TRƯỜNG ĐẠI HỌC KHOA HỌC, ĐẠI HỌC HUẾ

KHOA CÔNG NGHỆ THÔNG TIN

TIỂU LUẬN

TÌM HIỂU TẤN CÔNG DoS/DDoS TRONG MẠNG VÀ CÁCH THỨC PHÒNG CHỐNG

Giảng viên hướng dẫn: THS. Võ Việt Dũng

Nhóm : 11

1. Lê Thị Thuỳ Linh - 22T1020200
2. Phan Văn Tôn Bảo - 22T1020023
3. Trương Đức Mai Linh - 22T1020199
4. Nguyễn Thị Thuỳ Nhung - 21T1020572
5. Nguyễn Lê Xuân Tùng - 21T1020169

Huế, 12/2025

MỤC LỤC

CHƯƠNG I: TỔNG QUAN VỀ CÁC CUỘC TẤN CÔNG DOS/DDOS

1. Mở đầu

-Trong thế giới kết nối như ngày nay, an ninh mạng đã trở thành một cuộc đua không ngừng nghỉ giữa các chuyên gia bảo mật và các tin tặc. Các cuộc tấn công này nhắm vào mọi cơ quan tổ chức, các cơ quan chính phủ, các công ty lớn tới các tổ chức quốc tế với mục đích thị uy và trục lợi.

-Những cuộc tấn công gây ra thiệt hại về tài sản, thông tin kinh doanh mà còn về cả uy tín của các tổ chức ,trong đó các cuộc tấn công DoS và DDoS là những phương thức phổ biến, gây thiệt hại lớn về kinh tế và làm gián đoạn cuộc sống của hàng triệu người.

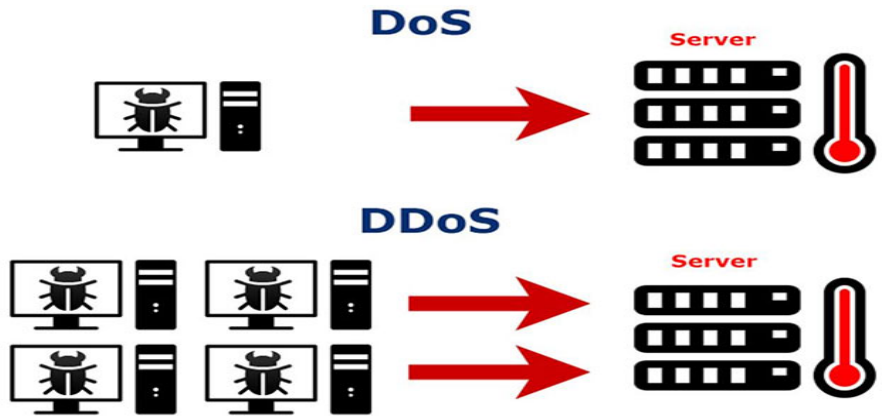
-Ddos là phương pháp phá hoại mạng, không được thực hiện để đánh cấp thông tin hay dữ liệu.

-Tác hại chính của phương pháp tấn công này là làm giảm khả năng đáp ứng của hệ thông dẫn đến hệ thống bị chậm hoặc tê liệt.

2. Khái niệm tấn công DoS/DDoS

2.1 Tấn công DoS

Dos (Denial of Service) là tấn công từ chối dịch vụ. Là cuộc tấn công từ một nguồn đơn lẻ máy tính, gửi một lượng lớn yêu cầu hoặc dữ liệu vượt quá khả năng xử lí dẫn đến một hệ thống, dịch vụ hoặc mạng bị treo hoặc không phản hồi.



2.2. Tấn công DDoS

DDoS (Distributed Denial of Service) là từ chối dịch vụ phân tán**.** Là một dạng nâng cao của tấn công DoS, DDoS sử dụng nhiều thiết bị, máy tính (botnet) để thực hiện cuộc tấn công với lưu lượng truy cập từ nhiều hệ thống khác nhau tạo ra một lưu lượng lớn hơn rất nhiều so với DoS làm quá tải tài nguyên của máy chủ hoặc mạng gây gián đoạn dịch vụ.

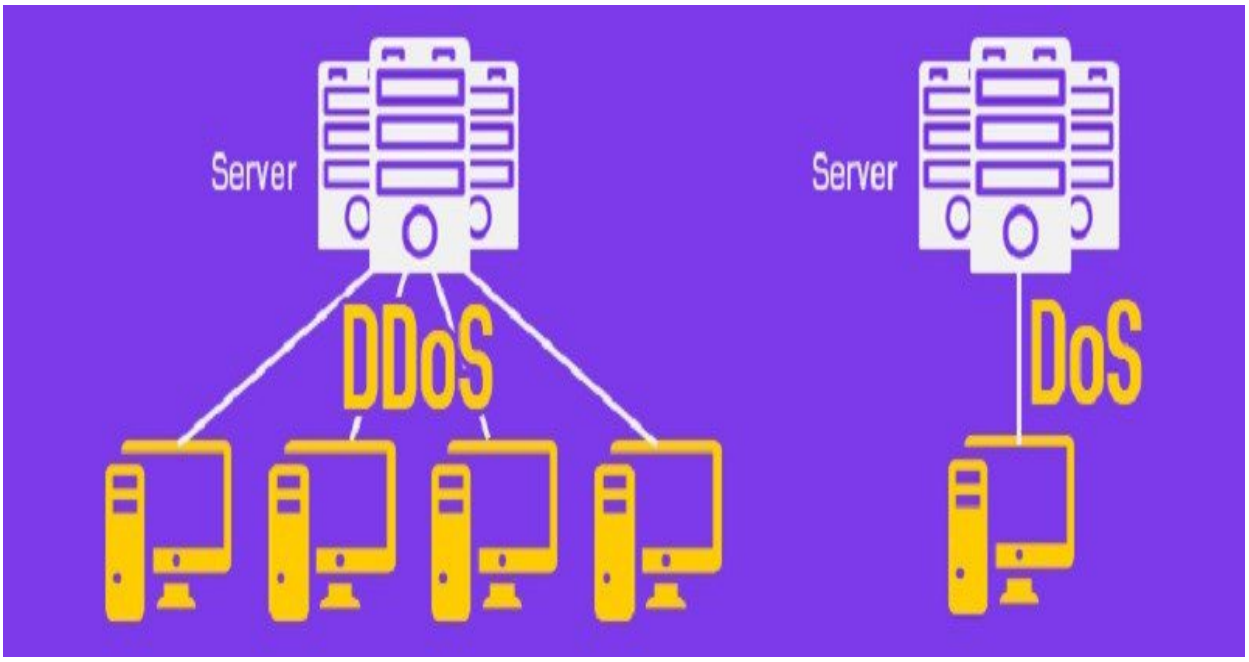
**** Botnet:***

- Botnet là một mạng lưới các thiết bị máy tính bị nhiễm phần mềm độc hại và được điều khiển bởi hacker từ xa. Một mạng botnet có thể bao gồm hàng trăm nghìn, thậm chí hàng triệu máy tính. Mỗi bot đóng vai trò như một công cụ để phát tán mã độc, virus và tấn công DDoS.

- Những thiết bị này thường được gọi là "bot" và chúng hoạt động như những "robot" tuân theo lệnh của kẻ tấn công.

2.3. Phân biệt DoS/DDoS

	DoS (Denial of Service)	***DDoS (Distributed Denial of Service)***
Nguồn gốc	Một hoặc một số ít máy tính	Nhiều máy tính (botnet)
Tốc độ tấn công	Chậm hơn (bắt đầu từ 1 địa điểm duy nhất)	Nhanh hơn (tấn công từ nhiều địa điểm)
Lượng truy cập	Ít hơn	Nhiều hơn (nhiều máy tính, mạng botnet)
Phức tạp	Thấp (sử dụng một tập lệnh hoặc một công cụ tấn công từ một máy duy nhất)	Cao (phối hợp nhiều máy chủ nhiễm phần mềm độc hại)
Tác động	Ít nghiêm trọng hơn	Nghiêm trọng hơn



3. Mục tiêu và xu hướng tấn công DoS/DDoS:

3.1. Mục tiêu

- Cuộc tấn công DDoS nhắm mục tiêu đến các trang web và máy chủ bằng cách làm gián đoạn dịch vụ mạng nhằm tìm cách làm cạn kiệt tài nguyên của ứng dụng. Thủ phạm đứng đằng sau các cuộc tấn công này sẽ gây tràn site bằng lưu lượng truy nhập lỗi, làm trang web hoạt động kém đi hoặc khiến trang web bị ngoại tuyến hoàn toàn.

- Những cuộc tấn công DDoS có phạm vi tiếp cận rộng, nhắm mục tiêu tới mọi loại ngành và tất cả các quy mô công ty trên toàn cầu. Một số ngành như trò chơi, thương mại điện tử và viễn thông bị nhắm mục tiêu nhiều hơn các ngành khác.

- Cuộc tấn công DDoS là một trong số các mối đe dọa trên mạng phổ biến nhất và chúng có thể xâm phạm tới doanh nghiệp, bảo mật trực tuyến, doanh thu và danh tiếng của bạn.

3.2. Xu hướng tấn công DoS/DDoS

- Các cuộc tấn công DoS/DDoS hiện nay đang diễn ra theo nhiều xu hướng mới. -
- Quy mô và cường độ tấn công tăng lên nhờ botnet lớn hơn, bao gồm nhiều thiết bị IoT bảo mật kém, cùng với các phương pháp khuếch đại như DNS và NTP amplification. Tấn công đa lớp, kết hợp giữa tấn công mạng và ứng dụng, làm cho việc phát hiện trở nên khó khăn hơn. Các dịch vụ đám mây trở thành mục tiêu chính, và kẻ tấn công ngày càng sử dụng trí tuệ nhân tạo để tự động hóa tấn công.

- Họ thường tấn công vào thời gian nhạy cảm và nhắm đến cả các tổ chức nhỏ và phi lợi nhuận. Sự phát triển công nghệ tấn công khiến việc phòng ngừa trở nên khó khăn hơn, yêu cầu các tổ chức nâng cao biện pháp bảo mật và theo dõi các mối đe dọa.

4. Tác động của tấn công DoS/DDoS

4.1.Gián đoạn dịch vụ

Người dùng không thể truy cập vào dịch vụ hoặc website bị tấn công, gây thiệt hại về kinh tế và danh tiếng.

4.2.Mất dữ liệu

Tấn công DoS/DDoS có thể dẫn đến mất dữ liệu quan trọng do lỗi hệ thống hoặc sự cố kĩ thuật.

4.3.Giảm hiệu quả hoạt động

Sự gián đoạn dịch vụ có thể làm giảm hiệu quả hoạt động của tổ chức, ảnh hưởng đến năng suất và hiệu quả.

4.4.Mất uy tín

Tấn công DoS/DDoS có thể làm tổ chức mất uy tín trong mắt khách hàng và đối tác, ảnh hưởng đến hình ảnh của tổ chức.

5. Lịch sử các cuộc tấn công Dos/DDos

5.1.Lịch sử

- Các cuộc tấn công DoS bắt đầu vào khoảng đầu những năm 90, bao gồm chỉ một kẻ tấn công khai thác băng thông tối đa từ nạn nhân, ngăn những kẻ khác được phục vụ, được thực hiện bằng cách sử dụng các phương pháp đơn giản như ping floods và UDP floods.

- Tấn công Ddos bắt đầu được biết đến từ năm 1996 và thuật ngữ "Ddos" trở nên phổ biến hơn từ năm 1999 với sự tấn công được công bố rộng rãi bằng chương trình Trinoo, nó dựa trên tấn công UDP flood và các giao tiếp master-slave. Các cuộc tấn công trở nên phức tạp và quy mô lớn hơn.

5.2. Các cuộc tấn công DDos nổi tiếng nhất lịch sử internet trên thế giới từ trước đến nay

5.2.1.Vụ tấn công DDoS vào 6 ngân hàng (2012)

- Ngày 12/03/2012, 6 ngân hàng của Mỹ đồng thời bị tấn công DDoS. Các ngân hàng này bao gồm Bank of America, JPMorgan Chase, U.S. Bank, Citigroup, Wells Fargo và PNC Bank.
- Các cuộc tấn công được tiến hành bởi hàng trăm máy chủ bị chiếm quyền thuộc mạng botnet có tên Brobot.
- Mỗi cuộc tấn công tạo ra tốc độ hơn 60Gbps.

5.2.2.Tấn công DDoS vào Dyn (2016)

- Ngày 30/09, một người tự xưng là tác giả của Mirai đã chia sẻ mã nguồn của phần mềm botnet Mirai DdoS trên các diễn đàn hacker khác nhau
- Ngày 21/10/2016, nhà cung cấp dịch vụ tên miền (DNS) lớn, đã bị tấn công bởi một trận "lũ lụt" lưu lượng truy cập lên tới 1Tbps, kỷ lục mới cho một cuộc tấn công DDoS.
- Lưu lượng truy cập đã đánh sập các dịch vụ của Dyn, khiến một số trang web nổi tiếng như GitHub, HBO, Twitter, Reddit, PayPal, Netflix và Airbnb không thể truy cập được.

5.2.3. Tấn công DDoS nhắm vào Brian Krebs và OVH (2016)

- Ngày 20/09/2016, blog của chuyên gia an ninh mạng Brian Krebs đã bị tấn công bởi một chiến dịch DDoS với tốc độ 620Gbps.
- Cuộc tấn công tiếp theo của Mirai nhắm vào OVH, một trong những nhà cung cấp dịch vụ lưu trữ lớn nhất châu Âu.
- Cuộc tấn công này nhắm vào một khách hàng của OVH, được thực hiện bởi khoảng 145.000 botnet và tạo ra lưu lượng truy cập 1.1Tbps, kéo dài trong 7 ngày.
- Nguồn gốc của cuộc tấn công tới từ mạng botnet Mirai.

5.2.4.Vụ tấn công vào Google (2017)

- Tháng 9 năm 2017 , Đội ngũ Google Cloud team bị một cuộc tấn công DDoS lớn chưa từng có
- Nhắm mục tiêu trực tiếp đến các dịch vụ của Google
- Cuộc tấn công DDoS này có độ lớn ước tính lên tới 2,54Tbps
- Cuộc tấn công DDoS đáng sợ nhất từng được ghi nhận trong lịch sử phát triển internet cho đến thời điểm hiện tại.

5.2.5.Cuộc tấn công DDoS nhắm vào GitHub (2018)

- Vào ngày 28/02/2018, GitHub, một nền tảng dành cho các nhà phát triển phần mềm, đã bị tấn công DDoS với tốc độ lên tới 1.35Tbps kéo dài trong khoảng 20 phút.

5.2.6.Cuộc tấn công DDoS vào AWS (2020)

- Tháng 2 năm 2020, Amazon Web Services (AWS), dịch vụ điện toán đám mây lớn nhất thế giới hiện tại, đã bị tấn công DDoS
- Dựa vào kỹ thuật CLDAP, kẻ tấn công đã khuếch đại lượng dữ liệu được gửi tới địa chỉ IP của nạn nhân lên từ 56 tới 70 lần.
- Cuộc tấn công kéo dài trong 3 ngày và lúc đỉnh điểm lưu lượng tấn công đạt 2.3 Tbps

5.2.7.Vụ tấn công vào khách hàng của Microsoft (2021)

- Microsoft bảo vệ thành công khách hàng sử dụng dịch vụ Azure tại châu Á trước cuộc tấn công DDoS có thông lượng lên tới 3,47 terabit mỗi giây (Tbps).
- Microsoft Azure DDoS cũng đã chặn hai cuộc tấn công DDoS khác nhắm vào các khách hàng châu Á với thông lượng lần lượt là 3,25 Tbps và 2,55 Tbps.

CHƯƠNG II: KỸ THUẬT TẤN CÔNG VÀ PHÒNG CHỐNG DOS

1. Cơ chế hoạt động của tấn công DoS/DDoS

Giai đoạn 1-Khởi tạo

Tin tặc hoặc botnet sẽ phát hiện và nhắm mục tiêu vào máy chủ hoặc dịch vụ mục tiêu.

Giai đoạn 2-Tấn công

Tin tặc gửi một lượng lớn lưu lượng truy cập hoặc yêu cầu không hợp lệ đến máy chủ mục tiêu.

Giai đoạn 3-Quá tải

Máy chủ bị quá tải, không thể xử lý các yêu cầu hợp pháp từ người dùng dẫn đến sự gián đoạn dịch vụ.

Giai đoạn 4-Hậu quả

Dịch vụ bị gián đoạn, người dùng không thể truy cập, gây thiệt hại về kinh tế và ảnh hưởng đến tổ chức.

2. Các kiểu tấn công DoS/DDoS

- Dựa vào những thành phần truyền thông tin và vận hành hệ thống trong mạng máy tính, tấn công DoS/DDoS có thể được phân loại dựa trên mục tiêu khai thác, bao gồm: tấn công dựa trên băng thông, tài nguyên hệ thống, giao thức, tầng ứng dụng và tấn công kết hợp.

- Một số kiểu tấn công:

1. UDP Flood
2. ICMP Flood
3. DNS Amplification Attack
4. Ping of Death
5. Teardrop Attack
6. Slowloris
7. SYN Flood
8. ACK Flood
9. Smurf Attack
10. HTTP Flood
11. Slow POST/GET Attack
12. XML Bomb

3.Tìm hiểu 1 số kĩ thuật tấn công

3.1. Ping of Death:

3.1.1. Khái niệm

-Tấn công Ping of death (PoD) là một cuộc tấn công từ chối dịch vụ (DoS) , trong đó kẻ tấn công nhắm mục tiêu làm gián đoạn máy mục tiêu bằng cách gửi một gói tin lớn hơn kích thước tối đa cho phép, khiến máy mục tiêu bị đóng băng hoặc sập.
-Dạng tấn công DoS này thường nhắm mục tiêu và khai thác các điểm yếu cũ mà các tổ chức có thể đã vá.

-Các hệ thống chưa được vá cũng có nguy cơ bị tấn công bằng ping, nhắm vào các hệ thống bằng cách làm quá tải chúng bằng các tin nhắn ping của Giao thức tin nhắn điều khiển Internet (ICMP) .

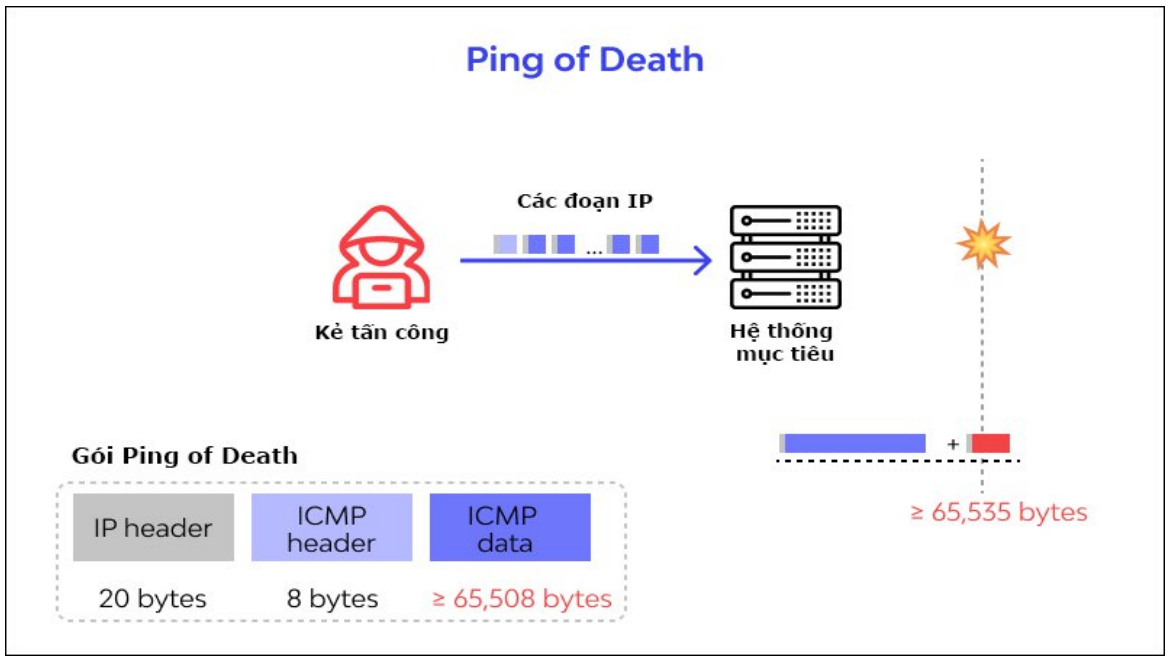
3.1.2. Cách thức hoạt động

-Kẻ tấn công gửi những gói tin IP lớn hơn số lượng bytes cho phép của tin IP là 65.535 bytes.

-Gói tin sẽ bị phân mảnh thành các phân đoạn, mỗi phân đoạn đều nhỏ hơn giới hạn kích thước tối đa. Khi máy mục tiêu cố gắng ghép các mảnh lại với nhau, tổng số vượt quá giới hạn kích thước và có thể xảy ra tràn bộ đệm, khiến máy mục tiêu bị đóng băng, sập hoặc khởi động lại.

-Quá trình chia nhỏ có thể thực hiện với gói IP lớn hơn 65.535 bytes. Nhưng hệ điều hành không thể nhận biết được độ lớn của gói tin này và sẽ bị khởi động lại, hay đơn giản là sẽ bị gián đoạn giao tiếp.

-Để nhận biết kẻ tấn công gửi gói tin lớn hơn gói tin cho phép thì tương đối dễ dàng.



3.1.3. Cách thức phòng chống

- Thêm các kiểm tra để đảm bảo giới hạn kích thước gói tối đa sẽ không bị vượt quá sau khi kết hợp lại.
- Tạo một bộ đệm bộ nhớ có đủ không gian để xử lý các gói tin vượt quá giới hạn tối đa.
- Sử dụng tường lửa để chặn các gói ICMP quá lớn hoặc bất thường.
- Giới hạn băng thông ICMP (Rate Limiting).
- Cập nhật hệ điều hành: hầu như các thiết bị tạo ra sau năm 1998 thường được bảo vệ chống lại tấn công này.

3.2. Tấn công Teardrop

3.2.1 Khái niệm

-Tấn công Teardrop là một cuộc tấn công từ chối dịch vụ (DoS) liên quan đến việc gửi các gói tin bị phân mảnh đến một máy mục tiêu. Vì máy nhận được các gói tin như vậy không thể lắp ráp lại chúng do lỗi trong quá trình lắp ráp lại phân mảnh TCP/IP, các gói tin chồng lên nhau, làm sập thiết bị mạng mục tiêu.

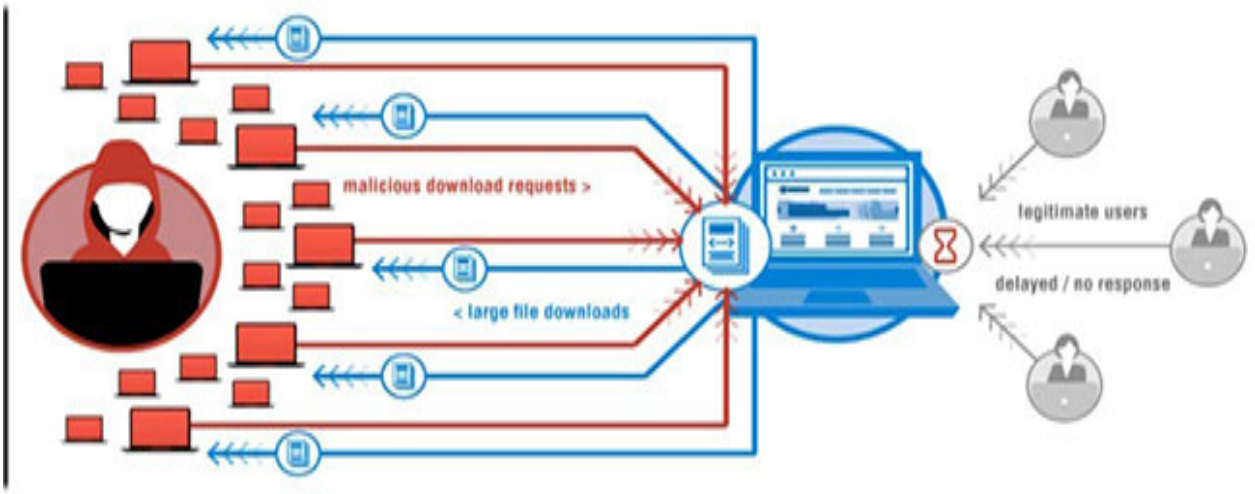
-Điều này thường xảy ra trên các hệ điều hành cũ hơn như Windows 3.1x, Windows 95, Windows NT và các phiên bản của hạt nhân Linux trước 2.1.63.

3.2.2 Cách thức hoạt động

-Gói tin IP rất lớn khi đến Router sẽ bị chia nhỏ làm nhiều phần nhỏ.

-Kẻ tấn công tạo ra các gói tin IP bị phân mảnh, trong đó thông tin về độ lệch (fragment offset) giữa các gói tin bị chỉnh sửa không hợp lệ, khiến chúng chồng chéo hoặc mâu thuẫn.

-Nếu hệ điều hành nhận được các gói tin đã được chia nhỏ và không hiểu được, hệ thống cố gắng build lại gói tin và điều đó chiếm một phần tài nguyên hệ thống, nếu quá trình đó liên tục xảy ra hệ thống không còn tài nguyên cho các ứng dụng khác, phục vụ các user khác.



3.2.3.Cách thức phòng chống

- Cập nhật phiên bản hệ điều hành của bạn.

Teardrop Attack khai thác lỗ hổng xử lý gói tin phân mảnh trên các hệ điều hành cũ.

- Giám sát hệ thống của bạn

Tìm các gói tin phân mảnh không hợp lệ.

Xác định nguồn IP của cuộc tấn công để chặn

- Tường lửa

Chặn gói tin phân mảnh, giới hạn lưu lượng

- Cấu hình router và thiết bị mạng

Bật kiểm tra phân mạnh.

Giới hạn MUT(Maximum Transmisson Unit) giới hạn kích thước gói tin.

3.3. Tấn công TCP SYN Flood (Transmission Control Protocol-synchronize Flood)

3.3.1.Khái niệm

Tấn công SYN (tấn công nửa mở) là một loại tấn công từ chối dịch vụ (DDoS) nhằm mục đích khiến máy chủ không thể tiếp cận lưu lượng hợp lệ bằng cách sử dụng hết tất cả các tài nguyên máy chủ khả dụng.

Bằng cách liên tục gửi các gói yêu cầu kết nối ban đầu (SYN), kẻ tấn công có thể làm quá tải tất cả các cổng khả dụng trên máy chủ mục tiêu, khiến thiết bị mục tiêu phản hồi chậm chạp hoặc không phản hồi lưu lượng hợp lệ.

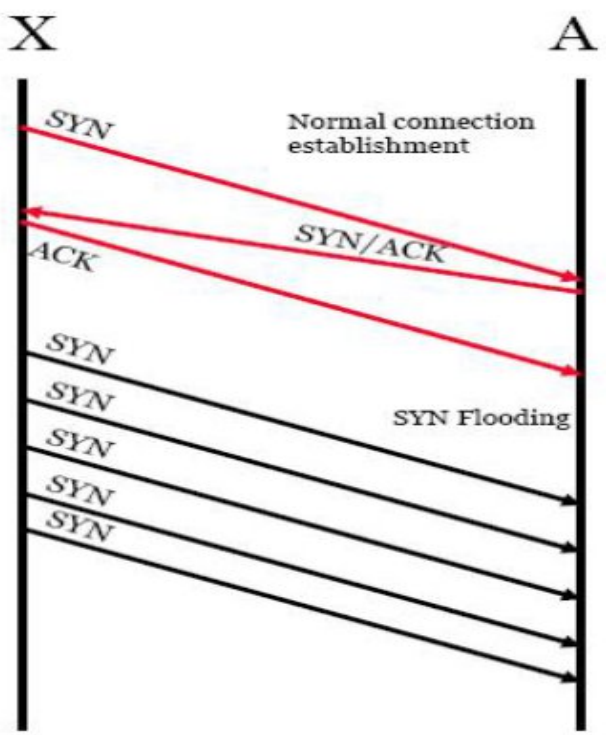
3.3.2.Cách thức hoạt động

Kẻ tấn công gửi các yêu cầu (request ảo) TCP SYN tới máy chủ bị tấn công. Để xử lý lượng gói tin SYN này hệ thống cần tốn một lượng bộ nhớ cho kết nối.

Khi có rất nhiều gói SYN ảo tới máy chủ và chiếm hết các yêu cầu xử lý của máy chủ. Một người dùng bình thường kết nối tới máy chủ ban đầu thực hiện Request TCP SYN và lúc này máy chủ không còn khả năng đáp lại - kết nối không được thực hiện

Đây là kiểu tấn công mà kẻ tấn công lợi dụng quá trình giao tiếp của TCP theo quy tắc bắt tay 3 bước.

Các đoạn mã nguy hiểm có khả năng sinh ra một số lượng cực lớn các gói TCP SYN tới máy chủ bị tấn công, địa chỉ IP nguồn của gói tin đã bị thay đổi.



- Hình bên trên thể hiện các giao tiếp bình thường với máy chủ và bên dưới thể hiện khi máy chủ bị tấn công gói SYN đến sẽ rất nhiều trong khi đó khả năng trả lời của máy chủ lại có hạn và khi đó máy chủ sẽ từ chối các truy cập hợp pháp.

- Quá trình TCP bắt tay 3 bước được thực hiện: Khi máy A muốn giao tiếp với máy B. (1) máy A bắn ra một gói TCP SYN tới máy B – (2) máy B khi nhận được gói SYN từ A sẽ gửi lại máy A gói ACK đồng ý kết nối – (3) máy A gửi lại máy B gói ACK và bắt đầu các giao tiếp dữ liệu.

- Máy A và máy B sẽ được kết nối ít nhất là 75 giây, sau đó lại thực hiện một quá trình TCP bắt tay 3 bước lần nữa để thực hiện phiên kết nối tiếp theo để trao đổi dữ liệu.

- Thật không may kẻ tấn công đã lợi dụng kẽ hở này để thực hiện hành vi tấn công nhằm sử dụng hết tài nguyên của hệ thống bằng cách giảm thời gian yêu cầu bắt tay 3 bước xuống rất nhỏ và không gửi lại gói ACK, cứ bắn gói SYN ra liên tục trong một thời gian nhất định và không bao giờ trả lời lại gói SYN&ACK từ máy bị tấn công.

3.3.3 Cách thức phòng chống

- Tường lửa và hệ thống phòng chống xâm nhập (IPS) :

Sử dụng tường lửa và thiết bị IPS để lọc lưu lượng truy cập độc hại và chặn các địa chỉ IP tham gia vào cuộc tấn công.

- Giới hạn tốc độ:

Triển khai giới hạn tốc độ để hạn chế số lượng kết nối đến mỗi giây từ một địa chí IP duy nhất.

- Bộ cân băng tải:

Phân phối lưu lượng truy cập đến nhiều máy chủ bằng bộ cân bằng tải để đảm bảo không có máy chủ nào trở thành mục tiêu của các cuộc tấn công tràn SYN.

- Củng cố ngăn xếp TCP/IP:

Tinh chỉnh các tham số ngăn xếp TCP/IP của máy chủ để xử lý các yêu cầu kết nối hiệu quả hơn và hạn chế số lượng kết nối mở một nửa.

- Phát hiện bất thường:

Sử dụng hệ thống phát hiện bất thường để xác định các mẫu lưu lượng truy cập bất thường và kích hoạt cảnh báo hoặc biện pháp đối phó.

- Mạng phân phối nội dung (CDN) :

CDN có thể giảm thiểu tác động của các cuộc tấn công tràn SYN bằng cách phân phối lưu lượng và lọc các yêu cầu độc hại

- Dịch vụ giảm thiểu DDoS :

Hãy cân nhắc đăng ký dịch vụ giảm thiểu DDoS có khả năng hấp thụ và lọc lưu lượng độc hại trước khi chúng đến mạng của bạn.

- **Cập nhật và vá lỗi thường xuyên:**

Luôn cập nhật các bản vá và cập nhật bảo mật mới nhất cho máy chủ và cơ sở hạ tầng mạng của bạn.

3.4. Tấn công DNS Amplification Attack

3.4.1. Khái niệm

DNS Amplification Attack là một kiểu tấn công DDoS (Distributed Denial of Service), trong đó kẻ tấn công lợi dụng các máy chủ DNS công khai để khuếch đại lưu lượng tấn công, làm quá tải và gián đoạn dịch vụ của máy chủ mục tiêu. Tấn công này sử dụng các yêu cầu DNS giả mạo, khiến máy chủ DNS phản hồi với dữ liệu lớn hơn rất nhiều so với yêu cầu ban đầu, từ đó gây ngập lưu lượng và làm mục tiêu không thể tiếp nhận kết nối hợp lệ.)

DNS Amplification là một kiểu tấn công phản chiếu, nhằm thao túng các DNS có thể truy cập công khai, khiến chúng trở thành mục tiêu với số lượng lớn các gói UDP. Bằng cách sử dụng nhiều kỹ thuật khác nhau, thủ phạm có thể "thổi phồng" kích thước của các gói UDP này, khiến cuộc tấn công trở nên mạnh mẽ đến mức phá hủy cả cơ sở hạ tầng Internet mạnh mẽ nhất.

3.4.2. Cách thức hoạt động

- Kẻ tấn công gửi một lượng lớn yêu cầu DNS giả mạo đến các máy chủ DNS công khai.

- Trong các yêu cầu này, địa chỉ IP đích được giả mạo thành địa chỉ IP của nạn nhân.

- Khi nhận được yêu cầu, máy chủ DNS sẽ trả lời lại địa chỉ IP đã được chỉ định (tức là địa chỉ IP của nạn nhân).

- Do lượng yêu cầu lớn và kích thước phản hồi có thể được khuếch đại, nạn nhân sẽ nhận được một lượng lớn lưu lượng truy cập, dẫn đến quá tải và ngừng hoạt động.

- "Khuếch đại" ở đây đề cập đến việc phản hồi của máy chủ không tương xứng với yêu cầu gói ban đầu được gửi.

*** Tính chất của phản hồi DNS**

- <u>Truy vấn nhỏ, phản hồi lớn:</u>

Kẻ tấn công gửi các truy vấn DNS nhỏ (chỉ vài chục byte), nhưng yêu cầu phản hồi chứa nhiều dữ liệu hơn (hàng trăm đến hàng nghìn byte).

- DNSSEC (DNS Security Extensions):

Nếu tên miền hỗ trợ DNSSEC, phản hồi DNS sẽ bao gồm các chữ ký số (cryptographic signatures), làm tăng kích thước phản hồi đáng kể.

*** Một số bản ghi trong hệ thống DNS** :

1. A Record (Address Record):

   Liên kết một tên miền với địa chỉ IPv4 của một máy chủ.

2. AAAA Record (IPv6 Address Record):

   Liên kết một tên miền với địa chỉ IPv6 của một máy chủ.

3. CNAME Record (Canonical Name Record):

   Chỉ định rằng một tên miền là bí danh (alias) của một tên miền khác.

4. MX Record (Mail Exchange Record):

   Xác định máy chủ nào chịu trách nhiệm nhận email cho tên miền.

5. NS Record (Name Server Record):

   Xác định các máy chủ DNS chịu trách nhiệm cho việc phân giải tên miền.

6. PTR Record (Pointer Record):

   Dùng trong reverse DNS lookup, giúp xác định tên miền từ một địa chỉ IP.

7. SOA Record (Start of Authority Record):

   Cung cấp thông tin cơ bản về một vùng DNS, bao gồm máy chủ chính (primary DNS server) và thông tin liên quan đến việc quản lý bản ghi của vùng.

8. TXT Record (Text Record):

   Cho phép lưu trữ văn bản hoặc thông tin dưới dạng văn bản tự do, thường dùng để xác thực và bảo mật.

9. SRV Record (Service Record):

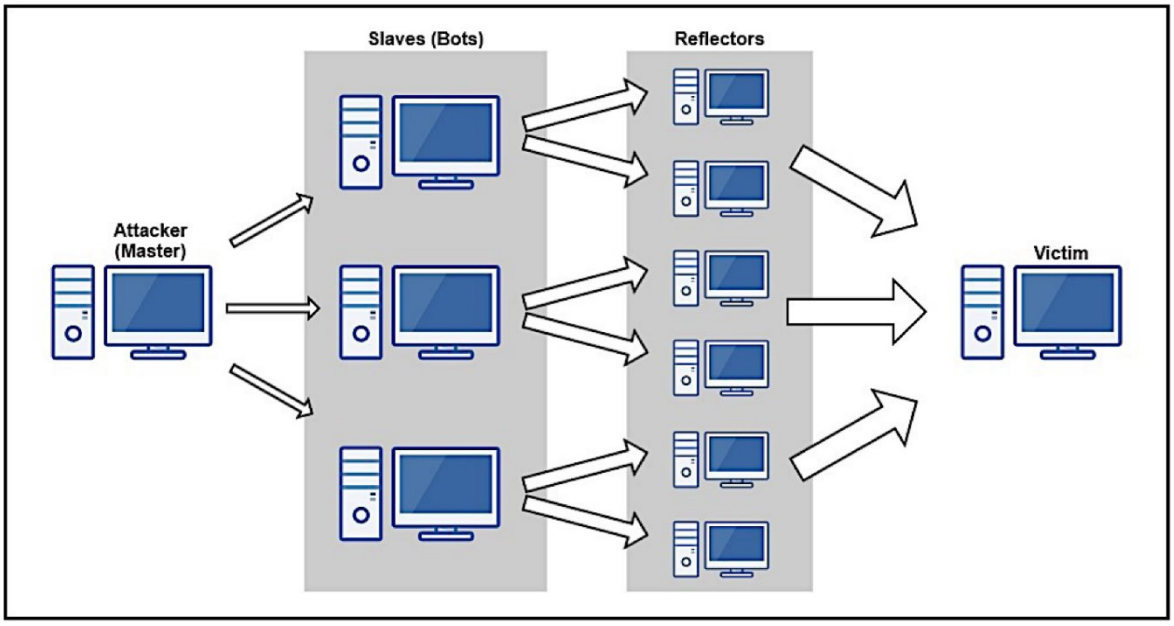
   Xác định các dịch vụ có sẵn trong mạng, chẳng hạn như dịch vụ tìm kiếm máy chủ hoặc chuyển tiếp tin nhắn.

10.CAA Record (Certification Authority Authorization Record):

Xác định tổ chức chứng nhận (CA) nào có quyền cấp chứng chỉ SSL/TLS cho tên miền.

-Thông qua các phương pháp này và những phương pháp khác, một thông báo yêu cầu DNS có kích thước khoảng 60 byte có thể được cấu hình để gửi thông báo phản hồi trên 4000 byte tới máy chủ đích – dẫn đến hệ số khuếch đại 70:1.

- Điều này làm tăng đáng kể khối lượng lưu lượng truy cập mà máy chủ mục tiêu nhận được và tăng tốc độ cạn kiệt tài nguyên của máy chủ.



3.4.3.Cách thức phòng chống

- Thắt chặt bảo mật DNS server, chặn những DNS server cụ thể hoặc tất cả các recursive relay server và giới hạn tốc độ.
- Giữ cho trình phân giải ở chế độ riêng tư và được bảo vệ.
- Quản lý DNS server một cách bảo mật
- Sử dụng các dịch vụ DNS bảo mật như Cloudflare, Google Public DNS, hoặc OpenDNS. Chống lại các kiểu tấn công khuếch đại
- Sự dụng hệ thống giám sát và phát hiện tấn công IPS/IDS.
- Thuê tìm thuê DDoS Proxy DDoS Filter ở VinaHost. DDoS Proxy DDoS Filter cản lọc được các loại tấn công sau: UDP Attacks, TCP SYN Flood, SYN-ACK Reflection Attacks, ICMP AttacksS, DNS Amplification Attacks, HTTP Attacks…với mức giá phù hợp với nhiều doanh nghiệp.

CHƯƠNG III: THỰC HÀNH

* Chuẩn bị môi trường thực hiện

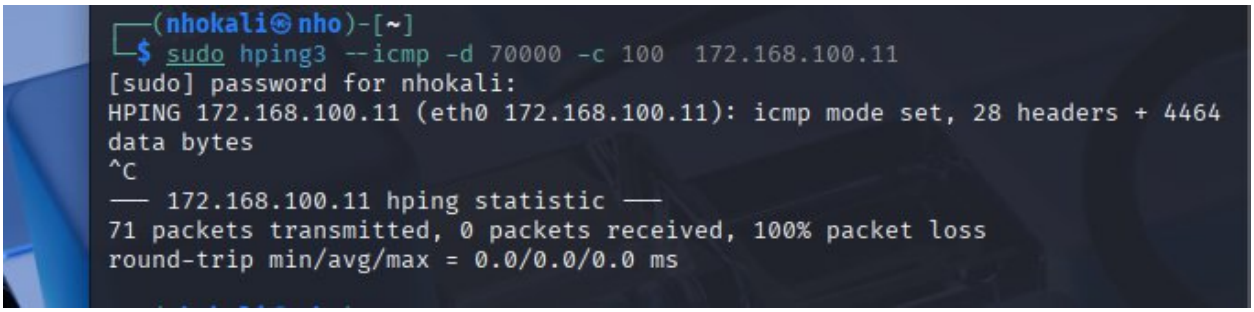
*** Cấu hình sẵn: OPNsense, 1 máy kali linux và 1 windows trên Vmwere workstation pro.**

- IP Windown: 172.16.100.11
- Default gateway: 172.16.100.1
- Subnet mask: 255.255.255.0
- IP Kali linux: 192.168.225.130
- Default gateway: 192.168.225.145
- Subnet mask: 255.255.255.0
- OPNsense :
- LAN à IPv4: 172.16.100.1/24
- WAN à Ipv4/DHCP: 192.168.225.131/24

1.Tấn công Ping of Death

1.1.Phân tích tấn công Ping of Death

- Mô phỏng tấn công bằng Kali lunux trên vmware



- Phân tích câu lệnh tấn công

SUDO HPING3 —ICMP –D 70000 –C 100 172.16.100.10

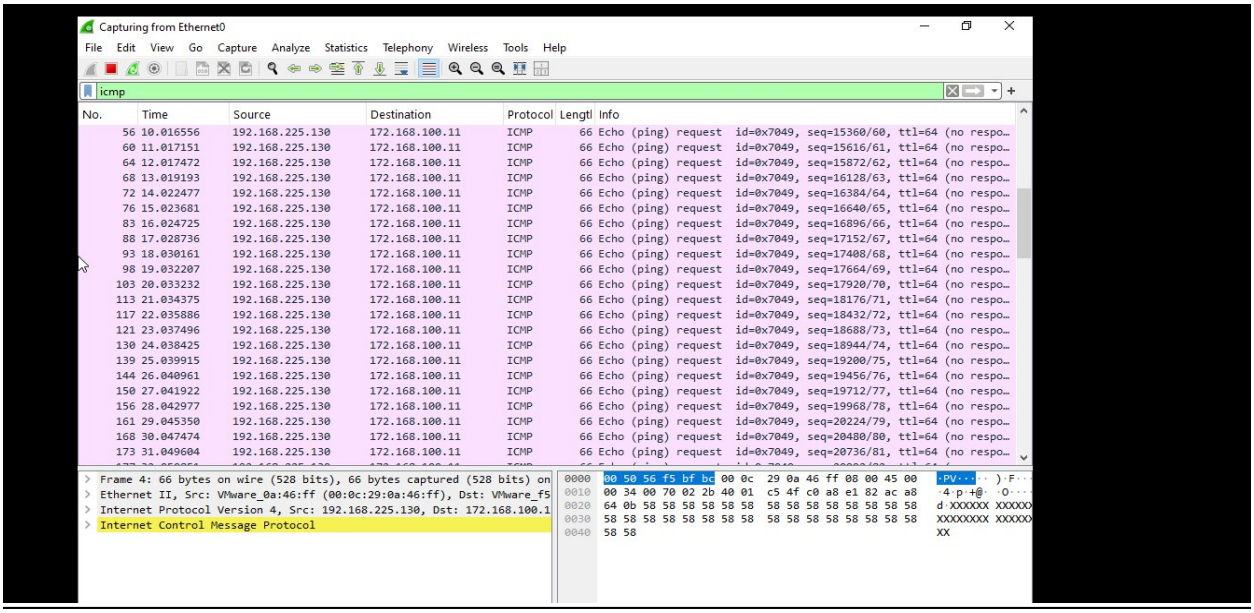
- Sudo: chạy lệnh với quyền root.
- Hping3: công cụ thực hiện mô phỏng.
- ICMP: giao thức điều khiển.
- D: Kích thước payload(dữ liệu trong gói tin). Để thực hiện tấn công ping of death phải dùng gói tin có kích thước lớn hơn MTU(Maximum Transmission Unit=65535 byte)
- C: Số lượng gói tin(thông thường trong các cuộc tấn công ping of death có số lượng gói tin thường bé nhưng vì dây là tấn công mô phỏng nên để dễ dàng bắt gói tin đã sử dụng số lượng gói tin lớn)
- 172.16.100.11: Địa chỉ IP của mục tiêu bị tấn công.

-Câu lệnh trả về

100 packets transmitted, 0 packets received, 100% packet loss

- 100 packets transmitted: Đã gửi thành công 100 gói tin từ máy của mình.
- 0 packets received: Máy không nhận được bất kỳ phản hồi nào từ địa chỉ đích.
- 100% packet loss: Tất cả gói tin bị mất (không nhận được phản hồi).

-Bắt gói tin bằng wireshak



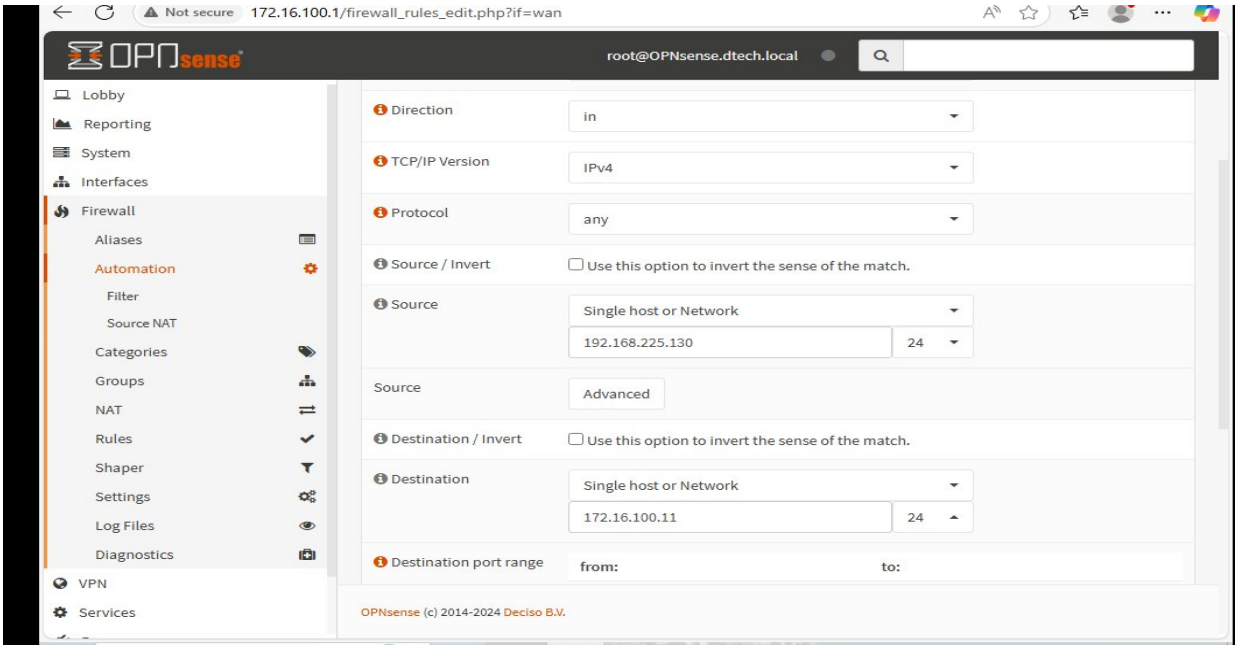
Phân tích gói tin trên wireshak

- Địa chỉ nguồn của gói tin là: 192.168.100.130
- Địa chỉ đích của gói tin là: 172.16.100.11
- Giao thức được sử dụng là : ICMP
- Dữ liệu gói tin ICMP (58 58 58...) được lặp đi lặp lại. Đây là một đặc điểm thường thấy khi tấn công Ping of Death
- Gói tin có cùng ID = 0x7049 và TTL = 64 cho thấy các gói tin thuộc cùng một phiên hoặc cùng một chuỗi tấn công, có khả năng là các gói phân mảnh thuộc một gói tin ICMP lớn duy nhất.
- Kích thước gói tin là 66 bytes (ở cột Length) cho một phân đoạn, nhưng nếu các gói phân mảnh này hợp nhất thành một gói lớn thì sẽ gây lỗi tràn bộ đệm.

1.2. Phòng phủ Ping of Death bằng OPNsense

Có thể sử dụng các rule có sẵn trên OPNsense hay tạo thêm 1 rule mới:

Tạo 1 rule mới



Phân tích rule

- Action đặt là Block : tất cả các gói tin phù hợp với quy tắc này sẽ bị chặn lại.
- Quick bật Apply the action immediately on match: khi một gói tin khớp với quy tắc này, hành động Block sẽ được áp dụng ngay lập tức mà không cần kiểm tra thêm các quy tắc khác.
- Interface là WAN: áp dụng cho tất cả lưu lượng đi vào qua giao diện mạng WAN (mạng ngoài internet).
- Direction: in: quy tắc này áp dụng cho lưu lượng đến (inbound) từ bên ngoài vào mạng nội bộ. Nghĩa là tất cả các gói tin ICMP từ mạng WAN (Internet) đến mạng LAN sẽ bị chặn.
- Protocol đặt là ICMP: quy tắc này chỉ áp dụng cho giao thức ICMP.
- TCP/IP Version: IPv4: giao thức mạng IPv4 (Internet Protocol Version 4).
- ICMP Type là any: tất cả các loại gói tin ICMP.
- Source: 192.168.225.130: địa chỉ nguồn(có thể để any để chạn tất cả gói tin phù hợp với rule từ mọi nguồn).
- Source Invert: không chọn : quy tắc này áp dụng chỉ cho các gói tin có địa chỉ nguồn là 192.168.225.130.
- Destination: 172.16.100.11: địa chỉ đích.

- Destination Invert: không chọn: quy tắc này chỉ áp dụng cho các gói tin có địa chỉ đích là 172.16.100.11.

- Chọn save.

- Applys changes.

CHƯƠNG IV: KẾT LUẬN

Tấn công DoS/DDoS là một mối đe dọa nghiêm trọng đối với hệ thống mạng và các dịch vụ trực tuyến. Hiểu rõ bản chất, cơ chế hoạt động và các phương pháp phòng thủ là điều cần thiết để bảo vệ hệ thống mạng khỏi những mối đe dọa này. Bằng cách áp dụng các biện pháp bảo mật cần thiết, doanh nghiệp và tổ chức có thể giảm thiểu rủi ro và nâng cao khả năng bảo vệ hệ thống mạng của mình trước các cuộc tấn công DoS/DDoS.

TÀI LIỆU THAM KHẢO

Lịch sử hình thành các cuộc tấn công Dos/Ddos:

https://www.viettelidc.com.vn/tin-tuc/lich-su-cac-cuoc-tan-cong-va-su-phat-trien-cua-tan-cong-tu-choi-dich-vu-dos

https://quantrimang.com/lang-cong-nghe/5-cuoc-tan-cong-ddos-noi-tieng-nhat-lich-su-internet-tu-truoc-toi-nay-175614

Cuộc tấn công DDoS là gì? | Microsoft Security

Khái niệm DoS/DDoS:

https://www.thegioididong.com/game-app/dos-ddos-la-gi-nhan-biet-ngan-chan-tan-cong-tu-choi-dich-vu-1392351

https://s.net.vn/c35x

Botnet:

https://www.vnetwork.vn/news/botnet-la-gi-cach-phong-chong-ddos-botnet-check-botnet-2022/

Ping of Death:

https://www.fortinet.com/resources/cyberglossary/ping-of-death

https://www.cloudflare.com/learning/ddos/ping-of-death-ddos-attack/

Teardrop:

https://www.radware.com/security/ddos-knowledge-center/ddospedia/teardrop-attack/

https://www.cloudns.net/blog/what-is-teardrop-attack-and-how-to-protect-ourselves/

TCP SYN Flood:

https://www.cloudflare.com/learning/ddos/syn-flood-ddos-attack/

https://vnso.vn/syn-flood-attack-ddos-la-gi-cach-thuc-phong-chong/

https://www.vnetwork.vn/news/cach-chong-ddos-attack-tcp-syn-flood-hieu-qua/

https://spyboy.blog/2023/10/12/understanding-tcp-syn-flood-attacks-a-comprehensive-guide/

DNS Amplification Attack :

https://quantrimang.com/cong-nghe/dns-amplification-la-gi-179132

https://blog.cloud365.vn/linux/dns-record/