BỘ GIÁO DỤC VÀ ĐÀO TẠO

TRƯỜNG ĐẠI HỌC CÔNG NGHỆ TP. HCM

BÁO CÁO MÔN HỌC BẢO MẬT THÔNG TIN

Nghiên cứu một phương pháp tấn công mạng và công cụ hỗ trợ phương pháp tấn công đó

Tấn công DOS (Denial of Service)

Ngành: **AN TOÀN THÔNG TIN**

Giảng viên hướng dẫn :

Lớp : **21DATA1**

Sinh viên thực hiện : **Nguyễn Phạm Tuyên 2187701032**

Trần Nhật Vũ 2187701120

Hoàng Kim Vũ 2187701279

TP. Hồ Chí Minh, tháng 07 năm 2023

Lời Cảm Ơn

Mục Lục

Chương 1: Tổng Quát đề tài nghiên cứu

1.1 Tổng quan về đề tài nghiên cứu

Đồ án này, sẽ giới thiệu cho chúng ta biết về cuộc tấn công DOS mạng phổ biến hiện nay. Ngoài ra giúp chúng ta hiểu rõ các phương thức tấn công, phát hiện các xu hướng mới và phát triển các biện pháp bảo mật hiệu quả để bảo vệ hệ thống mạng khỏi tác động của tấn công này.

1.2 Nhiệm vụ về đề tài nghiên cứu

- Nghiên cứu và phân tích các phương pháp tấn công DOS phổ biến hiện nay.
- Các giải pháp và thuật toán để phát hiện sớm các hành vi tấn công DOS.
- Đo lường và đánh giá hiệu suất của các biện pháp phòng ngừa và ứng phó với tấn công DOS.
- Nắm bắt các xu hướng kỹ thuật tấn công mới để từ đó đưa ra các biện pháp phòng ngừa và ứng phó.

1.3 Cấu trúc đề tài nghiên cứu

Đề tài nghiên cứu đồ án gồm có 3 chương:

- Chương 1: Tổng quan đề tài nghiên cứu

• Phần này giới thiệu tổng quan, nhiệm vụ của đề tài nghiên cứu và giúp chúng ta hiểu nội dung cơ bản của đề tài nghiên cứu này

- Chương 2: Lý Thuyết đề tài nghiên cứu

• Phần này giới thiệu cụ thể về khái niệm tấn công DOS, hình thức và cách thức hoạt động của cuộc tấn công DOS để từ đó chúng ta đưa ra cách phòng tránh để ứng phó kịp thời.

- Chương 3: Phân tích công cụ được dùng để tấn công DOS

- Phần này sẽ cho chúng ta thấy được công cụ tấn cồn và mô hình tấn công của DOS.

- Chương 4: Kết Luận

- Phần này sẽ đúc ra, kết ra nghiên cứu đề tài này.

Chương 2: Lý Thuyết

2.1 Khái niệm về phương pháp tấn công DOS (Denial of Service)

- Đây là một trong những phương pháp tấn công cố gắng làm cho dịch vụ hoặc hệ thống của máy chủ trở nên không khả dụng cho người dùng hợp lệ. DOS làm cho tài nguyên quan trọng của một hệ thống bị quá tải, gây ra sự cố hoặc hủy hoại chúng.

- Kẻ tấn công sẽ tuồn các traffic hoặc gửi thông tin có thể kích hoạt sự cố đến máy chủ, hệ thống hoặc mạng mục tiêu từ đó khiến người dùng hợp pháp không thể truy cập dịch vụ, tài nguyên họ mong đợi.

2.2 Hình thức tấn công DOS

2.2.1 Các loại tấn công DOS căn bản

- DoS Attack (Tấn công từ chối dịch vụ): Kẻ tấn công sẽ tạo ra một lượng lớn yêu cầu không hợp lệ hoặc yêu cầu tài nguyên quá nhiều để làm quá tải hệ thống. Điều này dẫn đến, khiến việc hệ thống không thể xử lý các yêu cầu này và trở nên không khả dụng đối với người dùng hợp lệ.

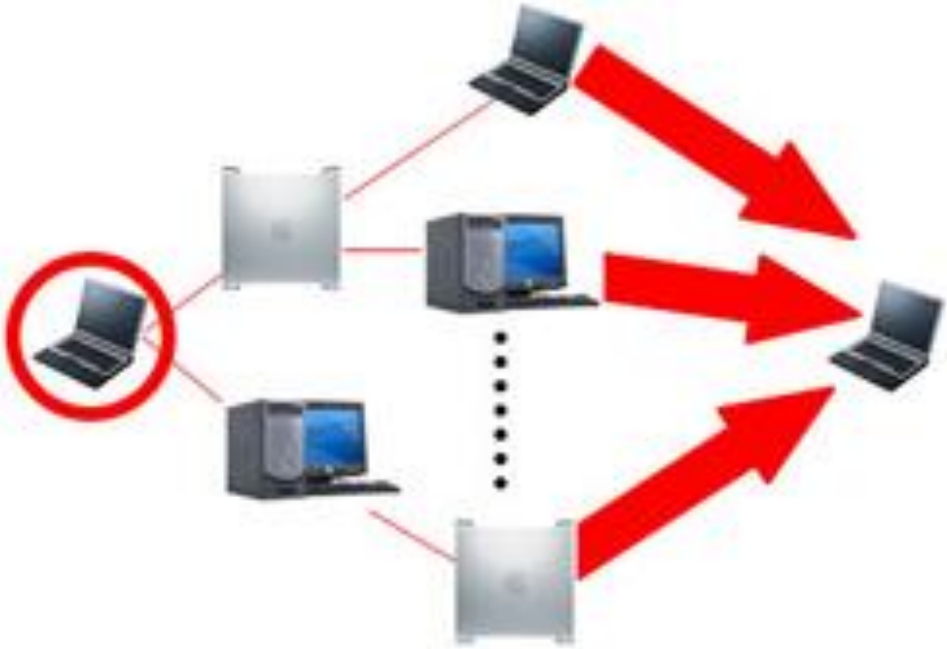
- Tấn công phân tán dịch vụ: Đây là phiên bản mạnh mẽ hơn của tấn công từ chối dịch vụ. Kẻ tấn công thường sử dụng một **Botnet** (một mạng các máy tính bị Hacker kiểm soát từ xa) để gửi một lượng lớn yêu cầu không hợp lệ hoặc tài nguyên quá tải đến mục tiêu. Số lượng lớn các hệ thống trong **Botnet** làm tăng sức mạnh tấn công và làm quá tải hệ thống máy chủ.

- Bandwidth Attacks (Tấn công áp lực băng thông): Hacker sẽ gửi lưu lượng mạng lớn tới hệ thống máy chủ nhằm làm chiếm hết băng thông mạng. Điều này làm cho hệ thống không thể đáp ứng được yêu cầu từ người dùng được nữa.

- Resource Consumption Attacks (Tấn công tiêu hao tài nguyên): Hacker thường sẽ tận dụng các lỗ hổng trong hệ thống để tiêu thụ tài nguyên, chẳng hạn như CPU, bộ nhớ hoặc bộ xử lý mạng máy chủ. Khi các tài nguyên này bị tiêu thụ quá nhiều mức cho phép, thì hệ thống trở nên quá tải và không thể hoạt động bình thường.

- Logic Attacks (Tấn công tổ chức hệ thống): Hacker sẽ tìm kiếm các lỗ hỏng trong cách tổ chức hệ thống của máy chủ để gửi các yêu cầu hoặc tạo ra tình huống không bất hợp lý, gây ra sự cố hoặc làm quá tải hệ thống.

- Service Disruption Attacks (Tấn công hỏng dịch vụ): Hacker tấn công vào các thành phần cụ thể của dịch vụ, chẳng hạn như: cơ sở dữ liệu, máy chủ DNS, máy chủ trang web, để làm cho dịch vụ không khả dụng gây ra sự cố gián đoạn hoạt động truy cập của người dùng.



2.2.2 Phân tích các hình thức tấn công DOS thường gặp

- **SYN FLOOD:** là loại hình tấn công lợi dụng những yếu điểm trên chuỗi kết nối TCP là khi người dùng thực hiện request TCP Syn thì sẽ không nhận được phản hồi gói tin SYN-ACK từ máy chủ đồng nghĩa với việc kết nối không hoạt động. Với việc gửi lien tục nhiều gói tin yêu cầu kết nối SYN, khiến cho các máy chủ Client không thể đáp ứng lưu lượng hoặc đáp ứng một cách chậm chạp.

- **UDP Flood:** đây là một loại giao thức kết nối mạng không đáng tin cậy thông qua việc gói tin được gửi đi mà không cần phải thiết lập TCP. Điều này sẽ khiến UDP Flood trở thành một hình thức tấn công phổ biến vì sẽ rất dễ dàng gửi một lượng lớn gói tin UDP đến mục tiêu mà không phải mất thời gian và tài nguyên để thiết lập kết nối.

- **HTTP Flood:** sử dụng các yêu cầu HTTP GET hoặc POST(Get được sử dụng để truy xuất dữ liệu, trong khi POST được dùng để gửi dữ liệu lên máy chủ và thực hiện thay đổi dữ liệu) gần như hợp pháp nhưng bị khai thác bởi các HACKER. Về hình thức này sẽ sử dụng

nhiều BONET và hàng ngàn máy tính bị kiểm soát buộc máy chủ phải sử dụng tối đa nguồn tài nguyên.

- **Ping of Death:** là hình thức gửi rất nhiều Ping độc hại đến hệ thông được sử dụng phổ biến ở hệ điều hình Windows NT trở xuống từ thập kỷ trước nên ít đem lại hiệu quả cao ở hiện tại.

- **Smurf Attack:** là hình thức loại dụng địa chỉ IP và các giao thức ICMP thông qua các chương trình độc hại. Hacker loại dụng địa chỉ IP nguồn làm mục tiêu tấn công ICMP đến các địa chỉ Broadcast trên nhiều mạng. Gây nên việc phải phản hồi số lượng lớn ICMP khiến cho mạng bị chậm lại không thể đáp ứng được dịch vụ khác.

- **Fraggle Attack:** tương tự như Smurf nhưng hình thức này không sử dụng nhiều ICMP . Hình thức này sử dụng nhiều lưu lượng UDP vào Router.

- **Slowloris:** là hình thức gửi yêu cầu kết nối TCP hợp lệ nhưng không hoàn chỉnh với số lượng lớn HTTP đến máy chủ web việc giữ duy trì kết nối này sẽ khiến trang web không giải phóng được tài nguyên cho các kết nối mới. Khi đó, máy chủ web sẽ không thể xử lý các yêu cầu từ người dùng hợp lệ và trở nên không khả dụng.

- **NTP Amplification:** là hình thức giả mạo địa chỉ IP với nguồn bị giả định tới máy chủ NTP thường là địa chủ IP của nạn nhân. Khiến cho máy chủ NTP cho rằng yêu cầu hợp lệ sẽ phản hồi lại với một gọi tin phản hồi có kích thược lớn hơn đáng kể. Gây nên quá tải mạng bằng lưu lượng lớn truy cập khiến cho băng thông của nạn nhân cạn kiệt tài nguyên mạng và gây ra tình trạng từ chối dịch vụ.

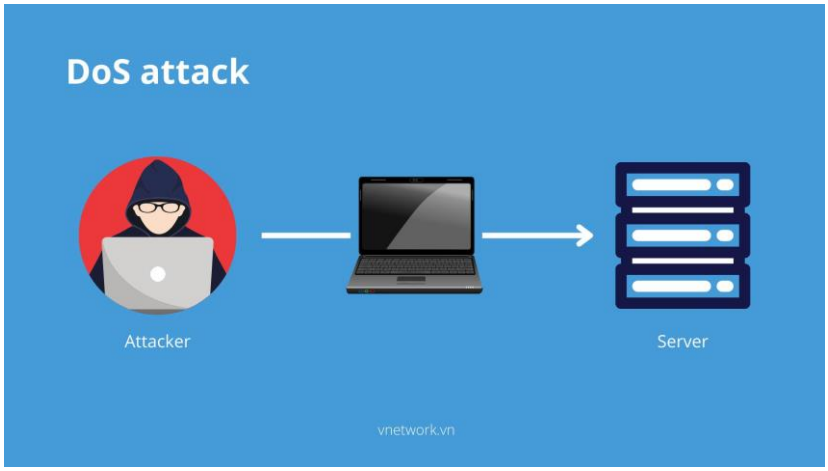
- **HTTP GET:** sử dụng một lượng lớn yêu cầu GEY giả mạo đến một máy chủ web hoặc ứng dụng cụ thể từ nhiều nguồn khác nhau. Điều này gây ra một lượng lớn yêu cầu đồng thời, quá tải tài nguyên của máy chủ và ảnh hưởng đến khả năng hoạt động của web.

- **Advanced persistent Dos (APDos):** là hình thức tấn công vô cùng phức tạp và nghiêm trọng bởi vì sử dụng những hình thức tấn công khác như HTTP Flood, SYN Flood,…

Làm ngừng hoạt động dịch vụ mục tiêu trong thời gian ngắn, mà còn gây ra hậu quả và thiệt hại vô cùng nghiêm trọng.

2.3 Cách thức hoạt động của tấn công DOS

- Tấn công DOS hoạt động bằng cách sử dụng một hệ thống để nhắm mục tiêu vào hệ thống của nạn nhân. Hệ thống bị nhắm làm mục tiêu của DOS được load từ gói dữ liệu gửi từ một vị trí duy nhất. DOS chủ yếu tập trung vào các loại tấn công như: tràn bộ đệm, tấn công Ping of Death hoặc ICMP flood, tấn công Teardrop Attack….



Quá trình của một cuộc tấn công DOS:

- Đầu tiên Hacker thường xác định mục tiêu tấn công có thể là một dịch vụ trực tuyến như: trang web, dịch vụ mạng: DNS hoặc hệ thống tường lửa.

- Sau đó sẽ thu thập thông tin mục tiêu bằng cách quyets, nghiên cứu cấu trúc mạng, phân tích các yếu tố bảo mật các lỗ hỏng để khai thác.

- Tiếp đến là lựa chọn công cụ và phương pháp thực hiện sao cho phù hợp với mục tiêu.

- Tiến hành tấn công mục tiêu bằng cách gửi lưu lượng truy cập lớn đến mục tiêu hoặc các phương thức tấn công như đã kể ở trên.

- Duy trì kiểm soát cuộc tân công cho hiểu qua hơn bằng cách thay đổi địa chỉ IP nguồn, thay đổi phương pháp tấn công,…

- Cuối cùng hậu quả của cuộc tấn công sẽ làm giảm hiệu suất hoạt động của hệ thống, gây mất niềm tin của khách hàng và người dùng. Đem lại thiệt hại tài chính to lớn đối với doanh nghiệp.

2.4 Mục tiêu của tấn công DOS

Các mục tiêu có thể bao gồm như:

- Dịch vụ trực tuyến: như trang web, hệ thống email, cổng thanh toán trực tuyến, trò chơi trực tuyến, và các dịch vụ trực tuyến khác …

- Hệ thống mạng như: cơ sở hạ tầng mạng, máy chủ DNS tường lửa, bộ chuyển mạch, hay các hệ thống kết nối mạng khác.
- Máy chủ: Cuộc tấn công có thể nhắm vào các máy chủ như máy chủ web, máy chủ ứng dụng, máy chủ cơ sở dữ liệu, máy chủ email, hoặc các máy chủ khác trên mạng.
- Hệ thống quản lý như hệ thống quản lý mạng (NMS), hệ thống quản lý bảo mật (SIEM), hoặc các hệ thống quản lý tổng thể của tổ chức.
- Cuộc tấn công có thể nhắm vào các công ty, tổ chức hoặc tổ chức chính phủ để làm gián đoạn hoạt động, gây thiệt hại tài chính hoặc đánh cắp thông tin quan trọng.

Tóm lại các mục tiêu bị tấn công nhằm phá hoại và gây thiệt hại đến cho các tổ chức hoặc cá nhân. Làm gián đoạn hoạt động kinh doanh, gây mất uy tín, gây thiệt hại tài chính và tiềm tàng đe dọa đến an ninh thông tin và dữ liệu của tổ chức.

2.5 Ứng phó và phòng ngừa tấn công DOS

- Thường xuyên giám sát lưu lượng mạng để phát hiện kịp thời các hoạt động bất thường hoặc lưu lượng truy cập tăng đột ngột
- Xác định và phân tích các biểu hiện của tấn công DOS như lưu lượng truy cập, gói tin độc hại và các yêu cầu không hợp lệ,….

- Triển khai giải pháp cân bằng tải để điều phối lưu lượng truy cập đều đặn và chống lại tấn công tập trung vào một điểm duy nhất.
- Nâng cấp và mở rộng khả năng hạ tầng của hệ thống.
- Sử dụng các dịch vụ bảo mật chuyên nghiệp. Những dịch vụ có các kiến thức sâu sắc về tấn công DOS và có thể cung cấp được cho chúng ta giải pháp bảo vệ tốt
- Lập kế hoạch phục hồi sau tấn công để khôi phục hoạt động bình thường của hệ thống.

2.6 Tình hình tấn công DOS ở Việt Nam

Theo như các báo cáo an ninh mạng Quý I/2021, Việt Nam ta thuộc Top 8 quốc gia chịu nhiều cuộc tấn công DOS. Nguyên nhân của vấn đề này là do các cá nhân hoặc nhóm tin tặc lợi dụng sự phát triển nhanh chóng các hoạt động trên không gian mạng.

Các kỹ thuật tấn công hiện nay được nâng cấp lien tục để tăng hiệu quả tấn công và các mục tiêu khác nhau. Do các kỹ thuật cũ trước đây dễ bị theo dõi và ngăn chặn nên đã có phiên bản cải tiến mới với tên gọi DDOS. Tấn công này điều khiển nhiều thiết bị tại nhiều vị trí khác nhau để khởi động cuộc tấn cồn nên rất khó để ngắn chặn.

Chương 3: Phân tích công cụ được dùng để tấn công DOS

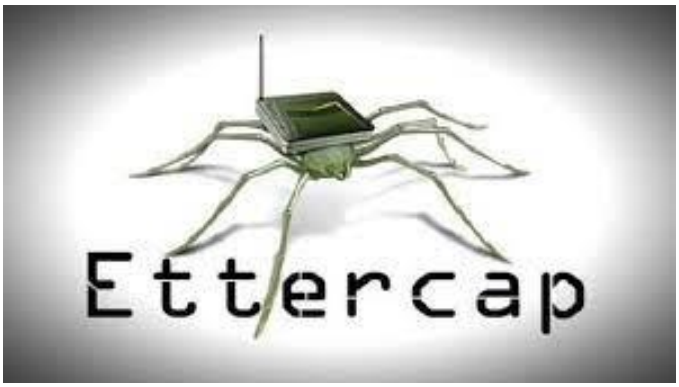
3.1 Công cụ Ettercap được dùng để tấn công DOS

3.1.1 Khái niệm sơ lược về Ettercap

Ettercap là một bộ phần mềm toàn diện dành cho các cuộc tấn công trung gian. Nó có tính năng đánh hơi các kết nối trực tiếp, lọc nội dung nhanh chóng và nhiều thủ thuật thú vị

Ettercap hỗ trợ phân tách chủ động và thụ động nhiều giao thức (thậm chí cả những giao thức được mã hóa) và bao gồm nhiều tính năng để phân tích mạng và máy chủ.

Ettercap cũng có khả năng phát hiện mạng LAN đã chuyển đổi và sử dụng dấu vân tay của hệ điều hành (chủ động hoặc thụ động) để tìm hình dạng của mạng LAN.



Ettercap chủ yếu là một công cụ dành cho Linux và các hệ điều hành tương tự Unix khác. Nó có sẵn cho các bản phân phối Linux sau: Debian, Ubuntu, Kali, BackTrack, Mint, Fedora, … Ngoài ra còn chạy trên Unix: FreeBSD, OpenBSD, NETBSD,… Trên Windows thì các phiên bản được nhà phát triển đề cập đến là: Windows Vista, 7,8.

3.1.2 Hình thức hoạt động của Ettercap

Ettercap là một công cụ mạng được sử dụng chủ yếu để thực hiện các cuộc tấn công trung gian và phân tích mạng. Sau đây là các hình thức hoạt động chính của Ettercap:

1. Đánh hơi (sniffing): kết nối trực tiếp giữa các máy tính trong mạng. Điều này cho phép Ettercap thu thập thông tin và lọc nội dung truyền qua mạng.

2. Phân tích giao thức: Ettercap hỗ trợ phân tích nhiều giao thức mạng, bao gồm cả các giao thức được mã hóa, nó có thể phân tích và hiển thị thông tin về các giao thức như TCP, UDP, ARP, ICMP,…

3. Thực hiện cuộc tấn công trung gian: Với các cuộc tấn công ARP (Address Resolution Protocol) spoofing, Ettercap có thể mạo danh địa chỉ IP của máy tính mục tiêu và làm cho máy tính mục tiêu tin rằng nó đang giao tiếp với một máy tính khác, chẳng hạn như một router. Điều này cho phép giành quyền kiểm soát lưu lượng truyền qua mạng và thực hiện các

hành động như thu thập thông tin xác thực, chuyển hướng lưu lượng hoặc thậm chí tấn công từ chối dịch vụ (DOS).

4. Lọc dữ liệu và thay đổi gói tin trong lưu lượng mạng: Ettercap có thể lọc (filter) các gói tin dựa trên các tiêu chí như địa chỉ IP nguồn/đích, cổng và nội dung. Ngoài ra\ cũng cho phép thay đổi gói tin bằng cách thay thế hoặc loại bỏ gói tin đã được nhận.

5. Phát hiện mạng LAN và tìm hình dạng mạng: Ettercap có khả năng phát hiện mạng LAN đã chuyển đổi và sử dụng dấu vân tay của hệ điều hành để phân tích và xác định cấu trúc của mạng LAN.

6. Giao diện người dùng đồ họa (GUI) và giao diện dòng lệnh: Ettercap cung cấp cả giao diện người dùng đồ họa (GUI) và giao diện dòng lệnh (CLI), cho phép người dùng lựa chọn giao diện tương thích với sở thích và kỹ năng của họ.

3.1.3 Các loại tấn công của Ettercap

Đầu độc ARP (ARP Poisoning): Trong cuộc tấn công này, Ettercap mạo danh (spoof) địa chỉ IP của máy tính mục tiêu và router trong mạng bằng cách gửi các gói tin ARP giả mạo. Điều này cho phép Ettercap giành quyền kiểm soát lưu lượng truyền qua mạng giữa các máy tính trong mạng và thực hiện các hành động như lắng nghe, chuyển hướng hoặc thay đổi gói tin.

Đánh cắp thông tin xác thực (Credential Sniffing): Ettercap có khả năng bắt và thu thập thông tin xác thực như tên người dùng và mật khẩu khi được truyền qua mạng. Với việc thực hiện cuộc tấn công ARP đầu độc, Ettercap có thể lắng nghe các gói tin truyền qua mạng và bắt các thông tin xác thực trong đó, cho phép kẻ tấn công lấy được thông tin đăng nhập của người dùng.

Chuyển hướng lưu lượng mạng (Traffic Redirection): Ettercap có khả năng chuyển hướng lưu lượng mạng từ máy tính mục tiêu sang máy tính của kẻ tấn công, cho phép kẻ tấn

công giữ quyền kiểm soát lưu lượng truyền qua mạng và thực hiện các hành động như đánh cắp thông tin, thay đổi dữ liệu hoặc ngăn chặn kết nối mạng.

Giả mạo DNS (DNS Spoofing): Ettercap có khả năng thực hiện cuộc tấn công giả mạo DNS bằng cách thay đổi các bản ghi DNS trong lưu lượng mạng. Điều này cho phép kẻ tấn công chuyển hướng lưu lượng truy cập đến các trang web.

Tấn công từ chối dịch vụ (DoS): Ettercap có thể sử dụng để thực hiện các cuộc tấn công từ chối dịch vụ bằng cách tạo ra một lượng lớn yêu cầu hoặc gói tin không hợp lệ để làm quá tải hệ thống đích và làm cho nó không khả dụng.

Giả mạo SSL (SSL Stripping): Ettercap có khả năng thực hiện cuộc tấn công giả mạo SSL, trong đó nó có thể thay thế các kết nối HTTPS bằng kết nối HTTP không được bảo mật. Điều này cho phép kẻ tấn công đọc và sửa đổi nội dung của các giao tiếp HTTPS.

3.1.4 Cách phòng chống tấn công Ettercap

Sử dụng giao thức bảo mật như HTTPS, SSH, VPN để mã hóa dữ liệu truyền qua mạng và ngăn chặn kẻ tấn công từ việc bắt và đọc thông tin nhạy cảm.

Cập nhật và áp dụng các bản vá đảm bảo hệ điều hành, ứng dụng và thiết bị mạng được cập nhật đầy đủ và áp dụng các bản vá bảo mật.

Sử dụng tường lửa (firewall và cấu hình an ninh để giới hạn lưu lượng truy cập đến và ra khỏi mạng của bạn. Cấu hình các quy tắc tường lửa để chặn hoặc kiểm soát lưu lượng truy cập không mong muốn và bất thường.

Kiểm tra và giám sát mạng định kỳ để phát hiện sớm các hoạt động đáng ngờ hoặc không hợp lệ. Sử dụng các công cụ giám sát mạng như: IDS (Intrusion Detection System) và IPS (Intrusion Prevention System) để phát hiện và cảnh báo về các cuộc tấn công trung gian và các hoạt động không hợp lệ khác.

Chứng thực hai yếu tố (2FA) cho các tài khoản quan trọng, đặc biệt là tài khoản quản trị và quyền truy cập cao. Điều này tăng cường bảo mật bằng cách yêu cầu người dùng xác thực

không chỉ bằng mật khẩu mà còn bằng một yếu tố khác như mã OTP (One-Time Password) hoặc thông báo xác minh.

Phân đoạn mạng: Phân chia mạng thành các mạng con nhỏ (subnets) và thiết lập các biên giới mạng (network boundaries) để giới hạn sự lan truyền của cuộc tấn công trong mạng nội bộ.

Chương 4: Kết Luận

Đề tài nghiên cứu tấn công DOS (Denial of Service) đã tập trung vào việc nghiên cứu và phân tích các phương pháp tấn công DOS, hiểu rõ cơ chế hoạt động và tác động của chúng lên hệ thống mục tiêu. DOS là một loại tấn công nhằm làm quá tải hệ thống bằng cách gửi một lượng lớn yêu cầu đến hệ thống mục tiêu, khiến nó không thể xử lý các yêu cầu từ người dùng hợp lệ. Từ đó phát triển các biện pháp phòng ngừa và giảm thiểu tác động của chúng. Việc nghiên cứu này góp phần quan trọng trong việc bảo vệ hệ thống mạng và đảm bảo sự ổn định và an toàn cho người dùng.