ĐẠI HỌC QUỐC GIA TP. HỒ CHÍ MINH

TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN

BÁO CÁO THỰC HÀNH MÔN:

AN TOÀN MẠNG

NHÓM 6 – NT101.N11.MMCL

Giảng viên hướng dẫn:

Ths.Tô Nguyễn Nhật Quang

Sinh viên thực hiện:		
STT	Họ tên	MSSV
1	Nguyễn Lê Thảo Nguyên	19521916

TP. HỒ CHÍ MINH – 12/2022

LỜI CẢM ƠN

Nhóm 6 xin gửi lời cảm ơn chân thành đến thầy Tô Nguyễn Nhật Quang – giảng viên hướng dẫn bộ môn An toàn mạng máy tính. Cảm ơn thầy vì thời gian qua với vai trò người lái đò đã luôn đồng hành và tận tình giảng dạy, hướng dẫn, đưa em đến bến bờ tri thức.

Tuy nhiên, trong quá trình làm bài do kiến thức chuyên ngành của em còn hạn chế nên không tránh khỏi những thiết sót khi đánh giá, thực hiện và trình bày vấn đề. Rất mong nhận được sự góp ý, đánh giá của thầy để chúng em có thể hoàn thiện hơn.

Một lần nữa, Em xin chân thành cảm ơn và chúc thầy luôn dồi dào sức khỏe, nhiệt huyết để tiếp tục truyền lửa, ươm mầm cho thế hệ sinh viên hôm nay và mai sau.

Tp. Hồ Chí Minh, ngày 30 tháng 12 năm 2022

Sinh viên thực hiên

Nguyễn Lê Thảo Nguyên

MỤC LỤC

MỤC LỤC

I. GIỚI THIỆU TỔNG QUAN ĐỀ TÀI

1. Lý do chọn đề tài

Việc bảo mật thông tin cho những dữ liệu quan trọng trên các thiết bị điện tử là điều mà chúng ta thường quan tâm để đảm bảo nguồn dữ liệu đó luôn được an toàn khi người dùng tiếp cận với môi trường Internet. Trong đó, các thông tin cá nhân

như thông tin về tài khoản ngân hàng, administrative là mục tiêu tấn công hang đầu từ các hacker. Bằng nhiều hình thức tấn công khác nhau mà kẻ xâm nhập có thể tìm ra được những lỗ hổng bảo mật để điều khiển hay thậm chí là chiếm quyền kiểm soát cao nhất trong hệ thống đó. Điều này lại đặc biệt quan trọng khi mọi thứ hiện nay đều được internet hóa.

Trong phạm vi báo cáo này, nhóm sẽ chỉ tập trung vào tấn công từ chối dịch vụ với trọng tâm là tấn công DoS (Denial of Service). Nhìn chung thì các kỹ thuật tấn công từ chối dịch vụ này ngăn người dùng truy cập các dịch vụ và trang web trực tuyến được kết nối thông qua việc khiến cho máy tính mục tiêu không thể xử lý kịp các tác vụ và dẫn đến quá tải.

2. Denial-of-Service (DoS) Attack

DoS tên đầy đủ tiếng Anh là Denial of Service, dịch ra tiếng Việt là từ chối dịch vụ. Tấn công từ chối dịch vụ DoS là cuộc tấn công nhằm làm sập một máy chủ hoặc mạng, khiến người dùng khác không thể truy cập vào máy chủ/mạng đó. Kẻ tấn công thực hiện điều này bằng cách "tuồn" ồ ạt 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 (nhân viên, thành viên, chủ tài khoản) không thể truy cập dịch vụ, tài nguyên họ mong đợi.

Nạn nhân của tấn công DoS thường là máy chủ web của các tổ chức cao cấp như ngân hàng, doanh nghiệp thương mại, công ty truyền thông, các trang báo, mạng xã hội...

Ví dụ, khi bạn nhập vào URL của một website vào trình duyệt, lúc đó bạn đang gửi một yêu cầu đến máy chủ của trang này để xem. Máy chủ chỉ có thể xử lý một số yêu cầu nhất định trong một khoảng thời gian, vì vậy nếu kẻ tấn công gửi ồ ạt nhiều yêu cầu đến máy chủ sẽ làm nó bị quá tải và yêu cầu của bạn không được xử lý. Đây là kiểu “từ chối dịch vụ” vì nó làm cho bạn không thể truy cập đến trang đó.

Kẻ tấn công có thể sử dụng thư rác để thực hiện các tấn công tương tự trên tài khoản email của bạn. Dù bạn có một tài khoản email của công ty hay dùng dịch vụ miễn phí như Gmail thì vẫn bị giới hạn số lượng dữ liệu trong tài khoản. Bằng cách

gửi nhiều email đến tài khoản của bạn, kẻ tấn công có thể làm đầy hòm thư đến và ngăn chặn bạn nhận được các mail khác.

3. Mục đích và tác hại của DoS

Khi DDoS, kẻ tấn công có thể sử dụng máy tính của bạn để tấn công vào các máy tính khác. Bằng cách lợi dụng những lỗ hổng về bảo mật cũng như sự không hiểu biết, kẻ này có thể giành quyền điều khiển máy tính của bạn. Sau đó chúng sử dụng máy tính của bạn để gửi số lượng lớn dữ liệu đến một website hoặc gửi thư rác đến địa chỉ email nào đó. Đây là kiểu tấn công phân tán vì kẻ tấn công sử dụng nhiều máy tính, bao gồm có cả máy tính của bạn để thực hiện tấn công DoS.

Mặc dù DDoS cung cấp một chế độ tấn công ít phức tạp hơn các dạng tấn công mạng khác, nhưng chúng đang ngày càng mạnh mẽ và tinh vi hơn. Có ba loại tấn công cơ bản:

- Volume-based: Sử dụng lưu lượng truy cập cao để làm tràn ngập băng thông mạng
- Protocol: Tập trung vào việc khai thác các tài nguyên máy chủ
- Application: Tập trung vào các ứng dụng web và được xem là loại tấn công tinh vi và nghiêm trọng nhất

Các cuộc tấn công DDoS được thực hiện với mạng các máy kết nối Internet.

Các mạng này bao gồm máy tính và những thiết bị khác (chẳng hạn như thiết bị IoT) đã bị nhiễm phần mềm độc hại, cho phép kẻ tấn công điều khiển chúng từ xa. Các thiết bị riêng lẻ này được gọi là bot (hoặc zombie) và một nhóm bot được gọi là botnet. Khi mạng botnet đã được thiết lập, kẻ tấn công có thể chỉ đạo một cuộc tấn công bằng cách gửi các hướng dẫn từ xa đến từng bot.

Khi máy chủ hoặc mạng của nạn nhân bị botnet nhắm mục tiêu, mỗi bot sẽ gửi yêu cầu đến địa chỉ IP của mục tiêu, có khả năng khiến máy chủ hoặc mạng bị quá tải, dẫn đến việc từ chối dịch vụ đối với lưu lượng truy cập bình thường. Bởi vì mỗi bot là một thiết bị Internet hợp pháp, việc tách lưu lượng tấn công khỏi lưu lượng truy cập thông thường sẽ rất khó khăn.

Đây là những hậu quả điển hình mà DDoS và DoS gây ra:

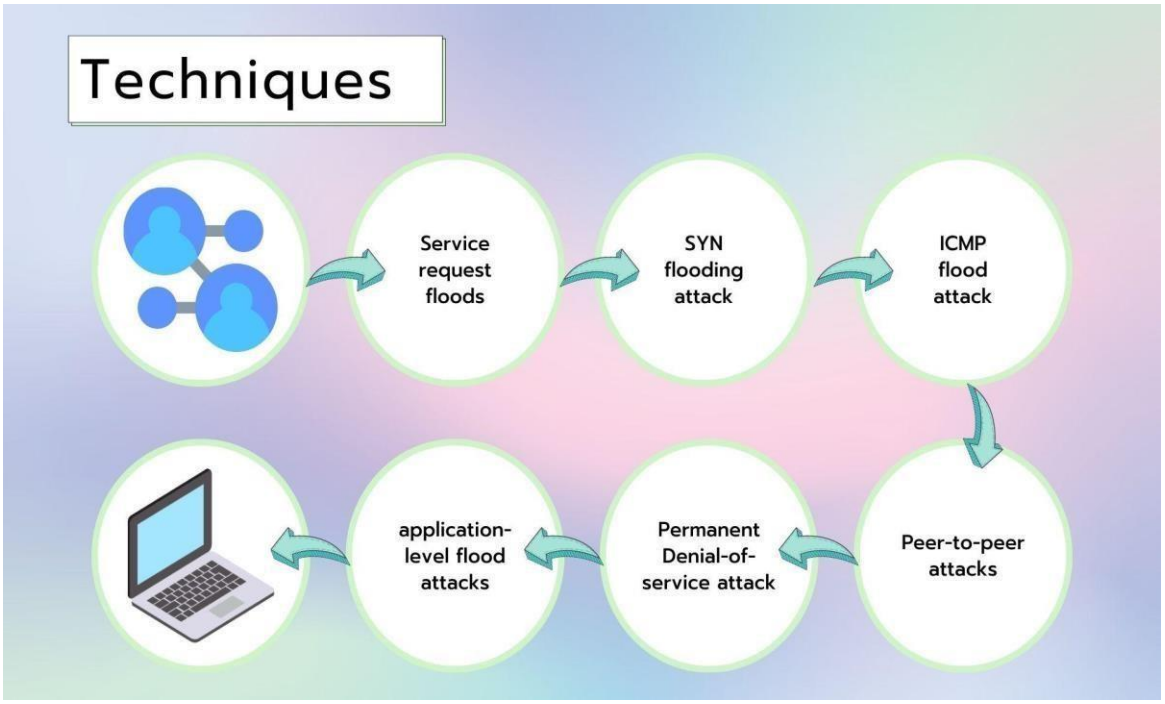
- Hệ thống, máy chủ bị DoS sẽ sập khiến người dùng không truy cập được
- Doanh nghiệp sở hữu máy chủ, hệ thống sẽ bị mất doanh thu, chưa kể đến khoản chi phí cần phải bỏ ra để khắc phục sự cố.
- Khi mạng sập, mọi công việc yêu cầu mạng đều không thể thực hiện, làm gián đoạn công việc, ảnh hưởng đến hiệu suất công việc.
- Nếu người dùng truy cập website khi nó bị sập sẽ ảnh hưởng đến danh tiếng của công ty, nếu website sập trong thời gian dài thì có thể người dùng sẽ bỏ đi, lựa chọn dịch vụ khác thay thế.
- Đối với những vụ tấn công DDoS kỹ thuật cao có thể dẫn đến việc lấy trộm tiền bạc, dữ liệu khách hàng của công ty.

4. Nhận biết tấn công DoS

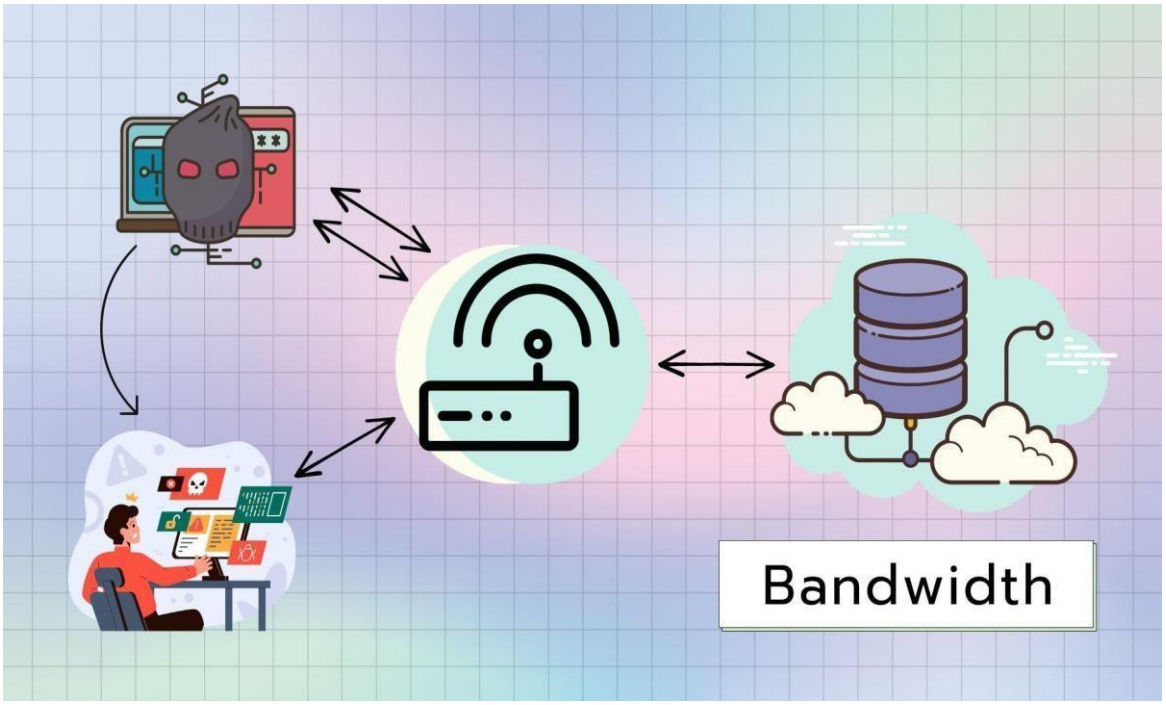
Không phải sự sập đổ hoàn toàn nào của dịch vụ cũng là kết quả của một tấn công từ chối dịch vụ. Có nhiều vấn đề kỹ thuật với một mạng hoặc với các quản trị viên đang thực hiện việc bảo trì và quản lý. Mặc dù thế nhưng với các triệu chứng dưới đây bạn có thể nhận ra tấn công DoS hoặc DDoS:

- Thực thi mạng chậm một cách không bình thường (mở file hay truy cập website)
- Không vào được website bạn vẫn xem
- Không thể truy cập đến bất kỳ một website nào
- Số lượng thư rác tăng một cách đột biến trong tài khoản của bạn.

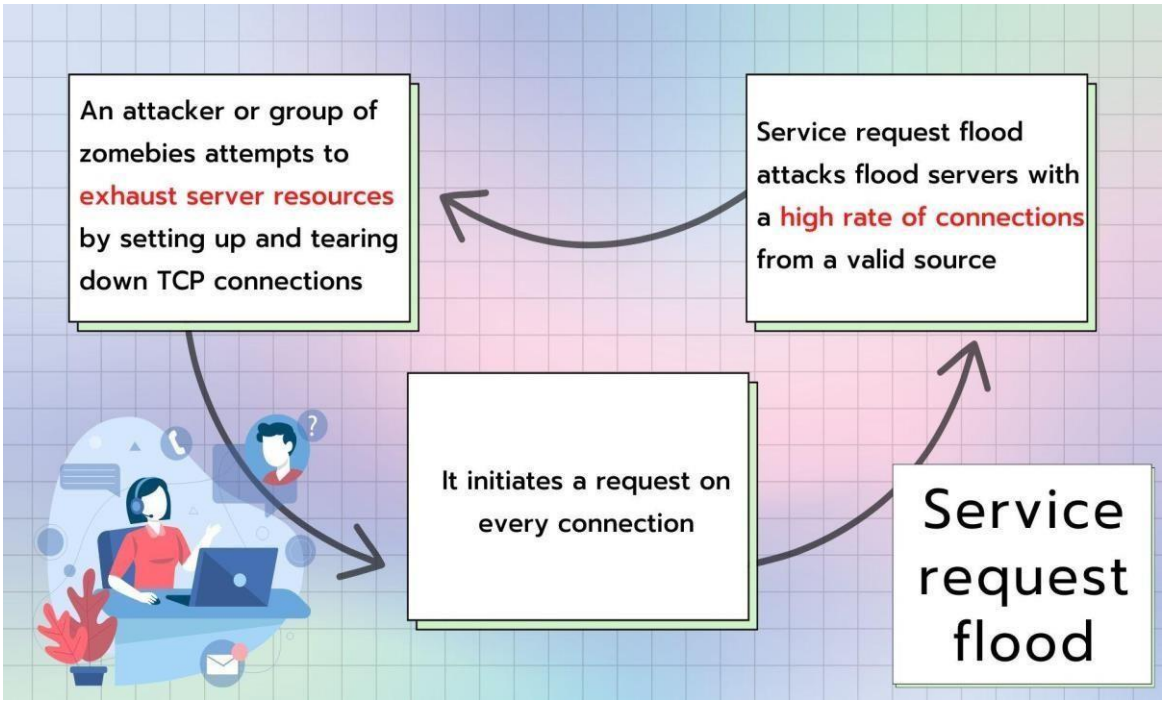
5. Một số kiểu tấn công hiện nay:



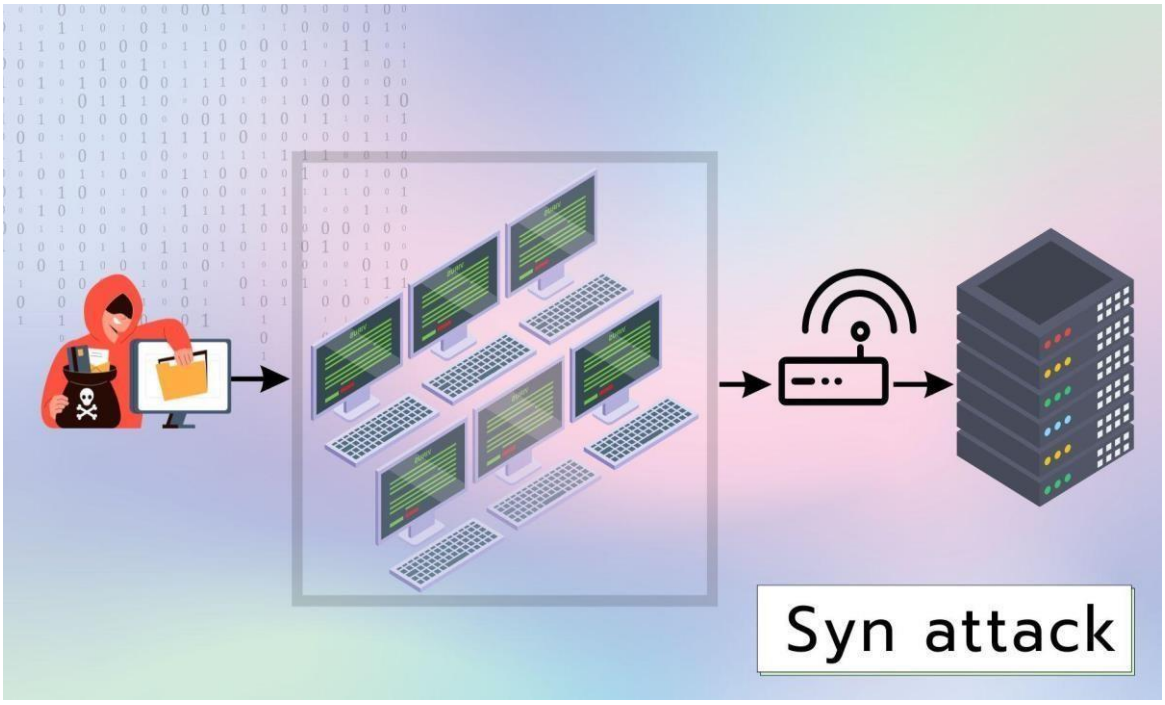
Hình 1. DoS Attack Techniques



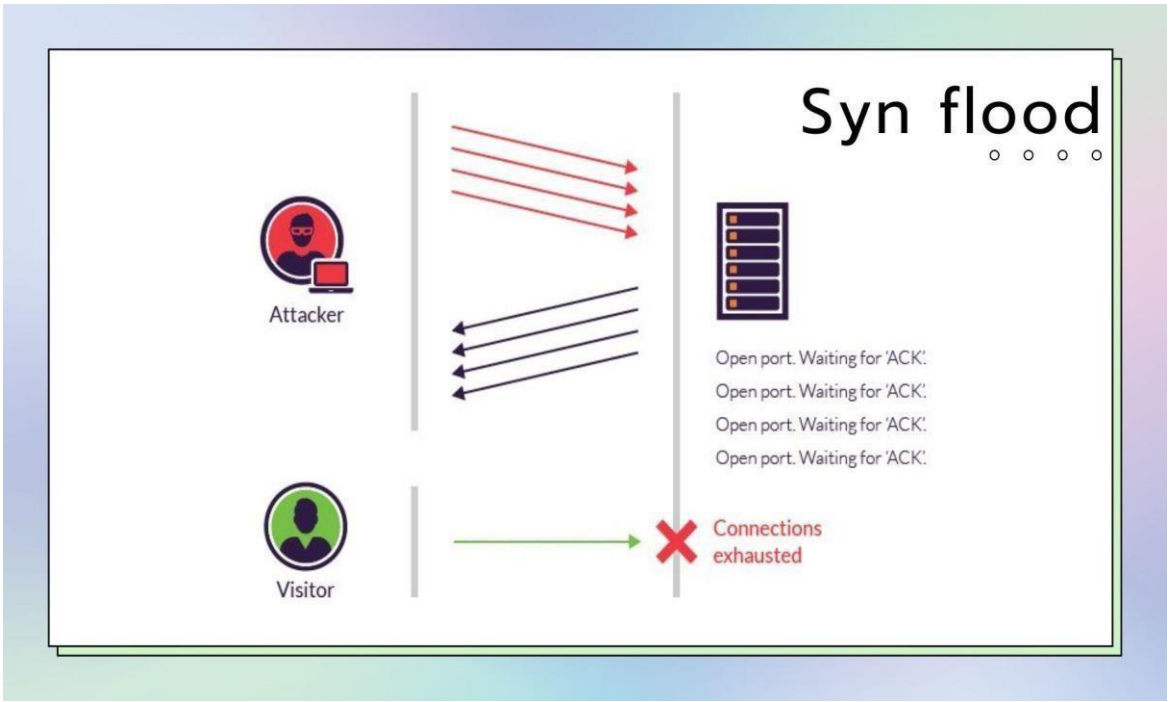
Hình 2. DoS Attack Bandwidth



Hình 3. Service request flood



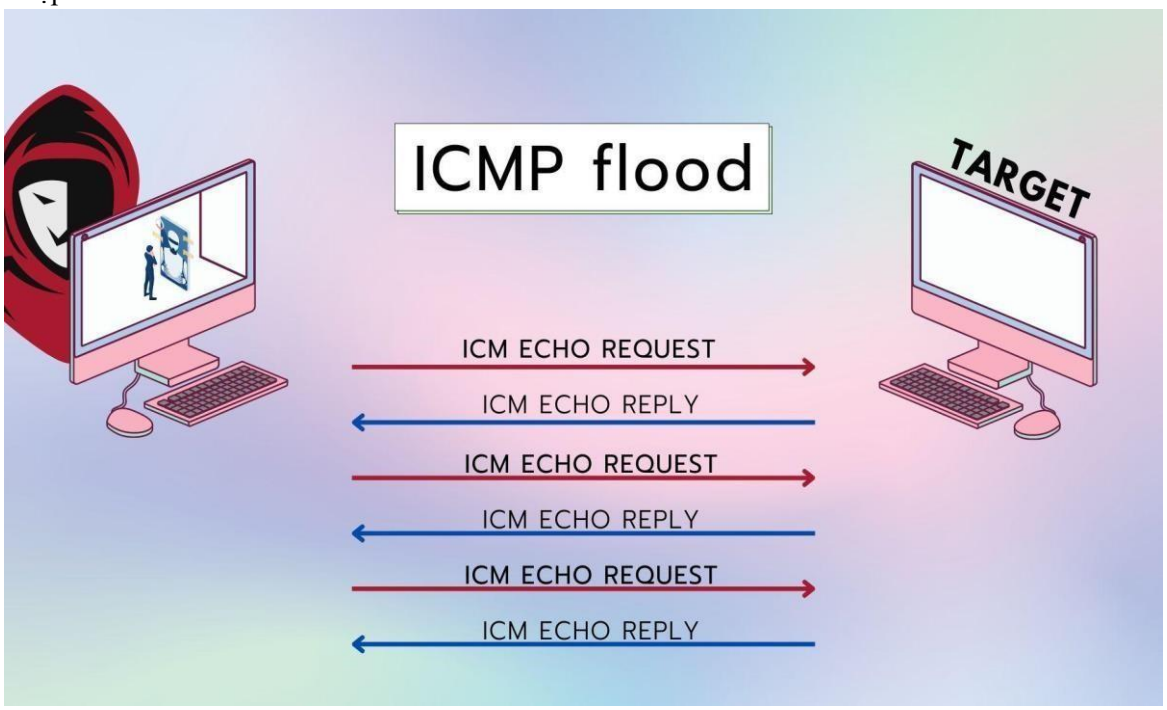
Hình 4. SYN attack



Hình 5. SYN flood

5.1 SYN flood (half-open attack)

Là một kiểu tấn công từ chối dịch vụ (DDos). Tấn công này với mục đích làm cho Server không có lưu lượng để truy cập hợp pháp. Bằng cách tiêu thụ tất cả tài nguyên server đang có sẵn. Người tấn công có thể áp đảo tất cả các cổng trên Server. Làm cho thiết bị Client đáp ứng lưu lượng hợp pháp một cách chậm chạp.



Hình 6. ICMP flood

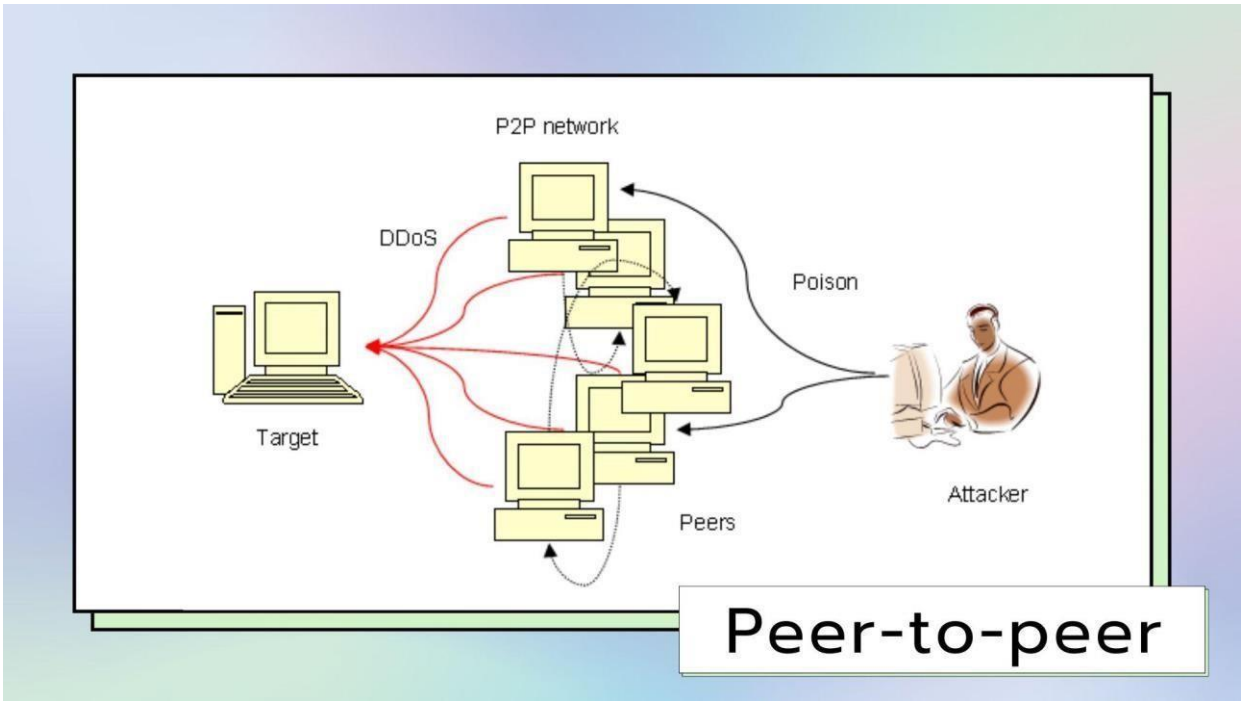
5.2 ICMP flood

Là cuộc tấn công Ddos, trong đó kẻ tấn công cố gắng áp đảo một thiết bị mục tiêu bằng các yêu cầu packets ICMP. Khiến mục tiêu không thể có lưu lượng truy cập bình thường.

Khi lưu lượng tấn công đến từ nhiều thiết bị, cuộc tấn công sẽ trở thành một tấn công DDoS hoặc phân tán.

Internet Control Message Protocol (ICMP) được sử dụng trong một cuộc tấn công Ping Flood. Là một giao thức internet được sử dụng bởi các thiết bị mạng để liên lạc. Các công cụ chẩn đoán mạng traceroute và ping đều sử dụng bằng ICMP. Thông thường, ICMP gửi các tin nhắn đến (echo-request) và phản hồi đi (echo-reply messages). Dùng để Ping các thiết bị trong mạng nhằm chuẩn đoán tình trạng sức khỏe. Kết nối của thiết bị, kết nối giữa người gửi và thiết bị.

Một yêu cầu ICMP cần một số tài nguyên server để xử lý từng yêu cầu và gửi phản hồi. Yêu cầu cũng cần tổng lưu lượng trên cả tin nhắn đến (echo-request) và phản hồi đi (echoreply). Cuộc tấn công Ping Flood nhằm áp đảo khả năng của thiết bị mục tiêu. Phản hồi với số lượng yêu cầu cao hoặc quá tải kết nối mạng với lưu lượng ảo. Bằng cách có nhiều thiết bị mạng botnet nhắm vào cùng một cơ sở hạ tầng hoặc cơ sở hạ tầng với các ICMP requests. Lưu lượng tấn công được tăng lên đáng kể. Có khả năng dẫn đến gián đoạn hoạt động mạng bình thường. Trong lịch sử, những kẻ tấn công thường giả mạo một địa chỉ IP để che giấu thiết bị gửi. Với các cuộc tấn công botnet hiện đại, hiếm khi thấy các kẻ xấu cần phải che giấu IP của bot. Thay vào đó dựa vào một mạng lưới lớn các bot không giả mạo để bão hòa công suất của mục tiêu tấn công.

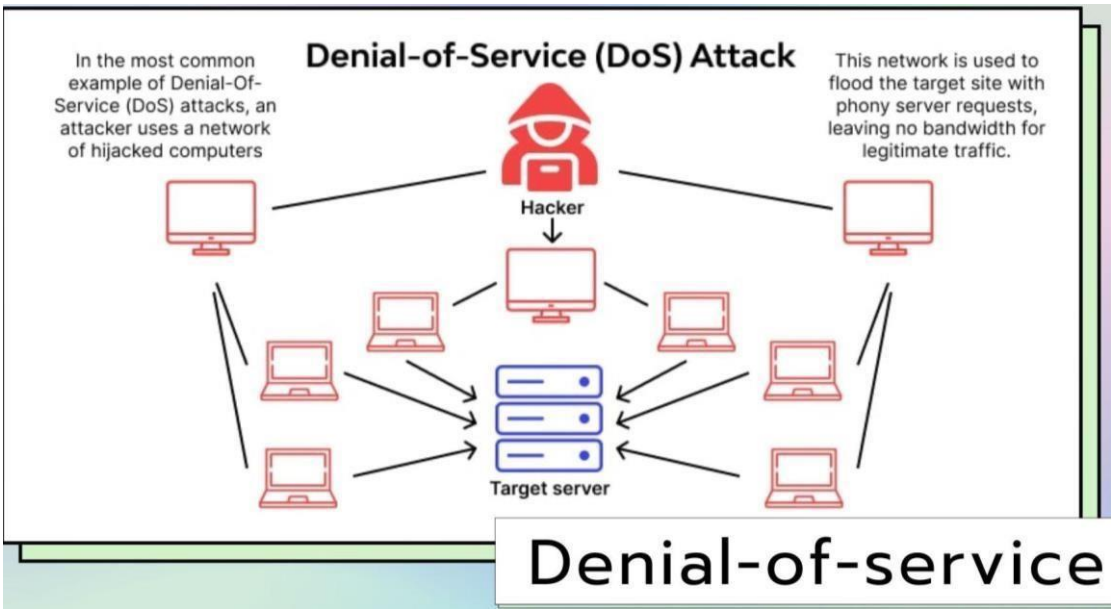


Hình 7. *Peer-to-peer*

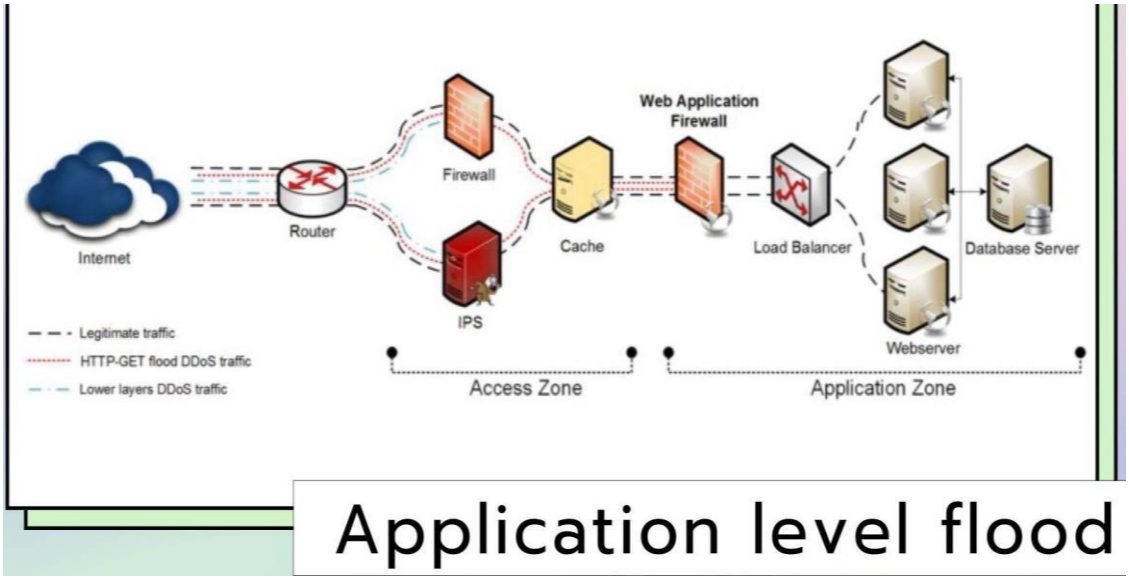
5.3 Mạng peer to peer (P2P)

Là một kiến trúc ứng dụng phân tán nhằm phân vùng nhiệm vụ hoặc khối lượng công việc giữa các peer. Các peer là những thiết bị tham gia trong ứng dụng có đặc quyền như nhau. Chúng tạo thành một mạng lưới các node ngang hàng.

Các peer tạo ra một phần tài nguyên của chúng, chẳng hạn như processing power, lưu trữ đĩa hoặc băng thông mạng, có sẵn cho những participant khác mà không cần sự điều phối trung tâm của server hoặc host ổn định. Các peer vừa là nhà cung cấp vừa là người tiêu thụ tài nguyên. Nó khác với mô hình client-server truyền thống ở chỗ việc tiêu thụ và cung cấp tài nguyên được phân chia. Trước đây hệ thống Peer to peer đã được sử dụng trong nhiều lĩnh vực ứng dụng. Kiến trúc này đã được phổ biến bởi hệ thống chia sẻ file Napster, phát hành vào năm 1999. Khái niệm này đã truyền cảm hứng cho các cấu trúc và triết lý mới trong nhiều lĩnh vực tương tác của con người. Trong bối cảnh xã hội như vậy, peer-to-peer as meme đề cập đến mạng xã hội bình đẳng đã xuất hiện trong toàn xã hội, được kích hoạt bởi công nghệ Internet nói chung.



Hình 8. . *Denial-of-service*



Hình 9. *Application level flood*

5.4 Application Layer Attack

Các cuộc tấn công lớp ứng dụng hay tấn công DDoS lớp 7 (L7) đề cập đến một loại hành vi độc hại được thiết kế để nhắm mục tiêu đến lớp "trên cùng" trong mô hình OSI, nơi xảy ra các yêu cầu Internet phổ biến như HTTP GET và HTTP POST. Các cuộc tấn công lớp 7 này, trái ngược với những cuộc tấn công lớp mạng như DNS Amplification, đặc biệt hiệu quả do chúng tiêu thụ tài nguyên máy chủ, ngoài tài nguyên mạng.

Để khám phá lý do tại sao lại như vậy, hãy xem xét sự khác biệt về mức tiêu thụ tài nguyên tương đối giữa một client đưa ra yêu cầu và server phản hồi yêu cầu. Khi người dùng gửi yêu cầu đăng nhập vào tài khoản trực tuyến chẳng hạn như tài khoản Gmail, lượng dữ liệu và tài nguyên mà máy tính của người dùng phải sử dụng là tối thiểu và không tương xứng với lượng tài nguyên được sử dụng trong quá trình kiểm tra thông tin đăng nhập, load dữ liệu người dùng có liên quan từ cơ sở dữ liệu, sau đó gửi lại phản hồi có chứa trang web được yêu cầu. Ngay cả khi không có thông tin đăng nhập, nhiều lần server nhận được yêu cầu từ client phải thực hiện các truy vấn cơ sở dữ liệu hoặc những lệnh gọi API khác để tạo ra một trang web. Khi sự chênh lệch này được tăng lên do nhiều thiết bị nhắm mục tiêu vào một thuộc tính web, như trong một cuộc tấn công mạng botnet, hiệu ứng có thể áp đảo máy chủ được nhắm mục tiêu, dẫn đến hiện tượng từ chối dịch vụ đối với lưu lượng truy cập hợp pháp. Trong nhiều trường hợp, chỉ cần nhắm mục tiêu một API với một cuộc tấn công L7 là đủ để đưa dịch vụ vào trạng thái ngoại tuyến.

II. HƯỚNG TRIỂN KHAI

1. Mô hình triển khai

Mô hình triển khai gồm: 1 máy áo Unbutu, 1 máy ảo Window sever 2016(IP: 192.168.20.136), 1 máy áo Window 10(IP: 192.168.20.132).

2. Cách tấn công

Dùng máy ảo Ubuntu (IP: để tấn công máy ảo Window 10 thông qua port đang mở(port 21 là port được chọn để tấn công trong bài lab này. Đầu tiên, dùng lệnh nmap -Pn 21 192.168.20.132 để quét, kiểm tra port (đóng hoặc mở). Sau đó dùng module synflood từ msfconsole để thực hiện tấn công.

III. KẾT LUẬN

Qua quá trình thực hiện tìm hiểm và năm được kiến thức về tấn công từ chối dịch vụ(DoS) và mô phỏng được về cách tấn công này.Từ đó, nhóm nhận thấy việc bảo vệ , và phòng. Mặc dù cố gắng triển khai càng nhiều biện pháp phòng chống cũng không thể ngăn chặn hoàn toàn 100%, nhưng nó cũng sẽ cải thiện khả năng bảo mật và sẽ làm cho kẻ tấn công cảm thấy khó khăn hơn trong việc tấn công.