mềm nào mà ta sử dụng hãy cập nhật hoặc sử dụng bản cập nhật mới nhất vì hai lý do :

thứ nhất là các lỗ hổng của phiên bản hiện tại họ sẽ cập nhật và sửa chữa trong phiên bản mới nhất.

Thứ hai là ngày càng có nhiều phương thức khác nhau để có thể tấn công vào hệ thống, và nhà cung cấp phần mềm luôn luôn phải hoàn thiện và đuổi theo hoặc đi trước các nguy cơ đấy nên chúng ta muốn bảo vệ hệ thống tốt hơn thì nên hướng hệ thống của chúng ta cập nhật theo họ.

**2.6.1.6 Monitoring**

Điểm quan trọng của việc phòng thủ không chỉ liên quan đến hệ thống và máy chủ, mà còn là việc hiểu và quan sát cả hệ thống khi có những điều bất thường xảy ra hoặc hệ thống , máy chủ đang hoạt động bình thường.

Cần hiểu biết về khi nào là cuộc tấn công DDOS hay là hệ thống đang vận hành thành công và khách hàng tìm đến với chúng ta , hoặc có thể là cả hai trường hợp trên

**2.6.1.6.1 Security Information and Event Management (SIEM)**

SIEM đóng vai trò bảo vệ chống lại các cuộc tấn công DDOS bằng cách cung cấp khả năng giám sát thời gian thực và phát hiện mối nguy hiểm và phản ứng xử lý chúng.

SIEM đem lại khả năng phát hiện, phản ứng khi có tấn công, và kết nối với các nền tảng bảo mật khác trong trường hợp khẩn và cả phòng chống lâu dài.

**2.6.1.6.2 XDR**

**2.6.1.7 SOAR**

Là một framework về an ninh mạng tiên tiến với sự kết hợp của nhiều nền tảng an ninh vào một nền tảng thống nhất để nhằm tăng cường bảo vệ , điều tra và phản ứng lại với các cuộc tấn công mạng với quy và phạm vi lớn hơn.

Điểm mạnh của SOAR nằm ở khả năng tự động hóa khi tấn công các bước như cô lập máy chủ bị ảnh hưởng, chận địa chỉ IP của nguồn tấn công, thu nhập nhật kí của cuộc tấn công, giúp cho tổ đội an ninh mạng có thời gian để xử lý các tác vụ quan trọng hơn.

**2.6.2 Phòng thủ theo phương thức tấn công**

**2.6.2.1 Phòng thủ chống lại cuộc tấn công Layer-4 DDOS**

Khi các cuộc tấn công DDOS Layer 4 được triển khai thì phải dựa vào IP Spoofing nên khi ta chặn được IP Spoofing thì ta sẽ chặn được cuộc tấn công DDOS. Tuy có thể phòng thủ bằng IPSEC bằng việc chứng thực các gói IP, tuy nhiên khi DDOS tấn công với quy mô lớn với bots hoặc là zombies. Các bots và zombies này rất đa dạng và đến từ nhiều nguồn khác nhau , nhiều khu vực khác nhau nên việc phân biệt giữa IP chính thống uy tín và giả gặp trở ngại , khó khăn. Ngoài ra kẻ xấu lợi dụng sự biến thiên của IP để cho các bots sao chép các địa chỉ IP hợp lệ, khiến việc nhận dạng và chặn lưu lượng độc hại trở nên phức tạp và tốn thời gian.

Biện pháp để khắc phục là không nên chỉ chú trọng vào IP và thay vào đó là dùng chiến thuật dựa vào các mẫu hành vi, nguồn, thuộc tính, đích đến, giao thức của các cuộc tấn công khác để lọc ra được các luồng hợp pháp. Khi đó việc kẻ tấn công làm giả IP trở nên vô dụng.

Cổ cố hàng phòng thủ với việc nhiều lớp bảo vệ và bộ lọc , và mỗi bộ lọc ta áp dụng các điều kiện khác nhau để bắt được các hoạt động gây hại.

**2.6.2.2 Phòng thủ chống lại các cuộc tấn công Layer - 7 DDOS**

Cuộc tấn công Layer-7 DDOS hay còn được biết đến như là tấn công lớp phần mềm , ứng dụng DDOS, do việc tấn công ở phần mềm và ứng dụng nên rất khó để truy vết và ta chỉ có thể nhận biết được cuộc tấn công đã thành công khi máy chủ , hệ thống chúng ta bị tổn hại.

Hiện tại có rất nhiều cách để có thể chống lại hình thức tấn công này như WAF, Rate Limiting ,CDN,Caching,CAPTCHAs and Human Verification,Behavioral Traffic Analysis,Loading Balancing, Ip Reputation and Geo Blocking, Application Layer DDOS Protection Services, …

Mấu chốt để chống lại kiểu tấn công này là chúng ta phải kết hợp nhiều chiến thuật phòng thủ với nhau nhiều tầng lớp để tăng sức chịu của hệ thống chống lại các thủ thuật tấn công.

# **2.7 Case study**

**2.7.1 Cuộc tấn công DDOS vào Google Services năm 2023**

Cuộc tấn công DDOS nhằm vào Google là cuộc tấn công “the novel HTTP/2 ‘Rapid Reset’ DDoS attack”, một kiểu tấn công mới dựa trên HTTP/2. Đỉnh điểm là vào cuối tháng 8 chỉ trong 2 phút đã tấn công 398 triệu rps. Tuy nhiên đa số đã được lọc và chặn ở rìa mạng lướt mạng nhờ vào các cơ sở global load balancing của Google và không gây ra tổn hại gì. Cuộc điều tra và phòng vệ được dựa trên kiến trúc proxy reverse.

Dưới đây sẽ là các tìm hiểu về cuộc tấn công kiểu mới và các chiến thuật được sử dụng để phát hiện và ngăn chặn HTTP/2 DDOS Attack.

**2.7.1.1 Tổng quan**

Những năm qua tổ đội “DDoS Response” của Google đã quan sát và nghiên cứu về các cuộc tấn công DDOS, cho thấy sự gia tăng trong quy mô và số lượng các cuộc tấn công DDOS. Trong năm 2024, có hai sự kiện được google thông báo là việc ngăn chặn được cuộc tấn công DDOS lớn nhất vào ngày 1 tháng 6 với đinh điểm là 46 triệu rps(request per second) và cuộc thứ 2 với quy mô lớn hơn 7.5 lần với kỹ thuật tấn công mới là HTTP/2 “Rapid Reset”.

Chúng ta sẽ tìm hiểu về cuộc tấn công thứ 2 với kỹ thuật tấn công mới là HTTP/2 và các kỹ thuật , cách hoạt động và hành động của google khi phát hiện và ngăn chặn cuộc tấn công.

**2.7.1.2 HTTP/2 là gì ?**

Trước tiên, ta tìm hiểu về kỹ thuật HTTP viết tắt của HyperText Transfer Protocol, là một giao thức truyền thông dữ liệu và là nền tảng của World Wide Wed. Các phiên bản của HTTP được xuất bản gồm có HTTP/0.9 năm 1991 , HTTP/1.0 năm 1996, HTTP/1.1 năm 1999 , và HTTP/2 năm 2015.

Điểm khác biệt và năng cấp của HTTP/2 là hiệu năng và giao thức nhị phân với điểm đặc biệt là không thể chỉnh sửa hoặc đọc thủ công. Ngoài ra , HTTP/2 cho phép người dùng dừng hoặc thiết lập lại “message” khi đang thực thi gửi mà không cần phải dừng và thiết lập lại kết nối HTTP. Tính năng cốt lõi của HTTP là đa luồng dữ liệu (stream Multiplexing) cho phép người dùng gửi nhiều luồng “request” mà không cần phải quản lý hết từng kết nối luồng của chúng. Đây là mấu chốt của chiến thuật tấn công HTTP/2 “Rapid Reset”, ta sẽ phân tích rõ hơn ở mục tiếp theo

**2.7.1.2 Cách Hoạt động của HTTP/2 “Rapid Reset” Atttack**

Dựa vào tính năng đa luồng và dừng ,cho phép thiết lập lại “message” trong khi các kết nối HTTP/2 vẫn mở đến máy chủ, hệ thống. Kẻ xấu đã hướng đến việc quá tải tài nguyên hệ thống khi hệ thống phải thiết lập cơ cấu luồng mới.

**2.7.1.3 Làm sao để phát hiện và phòng chống các cuộc tấn công ?**

Để phát hiện và ngăn chặn cuộc tấn công này, Google đã triển khai một loạt các biện pháp bảo mật. Các chiến thuật bao gồm:

* Giám sát lưu lượng mạng: Google sử dụng các công cụ phân tích lưu lượng để phát hiện các mẩu bất thường trong lưu lượng truy cập. Việc theo dõi các chỉ số như số lượng yêu cầu trên mỗi kết nối giúp xác định nhanh chóng các cuộc tấn công DDoS.
* Lọc và chặn lưu lượng: Các cơ sở hạ tầng global load balancing của Google cho phép lọc lưu lượng một cách hiệu quả. Lưu lượng đáng ngờ có thể được chặn ở rìa mạng trước khi nó đến máy chủ chính.
* Sử dụng AI và Machine Learning: Google áp dụng các thuật toán học máy để phát hiện các cuộc tấn công DDoS. Những hệ thống này có khả năng học hỏi từ các mẫu tấn công trước đó và cải thiện khả năng phát hiện theo thời gian.
* Kiến trúc proxy reverse: Sử dụng proxy reverse giúp tách biệt lưu lượng hợp lệ và không hợp lệ, giảm thiểu tác động của các cuộc tấn công

**2.7.1.4 Bài học được rút**

Từ cuộc tấn công DDoS vào Google Services, có một số bài học quan trọng mà các tổ chức khác có thể rút ra:

* Tăng cường bảo mật: Các tổ chức nên đầu tư vào các giải pháp bảo mật mạnh mẽ, bao gồm cả giám sát lưu lượng và lọc thông minh để phát hiện và ngăn chặn các cuộc tấn công DDoS.
* Đào tạo nhân viên: Đội ngũ IT cần được đào tạo về các loại tấn công DDoS và cách ứng phó hiệu quả. Việc hiểu rõ về các chiến thuật tấn công sẽ giúp họ chuẩn bị tốt hơn.
* Thực hiện các bài kiểm tra an ninh thường xuyên: Các tổ chức nên tiến hành kiểm tra an ninh định kỳ để đánh giá khả năng phòng vệ của hệ thống trước các cuộc tấn công tiềm năng.
* Chia sẻ thông tin và hợp tác: Các tổ chức nên hợp tác và chia sẻ thông tin về các mối đe dọa DDoS với nhau để nâng cao khả năng phòng ngừa chung.

**LỜI CẢM ƠN**

Trước tiên, nhóm chúng tôi xin gửi lời cảm ơn chân thành đến giảng viên và các thầy cô đã hướng dẫn và cung cấp những kiến thức quan trọng, giúp chúng tôi hoàn thành bài tiểu luận này. Sự chỉ bảo tận tình của quý thầy cô là nguồn động viên lớn lao trong suốt quá trình học tập và nghiên cứu.

Nhóm chúng tôi cũng xin cảm ơn gia đình, bạn bè đã luôn ủng hộ và chia sẻ, giúp tôi có đủ động lực và thời gian để hoàn thành tốt nhiệm vụ này.

Cuối cùng, xin chân thành cảm ơn tất cả những ai đã góp ý và cung cấp tài liệu, giúp cho tiểu luận được hoàn thiện hơn.

**TÀI LIỆU THAM KHẢO**

How Google Cloud blocked the largest Layer 7 DDoS attack at 46 million rps

<https://cloud.google.com/blog/products/identity-security/how-google-cloud-blocked-largest-layer-7-ddos-attack-at-46-million-rps>

Military, DOST links found in DDoS attacks on media – report

<https://www.rappler.com/technology/qurium-links-dost-military-found-ddos-attacks-altermidya-bulatlat/>

# So sánh sự khác nhau trong cách thức tấn công DoS và DDoS

<https://www.vnetwork.vn/news/so-sanh-su-khac-nhau-dos-va-ddos/>