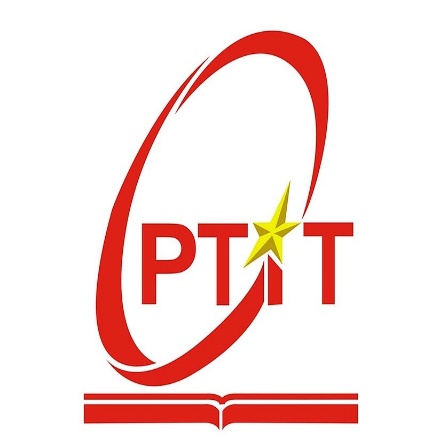
**HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG**

**KHOA AN TOÀN THÔNG TIN**



**ĐỒ ÁN TỐT NGHIỆP**

**ĐỀ TÀI**

**XÂY DỰNG HỆ THỐNG PHÁT HIỆN XÂM NHẬP**

**PHÁT HIỆN TẤN CÔNG DDOS DỰA TRÊN HỌC MÁY**

**Họ và tên: Nguyễn Đức Linh**

**Mã sinh viên: B20DCAT109**

**Nhóm lớp: 01**

**Giảng viên hướng dẫn: Đinh Trường Du**

**HÀ NỘI – 2023**

# **LỜI CẢM ƠN**

**a**

# **NHẬN XÉT, ĐÁNH GIÁ VÀ CHO ĐIỂM**

**(Của Giảng viên hướng dẫn)**

................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................

**Điểm**: ......................... (**Bằng chữ**: .......................................................................................)

**Đồng ý/Không đồng ý** cho sinh viên bảo vệ trước hội đồng chấm đồ án tốt nghiệp?

*Hà Nội, ngày ... tháng ... năm ...*

CÁN BỘ - GIẢNG VIÊN HƯỚNG DẪN

(Ký và ghi rõ họ tên)

# **NHẬN XÉT, ĐÁNH GIÁ VÀ CHO ĐIỂM**

**(của)**

................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................

**Điểm**: ......................... (**Bằng chữ**: .......................................................................................)

**Đồng ý/Không đồng ý** cho sinh viên bảo vệ trước hội đồng chấm đồ án tốt nghiệp?

*Hà Nội, ngày ... tháng ... năm ...*

CÁN BỘ - GIẢNG VIÊN HƯỚNG DẪN

(Ký và ghi rõ họ tên)

# **MỤC LỤC**

# **DANH MỤC TỪ VIẾT TẮT**

# **DANH MỤC HÌNH VẼ**

# **DANH MỤC BẢNG**

# **MỞ ĐẦU**

Ngày nay, Internet mang lại cho chúng ta những lợi ích vô cùng to lớn, và dần trở thành một phần không thể thiếu trong cuộc sống của con người. Tuy nhiên, bên cạnh những lợi ích và sự thuận tiện mà Internet mang lại đó là những hiểm họa, nguy cơ tiềm tàng từ tin tặc, những kẻ luôn lợi dụng những sở hở để tấn công, nhằm chuộc lợi riêng. Trong số các hiểm hoạ, nguy cơ thường trực thì tấn công từ chối dịch vụ DoS/DDoS là một trong các nguy cơ lớn đối với an toàn của hệ thống, mạng và người dùng. Các nạn nhân của DoS/DDoS không ngừng gia tăng và số lượng các mạng Botnet phục vụ DDoS cùng những quy mô của chúng ngày càng được mở rộng và sử dụng kỹ thuật công nghệ cao. Do đó, nhiều các công trình nghiên cứu cũng như các tổ chức đã tìm hiểu và đưa ra những giải pháp nhằm phát hiện sớm nhất tấn công DoS/DDoS hay giảm thiểu thiệt hại do chúng gây ra.

Chính vì vậy, đồ án lựa chọn sử dụng phương pháp học máy để có thể phát hiện sớm tấn công DDoS. Đồ án này tập trung vào nghiên cứu và ứng dụng các kỹ thuật học máy để xây dựng mô hình phát hiện sớm DDoS dựa trên lưu lượng mạng. Đề tài “Nghiên cứu phát hiện tấn công DDoS dựa trên học máy” bao gồm các nội dung chính sau:

Chương 1: Tổng quan về các dạng tấn công mạng phổ biến trên thế giới hiện nay. Từ đó đi sâu vào tìm hiểu về các dạng và cách phòng chống tấn công DoS/DDoS.

Chương 2: Tổng quan về học máy, phân loại các thuật toán học máy và một số thuật toán học máy sẽ được dùng để thử nghiệm trong đồ án. Ngoài ra, chương này cũng sẽ trình bày lý thuyết về cách ứng dụng học máy vào phát hiện tấn công DDoS.

Chương 3: Trong chương này, đồ án sẽ trình bày về cách xây dựng mô hình, tập dữ liệu, tiền xử lý dữ liệu và cách huấn luyện mô hình. Sau khi huấn luyện sẽ sử dụng các thông số tính điểm để đánh giá độ hiệu quả của các thuật toán được sử dụng và chọn ra thuật toán hiệu quả nhất cho mô hình.

# **CHƯƠNG 1: TỔNG QUAN VỀ TẤN CÔNG MẠNG, TẤN CÔNG DOS/DDOS VÀ PHÒNG CHỐNG**

*Trong chương này, đồ án sẽ trình bày các dạng tấn công mạng phổ biến hiện nay trên thế giới. Từ đó sẽ đi sâu vào phân tích các hình thức tấn công, đặc biệt là tấn công từ chối dịch vụ (DoS/DDoS), một trong những phương thức tấn công mạng thường gặp. Đồng thời, chương cũng sẽ đề xuất các biện pháp phòng chống để giảm thiểu rủi ro và bảo vệ hệ thống trước những mối đe dọa này.*

1. **Khái quát về tấn công mạng**
2. **Giới thiệu tấn công xâm nhập**

Trong bối cảnh công nghệ thông tin phát triển mạnh mẽ, đi cùng với các lợi ích to lớn mà internet mang lại là những nguy cơ mất an toàn trên không gian mạng. Bằng nhiều cách khác nhau, các tấn công mạng và xâm nhập đang trở thành những vấn đề đáng lo ngại đối với các tổ chức và cá nhân. Các dạng tấn công mạng ngày càng đa dạng và tinh vi, có thể gây ra thiệt hại lớn về tài chính, thông tin và uy tín. Vì thế cần phải có những phương pháp hiệu quả để phòng chống trước những cuộc tấn công, xâm nhập này. Trước tiên, chúng ta cần tìm hiểu hai khái niệm tấn công mạng và xâm nhập mạng.

Tấn công mạng (hoặc “tấn công không gian mạng”) trong tiếng Anh là Cyber attack là hành động cố ý gây ảnh hường tiêu cực hệ thống máy tính, website, cơ sở dữ liệu, hạ tầng mạng, thiết bị của một cá nhân hoặc tổ chức thông qua mạng internet. Những hành động này không chỉ làm gián đoạn hoạt động của hệ thống mà còn có thể dẫn đến mất mát dữ liệu và thông tin nhạy cảm.

Xâm nhập là một phần của quá trình tấn công, trong đó kẻ tấn công tìm cách truy cập trái phép vào hệ thống hoặc mạng để lấy cắp thông tin, cài đặt phần mềm độc hại hoặc thực hiện các hành động gây hại khác. Việc xâm nhập thường được thực hiện thông qua lỗ hổng bảo mật, kỹ thuật xã hội hoặc khai thác các điểm yếu trong phần mềm.

Các đối tượng thường bị kẻ tấn công nhắm vào có thể là một cá nhân, doanh nghiệp, các tổ chức chính phủ hoặc phi chính phủ, thậm chí là các cơ quan nhà nước. Các đối tượng này thường sở hữu các tài sản thông tin có giá trị và trở thành mục tiêu cho kẻ tấn công khai thác.

1. **Các dạng tấn công xâm nhập**

Có thể chia các dạng tấn công theo mục đích thực hiện thành 4 loại chính như sau:

* Giả mạo (Fabrication) là dạng tấn công thực hiện việc giả mạo thông tin (email, địa chỉ IP...) và thường được sử dụng để đánh lừa người dùng thông thường.
* Chặn bắt (Interception) là dạng tấn công thường liên quan đến việc nghe lén thông tin trên đường truyền và chuyển hướng thông tin để sử dụng trái phép.
* Gây ngắt quãng (Interruption) dạng tấn công làm ngắt, hoặc chậm kênh truyền thông, hoặc làm quá tải hệ thống, ngăn cản việc truy cập dịch vụ của người dùng hợp pháp.
* Sửa đổi (Modification) dạng tấn công thực hiện việc sửa đổi thông tin trên đường truyền hoặc sửa đổi dữ liệu file.

Theo hình thức thực hiện, có thể chia các dạng tấn công thành 2 kiểu chính như sau:

* Tấn công chủ động (Active attack) là sự đột nhập, xâm nhập về mặt vật lý vào hệ thống hoặc mạng. Các tấn công chủ động thực hiện sửa đổi dữ liệu trên đường truyền, sửa đổi dữ liệu trong file, hoặc giành quyền truy cập trái phép vào hệ thống máy tính hoặc hệ thống mạng.
* Tấn công thụ động (Passive attack) là kiểu tấn công thường không gây ra thay đổi trên hệ thống. Các cuộc tấn công thụ động điển hình là nghe lén và giám sát lưu lượng trên đường truyền.

Trên thực tế, tấn công thụ động thường là giai đoạn đầu của một cuộc tấn công chủ động, trong đó kẻ tấn công sử dụng các kỹ thuật tấn công thụ động để thu thập các thông tin về hệ thống mạng. Trên cơ sở các thông tin có được từ giai đoạn tấn công thụ động, kẻ tấn công sẽ lựa chọn kỹ thuật tấn công chủ động có xác suất thành công cao nhất.

1. **Một số dạng tấn công mạng điển hình**

Các dạng tấn công thường gặp là những dạng tấn công điển hình, xảy ra thường xuyên nhằm vào thông tin, hệ thống máy tính, hệ thống mạng và người dùng. Các dạng tấn công thường gặp bao gồm:

* Tấn công vào mật khẩu
* Tấn công bằng mã độc
* Tấn công từ chối dịch vụ và tấn công từ chối dịch vụ phân tán
* Tấn công giả mạo địa chỉ
* Tấn công nghe lén
* Tấn công kiểu người đứng giữa
* Tấn công bằng bom thư và thư rác
* Tấn công sử dụng các kỹ thuật xã hội
* Tấn công pharming
* Tấn công APT

Phần tiếp theo của mục này sẽ chỉ trình bày một số các dạng tấn công mạng điển hình trên và các biện pháp phòng chống tương ứng.

1. *Tấn công vào mật khẩu*

Tấn công vào mật khẩu (Password attack) là dạng tấn công nhằm đánh cắp mật khẩu và thông tin tài khoản của người dùng để lạm dụng. Tên người dùng và mật khẩu không được mã hóa có thể bị đánh cắp trên đường truyền từ máy khách chuyển đến máy chủ. Các thông tin này cũng có thể bị đánh cắp thông qua các dạng tấn công XSS, hoặc lừa đảo, bẫy người dùng cung cấp thông tin. Đây là một trong các dạng tấn công phổ biến nhất do hầu hết các ứng dụng sử dụng cơ chế xác thực người dùng dựa trên tên người dùng, hoặc địa chỉ email và mật khẩu. Nếu kẻ tấn công có tên người dùng và mật khẩu thì có thể đăng nhập vào tài khoản và thực hiện các thao tác như người dùng hợp pháp.

Có thể chia tấn công vào mật khẩu thành 2 dạng:

* Tấn công dựa trên từ điển (Dictionary attack): Dạng tấn công này khai thác vấn đề người dùng có xu hướng chọn mật khẩu là các từ đơn giản cho dễ nhớ. Kẻ tấn công thử các từ có tần suất sử dụng cao làm mật khẩu, nhờ vậy có thể giảm số lần thử và tăng khả năng thành công. Danh sách các từ có tần suất sử dụng cao làm mật khẩu thường được biên soạn sẵn gọi là từ điển được dùng trong dạng tấn công này.
* Tấn công vét cạn (Brute force attack): Tấn công vét cạn sử dụng phương pháp sinh các tổ hợp các ký tự, số và tính toán để tìm mật khẩu một cách tự động. Phương pháp này thường được sử dụng với các mật khẩu đã được mã hóa. Kẻ tấn công sinh tổ hợp ký tự, sau đó mã hóa với cùng thuật toán mà hệ thống sử dụng, tiếp theo so sánh chuỗi mã hóa tạo từ tổ hợp ký tự với chuỗi mật khẩu mã hóa thu thập được. Nếu hai chuỗi mã hóa trùng nhau thì tổ hợp ký tự là mật khẩu đúng.

Để đảm bảo an toàn cho mật khẩu, cần thực hiện kết hợp các biện pháp sau:

* Chọn mật khẩu đủ mạnh: Mật khẩu mạnh cho người dùng thông thường hiện nay cần có độ dài lớn hơn hoặc bằng 8 ký tự, gồm tổ hợp của 4 loại ký tự: chữ cái hoa, chữ cái thường, chữ số và ký tự đặc biệt (thuộc nhóm “?#$\*...”). Mật khẩu cho người quản trị hệ thống cần có độ dài lớn hơn hoặc bằng 10 ký tự, cùng với tổ hợp các loại ký tự như mật khẩu cho người dùng thông thường.
* Định kỳ thay đổi mật khẩu: Thời hạn đổi mật khẩu tùy thuộc vào chính sách an ninh của cơ quan, tổ chức, có thể là 3 tháng hoặc 6 tháng. Với yêu cầu này, hệ thống cần hỗ trợ cơ chế nhắc đổi mật khẩu khi đến hạn cho người dùng.
* Mật khẩu không nên lưu ở dạng rõ: Nên lưu mật khẩu ở dạng đã mã hóa sử dụng hàm băm một chiều.
* Hạn chế trao đổi tên người dùng và mật khẩu trên kênh truyền không được mã hóa.
* Nên hạn chế số lần đăng nhập lỗi, chẳng hạn nếu người dùng cố gắng đăng nhập với thông tin sai 3 lần liên tục sẽ bị khóa tài khoản trong một khoảng thời gian.

1. *Tấn công bằng mã độc*

Tấn công bằng mã độc (Malicious code attack) là dạng tấn công sử dụng các mã độc làm công cụ để tấn công hệ thống nạn nhân. Tấn công bằng mã độc có thể được chia thành 2 loại:

* Khai thác các lỗ hổng về lập trình, lỗ hổng cấu hình hệ thống để chèn và thực hiện mã độc trên hệ thống nạn nhân. Loại tấn công này lại gồm 2 dạng con:

+ Tấn công khai thác lỗi tràn bộ đệm

+ Tấn công khai thác lỗi không kiểm tra đầu vào, gồm tấn công chèn mã SQL (SQL injection) và tấn công sử dụng mã script, kiểu XSS, CSRF.

* Lừa người sử dụng tải, cài đặt và thực hiện các phần mềm độc hại như:

+ Các phần mềm quảng cáo (Adware), gián điệp (Spyware)

+ Các dạng mã độc như virus, zombie/bot hay trojan.

1. Tấn công giả mạo địa chỉ
2. Tấn công nghe lén
3. Tấn công kiểu người đứng giữa
4. Tấn công bằng bom thư và thư rác
5. Tấn công sử dụng các kỹ thuật xã hội
6. Tấn công pharming
7. Tấn công APT
8. **Tổng quan về tấn công DoS/DdoS**
9. **Tấn công DoS**

Tấn công từ chối dịch vụ (Denial of Service - DoS) là dạng tấn công nhằm ngăn chặn người dùng hợp pháp truy cập các tài nguyên mạng bằng cách làm cho các hệ thống máy chủ, trang web bị tê liệt không thể đáp ứng lại các yêu cầu của người dùng.

Có thể nói, đây là một trong các hình thức tấn công đem lại hiệu quả cao cho các hacker cũng như là giải pháp sau cùng nếu như không tìm được cách nào đột nhập vào mục tiêu. DoS đánh vào bản chất tự nhiên của một quá trình truyền thông của client và server, nếu có quá nhiều client truy cập thì server sẽ bị quá tải, buộc lòng phải từ chối các yêu cầu truy cập khác.

Tấn công DoS có thể được chia thành 2 loại như sau:

* Tấn công logic là dạng tấn công khai thác các lỗi phần mềm làm dịch vụ ngừng hoạt động hoặc làm giảm hiệu năng hệ thống.
* Tấn công gây ngập lụt là dạng tấn công mà kẻ tấn công gửi một lượng lớn yêu cầu gây cạn kiệt tài nguyên hệ thống hoặc băng thông đường truyền mạng

Các kỹ thuật tấn công DoS thường gặp trong thực tế bao gồm: SYN Flood, Smurf, Ping of Death, Land Attack, ICMP Flood, HTTP Flood, UDP Flood, ...

* Ping of Death: Các công cụ tấn công Ping of Death gửi nhiều gói tin IP với kích thước lớn đến mục tiêu làm cho các máy này phải mất nhiều thời gian và tài nguyên hệ thống để xử lý. Kết quả là không thể đáp ứng được các yêu cầu kết nối thông thường của những máy tính khác dẫn đến bị từ chối dịch vụ.
* LAND Attack: Những công cụ có chức năng tấn công LAND Attack sẽ gửi các gói tin có địa chỉ IP trùng lặp với các địa chỉ IP đích khiến cho việc xử lý các yêu cầu này có thể dẫn đến tình trạng bị lặp lại (loop) và không thể tiếp nhận thêm các yêu cầu truy cập khác.

Trong phạm vi của đồ án, chỉ trung đề cập đến 2 kỹ thuật tấn công DoS phổ biến nhất là SYN Flood và Smurf.

1. SYN Flood
2. Giới thiệu

Tấn công SYN Flood là kỹ thuật tấn công DoS khai thác điểm yếu trong thủ tục bắt tay 3 bước (3-way handshake) khi hai bên tham gia truyền thông thiết lập kết nối TCP để bắt đầu phiên trao đổi dữ liệu. SYN là bit cờ điều khiển của giao thức TCP dùng để đồng bộ số trình tự gói tin. Thủ tục bắt tay khi một người dùng hợp pháp thiết lập một kết nối TCP đến máy chủ, như minh họa bên dưới

// Hình

(1) Người dùng thông qua máy khách gửi yêu cầu mở kết nối (SYN hay SYN-REQ) đến máy chủ

(2) Máy chủ nhận được yêu cầu kết nối, lưu vào Bảng kết nối (gọi là Backlog) và gửi lại xác nhận kết nối SYN-ACK cho máy khách

(3) Khi nhận được SYN-ACK từ máy chủ, máy khách gửi lại xác nhận kết nối ACK đến máy chủ. Khi máy chủ nhận được xác nhận kết nối ACK từ máy khách, nó xác nhận kết nối mở thành công, máy chủ và máy khách bắt đầu phiên truyền thông TCP. Bản ghi mở kết nối được xóa khỏi Bảng kết nối.

1. Kịch bản tấn công

Kịch bản tấn công SYN Flood, như minh họa trên gồm các bước sau:

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

(2) Nhận được yêu cầu mở kết nối, máy nạn nhân lưu yêu cầu kết nối vào Bảng kết nối trong bộ nhớ

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

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

(5) Máy nạn nhân chỉ có thể xóa một yêu cầu mở kết nối chưa được xác nhận khi nó hết hạn (timed-out).

Do kẻ tấn công sử dụng địa chỉ giả mạo hoặc địa chỉ không có thực làm địa chỉ nguồn (Source IP) trong gói tin IP của yêu cầu mở kết nối, nên xác nhận kết nối SYN-ACK gửi từ máy nạn nhân không thể đến đích. Đồng thời, kẻ tấn công cố tình tạo một lượng rất lớn yêu cầu mở kết nối dở dang để chúng điền đầy Bảng kết nối. Hậu quả là máy nạn nhân không thể chấp nhận yêu cầu mở kết nối của những người dùng khác. Tấn công SYN Flood làm cạn kiệt tài nguyên bộ nhớ Bảng kết nối của máy nạn nhân, đồng thời có thể làm máy nạn nhân ngừng hoạt động và gây nghẽn đường truyền mạng.

1. Phòng chống

Nhiều biện pháp phòng chống tấn công SYN Flood được đề xuất, nhưng cho đến hiện nay chưa có giải pháp nào có khả năng ngăn chặn triệt để dạng tấn công này. Do vậy, để phòng chống tấn công SYN Flood hiệu quả, cần kết hợp các biện pháp sau:

* Sử dụng kỹ thuật lọc địa chỉ giả mạo (Spoofed IP Filtering): Kỹ thuật này đòi hỏi chỉnh sửa giao thức TCP/IP nhằm không cho phép kẻ tấn công giả mạo địa chỉ.
* Tăng kích thước Bảng kết nối: Tăng kích thước Bảng kết nối cho phép tăng khả năng chấp nhận các yêu cầu mở kết nối.
* Giảm thời gian chờ (SYN-RECEIVED Timer): Các yêu cầu mở kết nối chưa được xác nhận sẽ bị xóa sớm hơn khi thời gian chờ ngắn hơn
* Sử dụng SYN cache: SYN cache thay mặt máy chủ tiếp nhận yêu cầu mở kết nối và yêu cầu này chỉ được cấp phát không gian nhớ đầy đủ khi nó được xác nhận
* Sử dụng tường lửa và Proxy: Tường lửa và proxy có khả năng nhận dạng các địa chỉ IP nguồn là địa chỉ không có thực, đồng thời chúng có khả năng tiếp nhận yêu cầu mở kết nối, chờ đến khi có xác nhận mới chuyển cho máy chủ đích.

1. Smurf
2. Giới thiệu

Tấn công Smurf là dạng tấn công DoS sử dụng giao thức ICMP và kiểu phát quảng bá có định hướng để gây ngập lụt đường truyền mạng của máy nạn nhân. Trên mỗi phân vùng mạng IP thường có 1 địa chỉ quảng bá, theo đó khi có một gói tin gửi tới địa chỉ này, nó sẽ được bộ định tuyến của mạng chuyển đến tất cả các máy trong mạng đó.

1. Kịch bản tấn công

Hình dưới đây minh họa mô hình tấn công Smurf, với kịch bản gồm các bước như sau:

//Hình

(1) Kẻ tấn công gửi một lượng lớn gói tin chứa yêu cầu ICMP với địa chỉ IP nguồn là địa chỉ của máy nạn nhân (From: 9.9.9.9) đến một địa chỉ quảng bá của một mạng (To: 1.1.1.255)

(2) Bộ định tuyến của mạng nhận được yêu cầu ICMP gửi đến địa chỉ quảng bá sẽ tự động chuyển yêu cầu này đến tất cả các máy trong mạng (To: 1.1.1.\*)

(3) Các máy trong mạng nhận được yêu cầu ICMP sẽ gửi trả lời đến máy có địa chỉ IP là địa chỉ nguồn trong yêu cầu ICMP (To: 9.9.9.9). Nếu số lượng máy trong mạng rất lớn thì máy nạn nhân sẽ bị ngập lụt đường truyền hoặc ngừng hoạt động.

1. Phòng chống

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

* Cấu hình các máy trong mạng và router không trả lời các yêu cầu ICMP hoặc các yêu cầu phát quảng bá.
* Cấu hình các router không chuyển tiếp yêu cầu ICMP gửi đến các địa chỉ quảng bá của mạng.
* Sử dụng tường lửa để lọc các gói tin với địa chỉ giả mạo địa chỉ trong mạng.
* Việc cấu hình các bộ định tuyến không chuyển tiếp yêu cầu ICMP hoặc các máy trong mạng không trả lời các yêu cầu ICMP có thể gây khó khăn cho các ứng dụng dựa trên phát quảng bá và giao thức ICMP, như ứng dụng giám sát trạng thái hoạt động của các máy trong mạng dựa trên giao thức ICMP.

1. **Tấn công DDoS**

Tấn công từ chối dịch vụ phân tán (Distributed Denial of Service - DDoS) là một loại tấn công DoS đặc biệt, liên quan đến việc gây ngập lụt các máy nạn nhân với một lượng rất lớn các yêu cầu kết nối giả mạo. Điểm khác biệt chính giữa DDoS và DoS là phạm vi tấn công: trong khi số lượng máy tham gia tấn công DoS thường tương đối nhỏ, chỉ gồm một số ít máy tại một hoặc một số ít địa điểm, thì số lượng máy tham gia tấn công DDoS thường rất lớn, có thể lên đến hàng ngàn hoặc hàng trăm ngàn máy và đến từ rất nhiều vị trí địa lý khác nhau, phân tán trên toàn cầu. Bởi vì DDoS sử dụng các hệ thống mạng máy tính “ma” gọi là botnet và mỗi máy trạm trong hệ thống này gọi là một bot hay zombie đã được các hacker cài đặt trojan có thể điều khiển từ xa. Do vậy, việc phòng chống tấn công DDoS gặp nhiều khó khăn hơn so với việc phòng chống tấn công DoS.

Có thể chia tấn công DDoS thành 2 dạng chính theo mô hình kiến trúc:

* Tấn công DDoS trực tiếp (Direct DDoS): Trong tấn công DDoS trực tiếp, các yêu cầu tấn công được các máy tấn công gửi trực tiếp đến hệ thống nạn nhân
* Tấn công DDoS gián tiếp/phản xạ (Indirect/Reflective DDoS): Trong tấn công DDoS gián tiếp, các yêu cầu tấn công được gửi đến các máy phản xạ (Reflector) và sau đó gián tiếp chuyển đến hệ thống nạn nhân.

Thông thường DDoS gồm có 3 thành phần:

* Master hay Handler: Chương trình dùng để điều khiển.
* Slave hay zombie, bot là các máy tính bị cài đặt hay lây nhiễm các chương trình nguy hiểm và bị điều khiển bởi các master/ handler.
* Victim: Những mục tiêu bị tấn công từ chối dịch vụ.

1. Tấn công DDoS trực tiếp

Hình dưới đây minh họa kiến trúc điển hình của dạng tấn công DDoS trực tiếp. Theo đó, tấn công DDoS trực tiếp được thực hiện theo nhiều giai đoạn với kịch bản như sau:

//Hình

(1) Kẻ tấn công (Attacker) chiếm quyền điều khiển hàng ngàn, thậm chí hàng chục ngàn máy tính hoặc thiết bị tính toán (gọi chung là máy tính) có kết nối Internet, sau đó bí mật cài đặt các agent tự động lên các máy này. Các agent tự động cho phép kẻ tấn công điều khiển các máy này từ xa. Các máy tính được cài đặt agent tự động và bị điều khiển từ xa được gọi là các máy tính ma.

(2) Các máy tính ma (gọi chung là bot) hình thành mạng máy tính ma, được gọi là botnet hay zombie network (gọi chung là botnet). Các botnet không bị giới hạn bởi chủng loại thiết bị và topo mạng vật lý.

(3) Kẻ tấn công có thể giao tiếp với các bot thông qua một mạng lưới các máy trung gian (gọi là Handler) gồm nhiều tầng. Phương thức giao tiếp có thể là các giao thức truyền thông, như IRC (Internet Relay Chat), P2P (Peer to Peer), HTTP, ...

(4) Tiếp theo, kẻ tấn công ra lệnh cho các bot trong botnet mà mình quản lý đồng loạt tạo các yêu cầu giả mạo gửi đến các hệ thống nạn nhân (Victim) tạo thành một cuộc tấn công DDoS.

(5) Lượng yêu cầu giả mạo có thể rất lớn, đến từ rất nhiều máy trong botnet với vị trí địa lý khác nhau phân tán trên toàn cầu nên việc đối phó và lần vết để tìm ra kẻ tấn công thực sự là rất khó khăn.

1. Tấn công DDoS gián tiếp

Hình dưới đây minh họa kiến trúc tấn công DDoS gián tiếp, hay phản xạ. Theo đó, tấn công DDoS gián tiếp cũng được thực hiện theo nhiều giai đoạn theo kịch bản như sau:

//Hình

(1) Kẻ tấn công chiếm quyền điều khiển của một lượng lớn máy tính hoặc thiết bị tính toán trên mạng Internet, sau đó cài đặt agent tự động và biến chúng thành các bot, hay zombie (gọi là slave). Các bot hình thành nên mạng botnet.

(2) Kẻ tấn công giao tiếp với các bot thông qua một mạng lưới các máy trung gian (Masters) gồm nhiều tầng sử dụng các giao thức truyền thông như IRC (Internet Relay Chat), P2P (Peer to Peer), HTTP, ...

(3) Theo lệnh của kẻ tấn công, các Bot/Slave trong botnet gửi một lượng lớn yêu cầu (Request) giả mạo với địa chỉ nguồn là địa chỉ hệ thống nạn nhân đến một số lớn các máy khác (Reflectors – máy phản xạ) trên mạng Internet.

(4) Các Reflector gửi các phản hồi (Reply) đến hệ thống nạn nhân do địa chỉ của máy nạn nhân được đặt vào địa chỉ nguồn của yêu cầu giả mạo.

(5) Khi các yêu cầu giả mạo gửi đến các Reflector có số lượng rất lớn, số lượng phản hồi cũng sẽ rất lớn gây ngập lụt đường truyền mạng hoặc làm cạn kiệt tài nguyên của máy nạn nhân, dẫn đến ngắt quãng hoặc ngừng dịch vụ cung cấp cho người dùng. Các Reflector bị lợi dụng để tham gia tấn công thường là các hệ thống máy chủ có công suất và băng thông đường truyền lớn trên Internet và không chịu sự điều khiển của kẻ tấn công.

1. **Các biện pháp phòng chống tấn công DoS/DDoS**

Có nhiều cách thức để nhận biết và phòng chống bị tấn công từ chối dịch vụ khác nhau. Nhìn chung, để phòng chống tấn công hiệu quả cần kết hợp nhiều biện pháp và sự phối hợp của nhiều bên do tấn công DDoS có tính phân tán cao và hệ thống mạng máy tính ma được hình thành và điều khiển theo nhiều tầng, nhiều lớp. Trước tiên chúng ta cần vá những lổ hỗng bảo mật của các dịch vụ hay ứng dụng đang chạy trên máy chủ để tránh bị hacker lợi dụng tấn công từ chối dịch vụ như RPC Locator service. Sau đây là một số giải pháp cần được quan tâm:

* Network-ingress filtering: Tất cả các hệ thống hay thiết bị cung cấp những kết nối và truy cập mạng cần thực hiện cơ chế lọc Network-infgress filtering nhằm loại bỏ các luồng dữ liệu xuất phát từ các địa chỉ giả mạo, có nguồn gốc không rõ ràng. Điều này không ngăn ngừa được các cuộc tấn công nhưng có thể giúp chặn đứng chúng cũng như có thể truy tìm khi có những hành động trái phép diễn ra. Các thiết bị dạng này như Cisco IPS Source IP Reputation Filtering, Black Hole Filtering, ...
* Rate-limiting network system: Nhiều bộ định tuyến hiện nay có khả năng hạn chế và kiểm soát băng thông trên những giao thức khác nhau, kỹ thuật này còn được gọi là traffic shapping.
* Instruction Detect System: Triển khai các hệ thống dò tìm xâm phạm trái phép để phát hiện kịp thời các luồng truyền thông nguy hiểm, những cuộc tấn công hay các virus/ worm lan truyền trên mạng. Một trong các ứng dụng IDS nguồn mở được sử dụng phổ biến như Snort ([www.snort.org](http://www.snort.org)).
* Sử dụng công cụ Host-auditing: Một số chương trình có khả năng quét các tập tin trên hệ thống để tìm ra các công cụ tấn công DDoS hay các chương trình botnet nguy hiểm.
* Sử dụng công cụ Network-auditing: Chạy các chương trình quét mạng để phát hiện các agent (các thành viên của mạng botnet) và loại bỏ chúng ra khỏi các hệ thống máy tính hoặc các thiết bị tính toán có kết nối Internet của người dùng
* Sử dụng các chương trình dò tìm công cụ DoS: Thường xuyên quét tìm các công cụ DoS trên hệ thống với những chương trình thích hợp như Find\_ddos, SARA, Zombi Zapper để phát hiện và xử lý kịp thời các mầm mống gây nên sự cố từ chối dịch vụ.
* Tắt các dịch vụ không cần thiết: Đóng các cổng hay tắt những dịch vụ không cần thiết hay hạn chế sự dụng những chức năng như get, strcpy, ...
* Cấu hình firewall để chặn tất cả các tín hiệu ICMP từ bên ngoài. Sử dụng các hệ thống lọc đặt trên các bộ định tuyến, tường lửa của các nhà cung cấp dịch vụ Internet (ISP) để lọc các yêu cầu điều khiển (C&C – Command and Control) gửi từ kẻ tấn công đến các bot
* Thường xuyên cập nhật hệ thống: Cập nhật các bản vá lỗi mới nhất cho hệ thống và ứng dụng liên quan.
* Sử dụng các hệ thống bảo vệ DDoS chuyên dụng như IntelliGuard DDoS Protection System (DPS) hay các chương trình phòng chống DDoS như Hình 10.4

1. **Kết luận chương**

Chương này đã trình bày khái quát về tấn công mạng và dạng tấn công nguy hiểm hàng đầu hiện nay là DoS và DDoS cùng với các cách phòng chống hiệu quả.

Cụ thể chương đã đề cập các vấn đề sau:

* Trình bày khái niệm, phân loại tấn công, xâm nhập mạng.
* Các dạng tấn công mạng điển hình.
* Giới thiệu về tấn công DoS và 2 kỹ thuật tấn công DoS phổ biến là SYN Flood và Smurf.
* Giới thiệu về tấn công DDoS và 2 dạng kiến trúc tấn công DDoS là tấn công trực tiếp và gián tiếp.
* Trình bày các biện pháp phòng chống tấn công.

1. **A**

# **CHƯƠNG 2: TỔNG QUAN VỀ HỆ THỐNG PHÁT HIỆN XÂM NHẬP**

*Trong chương này, đồ án sẽ trình bày các dạng tấn công mạng phổ biến hiện nay trên thế giới. Từ đó sẽ đi sâu vào phân tích các hình thức tấn công, đặc biệt là tấn công từ chối dịch vụ (DoS/DDoS), một trong những phương thức tấn công mạng thường gặp. Đồng thời, chương cũng sẽ đề xuất các biện pháp phòng chống để giảm thiểu rủi ro và bảo vệ hệ thống trước những mối đe dọa này*

1. **Tổng quan về hệ thống phát hiện xâm nhập**

// Kỹ thuật giám sát ATM + CS ATTT

Hệ thống phát hiện xâm nhập (Intrusion Detection System - IDS) là một hệ thống giám sát lưu thông mạng, các hoạt động khả nghi và cảnh báo cho hệ thống, nhà quản trị.

Ngoài ra IDS cũng đảm nhận việc phản ứng lại với các lưu thông bất thường hay có hại bằng cách thực hiện các hành động đã được thiết lập trước như khóa người dùng hay địa chỉ IP nguồn đó không cho truy cập hệ thống mạng, ...

IDS cũng có thể phân biệt giữa những tấn công từ bên trong hay tấn công từ bên ngoài. IDS phát hiện tấn công dựa trên các dấu hiệu đặc biệt về các nguy cơ đã biết (giống như cách các phần mềm diệt virus dựa vào các dấu hiệu đặc biệt để phát hiện và diệt virus) hay dựa trên so sánh lưu thông mạng hiện tại với baseline (thông số đo đạc chuẩn của hệ thống) để tìm ra các dấu hiệu khác thường

<https://thuvienso.dau.edu.vn:88/bitstream/DHKTDN/2234/1/H%E1%BB%87%20th%E1%BB%91ng%20ph%C3%A1t%20hi%E1%BB%87n%20x%C3%A2m%20nh%E1%BA%ADp%20m%E1%BA%A1ng.pdf>

1. **Đặc điểm hệ thống phát hiện xâm nhập**
2. **Ứng dụng hệ thống phát hiện xâm nhập**
3. **Kết luận chương**

C2: Tổng quan về hệ thống IDS

* Lý thuyết
* Phân loại
* Cách hoạt động
* Ưu, nhược điểm

# **CHƯƠNG 3: PHÁT HIỆN TẤN CÔNG DOS/DDOS DỰA TRÊN HỌC MÁY**

*Ở chương 2, đồ án sẽ trình bày tổng quan về học máy, phân loại các thuật toán học máy và một số thuật toán học máy sẽ được dùng để thử nghiệm trong đồ án. Ngoài ra, chương này cũng sẽ trình bày lý thuyết về cách ứng dụng học máy vào phát hiện tấn công DDoS.*

1. **Tổng quan về học máy**
2. **Xây dựng mô hình phát hiện tấn công DoS/DdoS dựa trên học máy**

**CÁC ĐẶC TRƯNG CỦA KDD99**

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Feature** | **Meaning** | **Type** |
| 1 | duration | length (number of seconds) of the connection | continuous |
| 2 | **protocol\_type** | type of the protocol (tcp, udp, icmp) | discrete |
| 3 | service | network service on the destination (http, telnet, ...) | discrete |
| 4 | **flag** | normal or error status of the connection | discrete |
| 5 | **src\_bytes** | number of data bytes from source to destination | continuous |
| 6 | **dst\_bytes** | number of data bytes from destination to source | continuous |
| 7 | land | 1 if connection is from/to the same host/port; 0 otherwise | discrete |
| 8 | wrong\_fragment | number of “wrong” fragments | continuous |
| 9 | urgent | number of urgent packets | continuous |
| **Basic features of individual TCP connections** | | | |
| 10 | **hot** | number of “hot” indicators | continuous |
| 11 | **num\_failed\_logins** | number of failed login attempts | continuous |
| 12 | **logged\_in** | 1 if successfully logged in; 0 otherwise | discrete |
| 13 | **num\_compromised** | number of “compromised” conditions | continuous |
| 14 | **root\_shell** | 1 if root shell is obtained; 0 otherwise | discrete |
| 15 | **su\_attempted** | 1 if “su root” command attempted; 0 otherwise | discrete |
| 16 | **num\_root** | number of “root” accesses | continuous |
| 17 | **num\_file\_creations** | number of file creation operations | continuous |
| 18 | **num\_shells** | number of shell prompts | continuous |
| 19 | **num\_access\_files** | number of operations on access control files | continuous |
| 20 | **num\_outbound\_cmds** | number of outbound commands in an ftp session | continuous |
| 21 | **is\_host\_login** | 1 if the login belongs to the “hot” list; 0 otherwise | discrete |
| 22 | **is\_guest\_login** | 1 if the login is a “guest” login; 0 otherwise | discrete |
| **Content features within a connection suggested by domain knowledge** | | | |
| 23 | **count** | number of connections to the same host as the current connection in the past two seconds | continuous |
| *\** | *Note: The following features refer to these same-host connections.* | | |
| 24 | **srv\_count** | number of connections to the same service as the current connection in the past two seconds | continuous |
| 25 | serror\_rate | % of connections that have SYN errors | continuous |
| 26 | rerror\_rate | % of connections that have REJ errors | continuous |
| 27 | **same\_srv\_rate** | % of connections to the same service | continuous |
| 28 | **diff\_srv\_rate** | % of connections to different services | continuous |
| *\** | *Note: The following features refer to these same-service connections* | | |
| 29 | srv\_serror\_rate | % of connections that have SYN errors | continuous |
| 30 | srv\_rerror\_rate | % of connections that have REJ errors | continuous |
| 31 | srv\_diff\_host\_rate | % of connections to different hosts | continuous |
| **Traffic features computed using a two-second time window** | | | |
| 32 | dst\_host\_count |  |  |
| 33 | dst\_host\_srv\_count |  |  |
| 34 | dst\_host\_same\_srv\_rate |  |  |
| 35 | dst\_host\_diff\_srv\_rate |  |  |
| 36 | dst\_host\_same\_src\_port\_rate |  |  |
| 37 | dst\_host\_srv\_diff\_host\_rate |  |  |
| 38 | **dst\_host\_serror\_rate** |  |  |
| 39 | **dst\_host\_srv\_serror\_rate** |  |  |
| 40 | dst\_host\_rerror\_rate |  |  |
| 41 | dst\_host\_srv\_rerror\_rate |  |  |
| 42 |  |  |  |
| 43 |  |  |  |

"duration",

"protocol\_type",

"service",

"flag",

"src\_bytes",

"dst\_bytes",

"land",

"wrong\_fragment",

"urgent",

"hot",

"num\_failed\_logins",

"logged\_in",

"num\_compromised",

"root\_shell",

"su\_attempted",

"num\_root",

"num\_file\_creations",

"num\_shells",

"num\_access\_files",

"num\_outbound\_cmds",

"is\_host\_login",

"is\_guest\_login",

"count",

"srv\_count",

"serror\_rate",

"srv\_serror\_rate",

"rerror\_rate",

"srv\_rerror\_rate",

"same\_srv\_rate",

"diff\_srv\_rate",

"srv\_diff\_host\_rate",

"dst\_host\_count",

"dst\_host\_srv\_count",

"dst\_host\_same\_srv\_rate",

"dst\_host\_diff\_srv\_rate",

"dst\_host\_same\_src\_port\_rate",

"dst\_host\_srv\_diff\_host\_rate",

"dst\_host\_serror\_rate",

"dst\_host\_srv\_serror\_rate",

"dst\_host\_rerror\_rate",

"dst\_host\_srv\_rerror\_rate",

1. **Kết luận chương**

C3: Phát hiện tấn công DdoS dựa trên học máy

* Tổng quan về học máy

+/ Lý thuyết

+/ Một số kỹ thuật học máy

* Xây dựng mô hình học máy phát hiện ddos

+/ Tổng quan mô hình

+/ Các giai đoạn xử lý

# **CHƯƠNG 4: THỬ NGHIỆM VÀ KẾT QUẢ**

*Ở chương 3, đồ án sẽ trình bày về cách xây dựng mô hình, tập dữ liệu, tiền xử lý dữ liệu và cách huấn luyện mô hình. Sau khi huấn luyện sẽ sử dụng các thông số tính điểm để đánh giá độ hiệu quả của các thuật toán được sử dụng và chọn ra thuật toán hiệu quả nhất cho mô hình.*

1. **Xây dựng kịch bản**
2. **Huấn luyện và thử nghiệm mô hình**
3. **Thu thập và xử lý gói tin**
4. **Giả lập cuộc tấn công DoS/DdoS**
5. **Kết luận chương**

C4: Kiểm thử và kết quả

* Xây dựng kịch bản
* Huấn luyện và kiểm thử mô hình

+/ Mô tả dataset

+/ Các giai đoạn tiền xử lý

* Tiền xử lý
* Tích chọn đặc trưng quan trọng

+/ Huấn luyện và thử nghiệm 1 vài mô hình

* Decision tree
* Naive bayes
* Random forest
* Thu thập và xử lý gói tin từ cuộc tấn công

+/ Tool KDD99 extractor

+/

* Giả lập cuộc tấn công DdoS

+/ Mô tả các bước thực hiện

* Demo
* Kết luận

# **KẾT LUẬN**

# **DANH MỤC TÀI LIỆU THAM KHẢO**

# **PHỤ LỤC**