

BỘ THÔNG TIN VÀ TRUYỀN THÔNG
HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG



THỰC TẬP CƠ SỞ

Đề tài:

**Triển khai hệ thống phát hiện và phòng chống xâm nhập
với SNORT và SNORTSAM**

Người hướng dẫn : TS. HUỖNH TRỌNG THỬA
Lớp : D21CQAT01-N
Khóa : 2021 – 2026
Hệ : ĐẠI HỌC CHÍNH QUY
Sinh viên thực hiện : NHÓM 12

MÃ SỐ SINH VIÊN	HỌ VÀ TÊN
N21DCAT004	NGUYỄN CHÍ BẢO
N21DCAT011	LÊ QUANG ĐỊNH
N21DCAT025	TRẦN QUANG KHA
N21DCAT034	NGUYỄN TRUNG NGHĨA
N21DCAT052	TRẦN ĐỨC THIÊN

TP.HCM, tháng 05/2024

MỤC LỤC

LỜI CẢM ƠN.....	7
MỞ ĐẦU.....	10
I. Bối cảnh nghiên cứu và tổng quan về IDS/IPS	10
1. Tính cấp thiết của đề tài.....	10
2. Tổng quan về IDS/IPS [2].....	10
3. Các kỹ thuật thường được sử dụng trong giải pháp IDS, IPS [3].....	13
II. Các kiểu tấn công mạng và cách phòng chống [4].....	13
1. Khái niệm.....	13
2. Các kiểu tấn công.....	13
CƠ SỞ LÝ THUYẾT.....	18
III. SNORT	18
1. Giới thiệu SNORT [8] [9].....	18
2. Kiến trúc của SNORT	18
IV. SNORT'S RULES	21
1. Cấu trúc:.....	21
2. Rule Header (5 thành phần)	21
3. Rule Options (4 loại).....	22
V. Cơ chế hoạt động của Plugin SNORTSAM [10] [11]	23
CÀI ĐẶT HỆ THỐNG.....	25
VI. Cài đặt SNORT, thiết lập rules	25
1. Cài đặt Snort	25
2. Thiết lập rules	28
VII. Mô hình mạng.....	29
1. Mô hình mạng.....	29
2. Cấu hình các phụ thuộc.....	31
THỰC NGHIỆM.....	40
VIII. Tiến hành kịch bản	40
1. Rules Snort3 các kịch bản:.....	40
2. Kịch bản DOS.....	40
3. Kịch bản XSS	43
4. Kịch bản SQL Injection	44
5. Kịch bản tấn công Brute Force:	45
IX. Ngăn chặn xâm nhập bằng IPTABLES	46

Các bước thực hiện:	46
X. Gửi thông báo tấn công về email với Sendmail	48
A. Các bước thực hiện sendmail cơ bản:	48
B. Kết hợp với Snort3	51
<i>Tài liệu tham khảo</i>	54

MỤC LỤC HÌNH ẢNH

Hình 1: IDS là gì?	11
Hình 2: Nhập abc vào và nhấn search.....	14
Hình 3: Thay đổi bằng đoạn Script	14
Hình 4: Trang web hiện thông báo.....	14
Hình 5: Kiến trúc của Snort (1).....	18
Hình 6: Kiến trúc của Snort (2).....	19
Hình 7: Tiến hành cài đặt các thư viện	25
Hình 8: Tải và giải nén các gói (1).....	25
Hình 9: Tải và giải nén các gói (2).....	25
Hình 10: Tải và giải nén các gói (3).....	25
Hình 11: Tải và giải nén các gói (4).....	26
Hình 12: Cập nhật các thư viện chia sẻ.....	26
Hình 13: Cài đặt Snort 3 thành công.....	27
Hình 14: Vô hiệu hóa LRO & GRO.....	27
Hình 15: LRO & GRO đã bị vô hiệu hóa	28
Hình 16: Snort3 đã phát hiện ICMP.....	28
Hình 17: Mô hình mạng	29
Hình 18: Máy Attacker tấn công.....	30
Hình 19: Cấu hình của máy IDS/IPS	30
Hình 20: Cấu hình của máy WEB Server	31
Hình 21: Cài đặt Iptable	36
Hình 22: Thiết lập ban đầu cho iptables.....	36
Hình 23: Kích hoạt khả năng định tuyến (1).....	36
Hình 24: Kích hoạt khả năng định tuyến (2).....	37
Hình 25: Kiểm tra trong Chain NAT	37

Hình 26: Xin địa chỉ.....	38
Hình 27: Tạo tệp cấu hình.....	38
Hình 28: Khởi động lại dịch vụ mạng.....	39
Hình 29: Tấn công Slowloris vào Web Server port 80	41
Hình 30: Attacker gửi hàng loạt request đến Web Server	41
Hình 31: Kết quả.....	42
Hình 32: Snort nghe trên mạng ens33 phát hiện DOS	42
Hình 33: Tấn công XSS	43
Hình 34: Snort nghe trên mạng ens33 phát hiện tấn công XSS	43
Hình 35: Tấn công SQL Injection (2)	44
Hình 36: Tấn công SQL Injection (1)	44
Hình 37: Snort nghe trên mạng ens33 phát hiện tấn công SQL Injection.....	45
Hình 38: Tấn công Brute force tài khoản người dùng bằng Hydra.....	45
Hình 39: Chống xâm nhập bằng IPTABLE	46
Hình 40: Máy attacker đã được đưa vào iptables.....	47
Hình 41: Máy attacker không còn ping được đến máy chủ sau khi bị chặn	48
Hình 42: Cấu hình sSMTP	48
Hình 43: Bật xác minh 2 bước	49
Hình 44: Tạo mật khẩu ứng dụng	49
Hình 45: Cấu hình sSMTP liên kết với mật khẩu ứng dụng	49
Hình 46: Cài đặt mailutils	50
Hình 47: Test gửi email.....	50
Hình 48: Tạo các file .txt để điều hướng.....	51
Hình 49: Thay đổi nội dung file blockip.sh (1).....	51
Hình 50: Thay đổi nội dung file blockip.sh (2).....	52
Hình 51: Nội dung file sendmail.sh	52

Hình 52: Nội dung file service.sh	52
Hình 53: Cảnh báo được gửi về mail	53

LỜI CẢM ƠN

Lời đầu tiên, nhóm em xin được gửi lời cảm ơn chân thành nhất đến thầy Nguyễn Trọng Thừa và thầy Lê Ngọc Hiếu. Trong quá trình học tập và tìm hiểu môn Thực Tập Cơ Sở, nhóm em đã nhận được rất nhiều sự quan tâm, giúp đỡ, hướng dẫn tâm huyết và tận tình của thầy. Thầy đã giúp em tích lũy thêm nhiều kiến thức về môn học này để có thể hoàn thành được bài tiểu luận về đề tài: Triển khai hệ thống phát hiện và phòng chống xâm nhập với SNORT và SNORTSAM.

Trong quá trình làm bài chắc chắn khó tránh khỏi những thiếu sót. Do đó, nhóm em kính mong nhận được những lời góp ý của thầy để bài tiểu luận của nhóm em ngày càng hoàn thiện hơn.

Xin chân thành cảm ơn thầy!

Nhóm 12

DANH MỤC TỪ VIẾT TẮT

Cụm từ	Ý Nghĩa
VSEC (Vietnamese Security)	Công ty cổ phần An ninh mạng Việt Nam
PHP (Hypertext Preprocessor)	Ngôn ngữ lập trình kịch bản hay một loại mã lệnh chủ yếu dùng để phát triển ứng dụng
VPN (Virtual Private Network)	Mạng dành riêng để kết nối các máy tính lại với nhau
NAT (Network Address Translation)	Chuyển đổi từ một địa chỉ IP thành một địa chỉ IP khác
LAN (Local Area Network)	Mạng máy tính cục bộ
WAN (Wide Area Network)	Mạng diện rộng
sSMTP (secure Simple Mail Transfer Protocol)	Giao thức Truyền tải Thư tin Đơn giản hóa bảo mật
JSON (JavaScript Object Notation)	Một kiểu định dạng dữ liệu tuân theo một quy luật nhất định mà hầu hết các ngôn ngữ lập trình hiện nay đều có thể đọc được
DOM (Document Object Model)	Cho phép các ngôn ngữ lập trình như JavaScript truy cập và thay đổi nội dung, cấu trúc và kiểu dáng của trang web một cách động
XSS (Cross Site Scripting)	Một loại lỗ hổng bảo mật web
DOS (Denial of Service)	Tấn công từ chối dịch vụ
DDOS (Distributed Denial of Service)	Tấn công từ chối dịch vụ phân tán
IP (Internet Protocol)	Một giao thức hướng dữ liệu
TCP (Transmission Control Protocol)	Giao thức phân phối dữ liệu theo thứ tự giữa các ứng dụng
UDP (User Datagram Protocol)	Giao thức giao tiếp thay thế cho TCP

ICMP (Internet Control Message Protocol)	Giao thức báo cáo lỗi
DAQ (Data Acquisition)	Thư viện thu thập dữ liệu của snort
IDS (Intrusion Detection System)	Ứng dụng phần mềm giám sát mạng
IPS (Intrusion Prevention System)	Hệ thống phát hiện và ngăn chặn xâm nhập
SSL (Secure Sockets Layer)	Giao thức mật mã được thiết kế để cung cấp truyền thông an toàn qua một mạng
LAMP (Linux – Apache – MySQL – PHP)	Là giải pháp máy chủ kết hợp từ 4 giải pháp phần mềm
ASA (Adaptive Security Appliance)	Một loại tường lửa trong Cisco
HTTP (Hypertext Transfer Protocol)	Giao thức truyền tải siêu văn bản
HTTPS (Hypertext Transfer Protocol Secure)	Giao thức truyền tải siêu văn bản an toàn
FTP (File Transfer Protocol)	Giao thức truyền tập tin
URL (Uniform Resource Locator)	Địa chỉ trang web
DNS (Domain Name System)	Hệ thống phân giải tên miền
MSSP (Managed Security Service Provider)	Nhà cung cấp dịch vụ bảo mật cho Cloud
SNMP (Simple Network Monitoring Protocol)	Giao thức giám sát mạng đơn giản

MỞ ĐẦU

I. Bối cảnh nghiên cứu và tổng quan về IDS/IPS

1. Tính cấp thiết của đề tài

Theo báo cáo thống kê của Công ty an ninh mạng Việt Nam (VSEC) thì trong năm 2023, đơn vị này đã ghi nhận 148.615 sự cố và 2.630 lỗ hổng bảo mật. Về tổng quan, lượng lỗ hổng bảo mật được phát hiện tại Việt Nam đang có chiều hướng gia tăng. Nếu so với chỉ một năm trước đó, số lượng lỗ hổng mà VSEC phát hiện trong năm 2023 có sự nhảy vọt, lên tới 21%. Trong đó, tỷ lệ sự cố về truy cập trái phép, chiếm quyền điều khiển, chiếm tỷ trọng lớn nhất tại Việt Nam. Các sự cố an toàn thông tin dạng này thường xảy ra ở nhóm doanh nghiệp ngân hàng, tài chính và bảo hiểm. [1]

Dựa vào số liệu trên, chúng ta thấy được nhu cầu bảo mật mạng ngày càng trở nên cấp thiết. Các mối đe dọa mạng ngày càng tinh vi và nguy hiểm, đòi hỏi các giải pháp bảo mật hiệu quả và mạnh mẽ. Hệ thống phát hiện và chống xâm nhập (IDS/IPS) đóng vai trò quan trọng trong việc bảo vệ mạng khỏi các cuộc tấn công mạng.

Để hiểu rõ thêm về hệ thống phát hiện (IDS) và chống xâm nhập (IPS), nhóm chúng tôi sẽ tiến hành triển khai 1 hệ thống phát hiện và chống xâm nhập với Snort/SnortSam. Snort là một hệ thống IDS/IPS mã nguồn mở phổ biến và mạnh mẽ được sử dụng rộng rãi trên toàn thế giới. Được phát triển bởi Martin Roesch vào năm 1998, Snort ban đầu chỉ là một công cụ IDS đơn giản. Tuy nhiên, sau đó nó được phát triển thêm để trở thành một hệ thống IPS có khả năng ngăn chặn các cuộc tấn công mạng.

Sở hữu nhiều ưu điểm nổi bật như miễn phí, mã nguồn mở, cộng đồng hỗ trợ lớn giúp đạt hiệu quả cao trong việc phát hiện và ngăn chặn nhiều loại tấn công mạng khác nhau. Tuy nhiên, Snort cũng có một số nhược điểm như yêu cầu kiến thức chuyên môn để cấu hình và sử dụng hiệu quả, đồng thời có thể gây ra tình trạng báo động giả và bỏ sót.

2. Tổng quan về IDS/IPS [2]

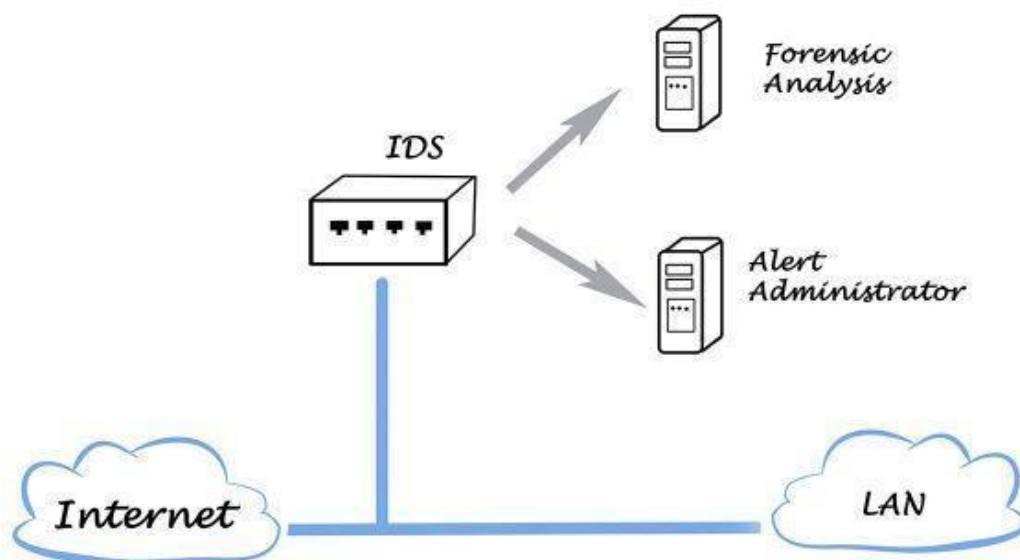
a. IDS

IDS là gì?

IDS trong lĩnh vực công nghệ thông tin thường được hiểu là “Intrusion Detection System”, có nghĩa “Hệ thống phát hiện xâm nhập”, là một công cụ được sử dụng để giám sát và phát hiện các hành vi xâm nhập vào hệ thống

mạng, giúp bảo vệ an toàn thông tin cho các tổ chức và doanh nghiệp hiệu quả.

Intrusion Detection System



Hình 1: IDS là gì?

Chức năng chính của IDS

Hệ thống này có nhiệm vụ giám sát và phát hiện các hành vi xâm nhập hoặc bất thường trong hệ thống mạng. Các chức năng chính bao gồm:

- Giám sát luồng dữ liệu mạng
- Phát hiện các mẫu tấn công
- Ghi lại và báo cáo
- Hỗ trợ phản ứng nhanh

Phân loại IDS

Loại	Tổng quan
Network-based Intrusion Detection System (NIDS) là gì	Là hệ thống phát hiện xâm nhập mạng. NIDS giám sát và phân tích lưu lượng mạng để phát hiện các hoạt động xâm nhập hoặc bất thường trên mạng.

Host-based Intrusion Detection System (HIDS)	Là hệ thống phát hiện xâm nhập trên máy chủ hoặc thiết bị cuối. HIDS giám sát và phân tích hoạt động của một máy chủ hoặc thiết bị đơn lẻ để phát hiện các hoạt động xâm nhập hoặc bất thường trên máy chủ.
--	---

b. IPS

IPS là gì?

IPS là một giải pháp bảo vệ tích cực nhằm ngăn chặn các hoạt động/mô hình độc hại có thể xảy ra, các sự cố bất thường và vi phạm chính sách. Nó có trách nhiệm dừng/ngăn chặn/chấm dứt sự kiện đáng ngờ ngay khi việc phát hiện được thực hiện.

Chức năng chính của IPS

Chức năng chính của IPS phát hiện và ngăn chặn các hành vi không mong muốn hoặc xâm nhập vào hệ thống.

Phân loại IPS

Loại	Tổng quan
Network Intrusion Prevention System (NIPS)	NIPS giám sát luồng lưu lượng từ các khu vực khác nhau của mạng. Mục đích là để bảo vệ lưu lượng trên toàn bộ mạng con. Nếu chữ ký được xác định, kết nối sẽ bị chấm dứt.
Behaviour-based Intrusion Prevention System or (Network Behaviour Analysis – NBA)	Tương tự NIPS và các hệ thống dựa trên hành vi yêu cầu một khoảng thời gian đào tạo (còn được gọi là “Baselining”) để tìm hiểu lưu lượng truy cập thông thường và phân biệt lưu lượng truy cập độc hại cũng như các mối đe dọa. Mô hình này cung cấp kết quả hiệu quả hơn trước các mối đe dọa mới.
Wireless Intrusion Prevention System (WIPS)	WIPS giám sát luồng lưu lượng từ mạng không dây. Mục đích là để bảo vệ lưu lượng không dây và ngăn chặn các cuộc tấn công có thể xảy ra từ đó.

Host-based Intrusion Prevention System (HIPS)	HIPS tích cực bảo vệ luồng lưu lượng từ một thiết bị đầu cuối duy nhất. Mục đích là để điều tra lưu lượng truy cập trên một thiết bị cụ thể.
--	--

3. Các kỹ thuật thường được sử dụng trong giải pháp IDS, IPS [3]

Signature-based: Kỹ thuật này dựa trên các quy tắc xác định các mẫu cụ thể của hành vi nguy hiểm đã biết. Mô hình này giúp phát hiện các mối đe dọa đã biết.

Behavior-based: Kỹ thuật này xác định các mối đe dọa mới bằng các mẫu mới đi qua chữ ký. Mô hình so sánh các hành vi đã biết/bình thường với các hành vi chưa biết/bất thường. Mô hình này giúp phát hiện các mối đe dọa mới hoặc chưa biết trước đây.

Policy-based: Kỹ thuật này so sánh các hoạt động được phát hiện với cấu hình hệ thống và chính sách bảo mật. Mô hình này giúp phát hiện các hành vi vi phạm chính sách.

II. Các kiểu tấn công mạng và cách phòng chống [4]

1. Khái niệm

Tấn công mạng là quá trình sử dụng các phương pháp, công nghệ hoặc kỹ thuật để xâm nhập, xâm phạm hoặc tạo ra cản trở đối với một hệ thống mạng, thiết bị hoặc ứng dụng. Mục tiêu là lấy cắp thông tin, hủy hoại hệ thống, ...

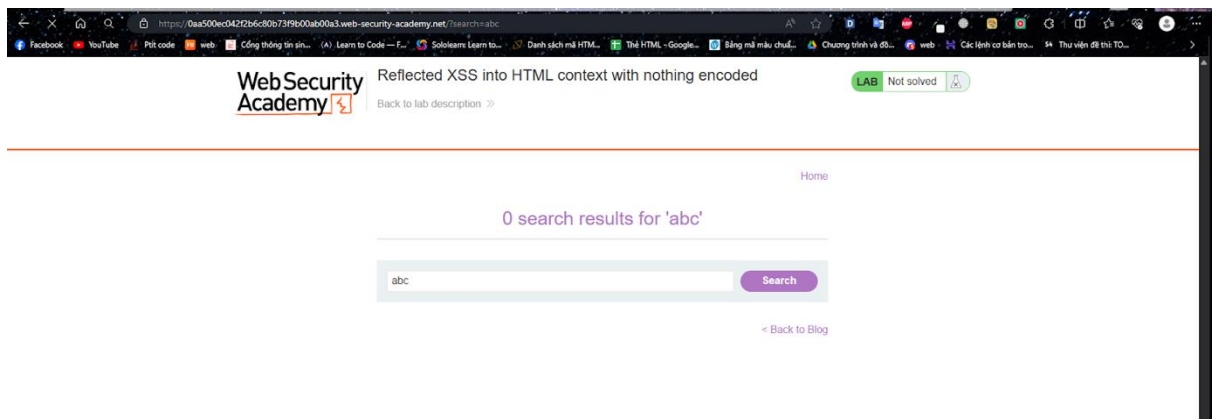
Các phương pháp tấn công mạng phổ biến bao gồm tấn công DDoS, tấn công mã độc, phishing, tấn công kiểm soát qua mạng, ...

2. Các kiểu tấn công

a. XSS [5]

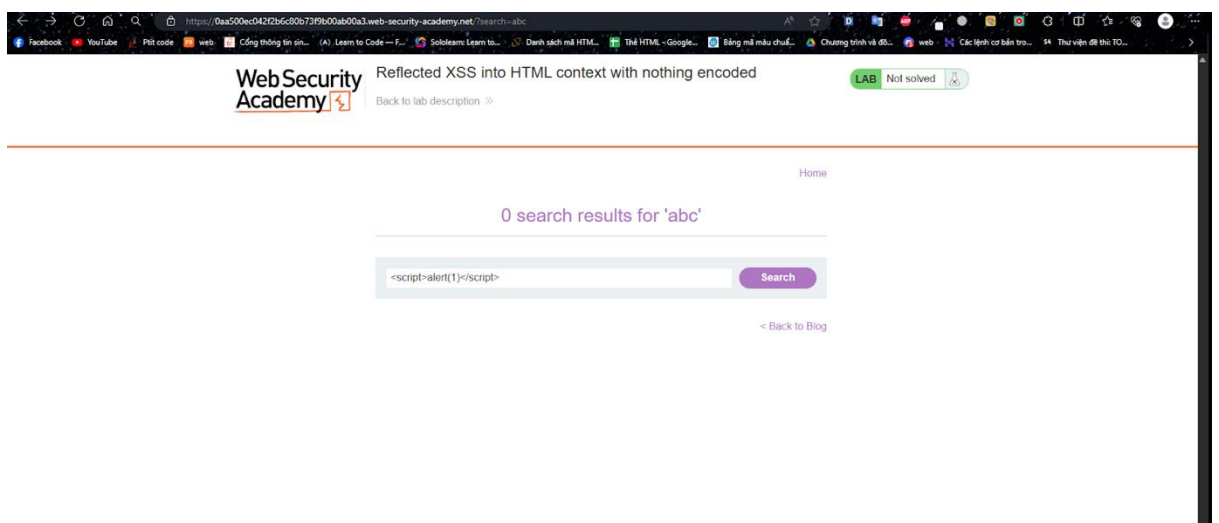
XSS là kiểu tấn công chèn mã độc Script vào các trang web hoặc ứng dụng web khiến cho người dùng cuối thực thi mã Script trong trình duyệt của họ

Ví dụ: Reflected XSS



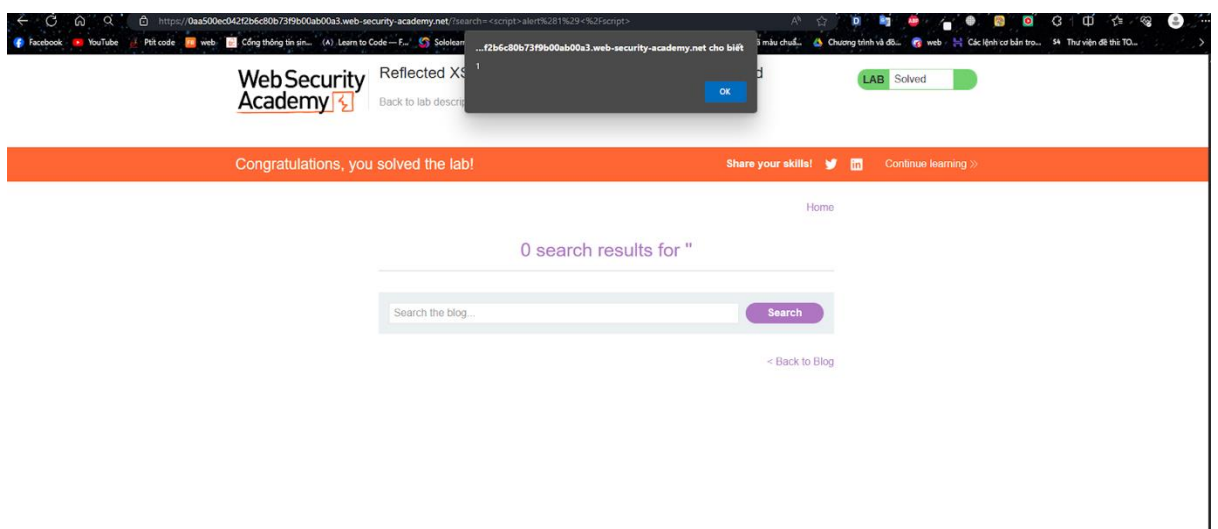
Hình 2: Nhập abc vào và nhấn search

Khi ta nhập abc và ấn search thì ở trên đường link của trang web sẽ có search=abc và ta thay đổi giá trị nhập thành 1 đoạn script



Hình 3: Thay đổi bằng đoạn Script

Thì trang web sẽ xuất hiện 1 bảng thông báo khi ta ấn search



Hình 4: Trang web hiện thông báo

- Cách phòng chống:

- Kiểm tra và escape các tham số của URL trước khi sử dụng.
- Thiết lập CSP để hạn chế các nguồn tài nguyên có thể được tải trên trang web giảm khả năng thực thi mã script độc.
- Thực hiện kiểm tra định dạng người dùng nhập vào.

b. SQL Injection [6]

Là một loại tấn công mà kẻ tấn công chèn các câu lệnh SQL độc hại vào trường dữ liệu của ứng dụng web, từ đó có thể thực thi có các lệnh SQL không mong muốn

Cách phòng chống:

- Sử dụng Prepared Statements hoặc Parameterized Queries: Sử dụng các câu lệnh SQL được chuẩn bị trước hoặc truy vấn có tham số để đảm bảo rằng dữ liệu không được xử lý như một phần của câu lệnh SQL.
- Escape dữ liệu: Nếu không sử dụng Prepared Statements hoặc Parameterized Queries, hãy đảm bảo rằng dữ liệu được "escape" trước khi chèn vào câu lệnh SQL.
- Principle of Least Privilege: Thiết lập quyền truy cập cơ sở dữ liệu sao cho các người dùng chỉ có thể thực hiện các thao tác cần thiết, và không có quyền thực hiện các thao tác đặc quyền.
- Tối ưu hóa cấu hình cơ sở dữ liệu: Tắt tính năng không cần thiết và giảm thiểu mức độ phức tạp của cơ sở dữ liệu để giảm khả năng tấn công SQL Injection.

c. DoS và DDoS [7]

DoS (Denial of Service) là hình thức tấn công dựa trên hình thức đánh sập tạm thời 1 hệ thống mạng bằng cách gửi lượng lớn yêu cầu truy cập đến 1 trang web cụ thể.

Kẻ tấn công sử dụng botnet, 1 mạng lưới các máy tính bị xâm nhập và kiểm soát từ xa để gửi yêu cầu truy cập cùng 1 lúc từ nhiều nguồn khác nhau.

- Cách phòng chống:

- Sử dụng giải pháp bảo mật mạng như bộ tường lửa và hệ thống phát hiện xâm nhập (IDS/IPS) để phát hiện và chặn các lưu lượng tấn công DDoS.
- Sử dụng dịch vụ bảo vệ chống DDoS từ các nhà cung cấp dịch vụ bảo mật mạng (MSSP) để giảm tác động của tấn công DDoS lên hệ thống mạng.

- Tăng cường khả năng chịu tải của hệ thống mạng bằng cách sử dụng công nghệ tải cân bằng tải (load balancing) và kỹ thuật phân tán lưu lượng (traffic engineering).

d. Brute Force

Brute Force Attack là hình thức tấn công mạng, trong đó tin tặc sử dụng phần mềm để “trộn” các ký tự khác nhau thành mật khẩu hợp lệ. Lúc này, chúng sẽ gửi các truy vấn đăng nhập vào file wp-login.php và thử mật khẩu. Quá trình này sẽ diễn ra liên tục cho đến khi tin tặc có thể đăng nhập thành công. Việc bẻ khóa mật khẩu này có thể mất từ vài giây cho đến vài ngày hay lâu hơn là vài tháng, tùy vào mức độ phức tạp của mật khẩu. Nhìn chung, mục đích chính của hình thức tấn công Brute Force Attack là để tìm ra mật khẩu và tài khoản của người quản trị cao nhất.

- Có 6 loại Brute Force Attack phổ biến hiện nay:
 - Simple Brute Force Attack: Loại này sẽ sử dụng cách tiếp cận có hệ thống để “đoán” username hay password mà không cần dựa vào external logic.
 - Hybrid Brute Force Attack: Dựa vào external logic nó có thể xác định các tổ hợp password có khả năng thành công cao nhất. Sau đó, nó tiếp tục tiếp cận với Simple Brute Force Attack để thử nhiều tổ hợp nhất có thể.
 - Dictionary Attack: Đây là loại sử dụng một từ điển các xâu hay cụm từ khả thi để đoán username và password của người dùng.
 - Rainbow Table Attack: Loại này là một bảng được tính toán trước để so khớp với kết quả của các hàm hash. Nó có thể dùng để đoán một hàm có độ dài xác định và chứa một tập hợp các ký tự cụ thể.
 - Reverse Brute Force Attack: Loại tấn công này sử dụng một password chung hay một tập hợp các password để thử với nhiều username khả thi. Nó sẽ nhắm vào một mạng người dùng mà các hacker đã đánh cắp được dữ liệu trước đó.
- Credential Snuffing: Đây là loại tấn công sử dụng các cặp password và username đã biết trước, và thử chúng trên nhiều trang web khác nhau. Bởi lẽ, hiện nay có không ít người dùng có thói quen sử dụng cùng một cặp password và username trên nhiều hệ thống trang web khác nhau.
- Cách phòng chống:

- Đặt mật khẩu có tính bảo mật cao
- Nên thay đổi mật khẩu thường xuyên
- Giới hạn số lần đăng nhập thất bại
- Đối với người thiết kế hệ thống nên mã hóa mật khẩu lưu xuống CSDL

CƠ SỞ LÝ THUYẾT

III. SNORT

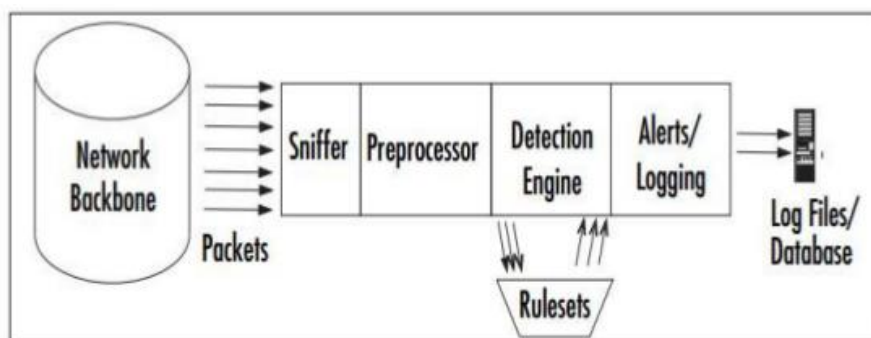
1. Giới thiệu SNORT [8] [9]

SNORT là hệ thống IDS/IPS thuộc dạng NIDS được phát triển bởi Martin Roesh dưới dạng mã nguồn mở hoàn toàn miễn phí. Snort ban đầu được xây dựng trên nền Unix nhưng sau đó phát triển sang các nền tảng khác. Snort được đánh giá cao về khả năng phát hiện xâm nhập. Kiến trúc thiết kế của Snort được thiết kế theo kiểu module, tức là người dùng hoàn toàn có thể thêm cho hệ thống Snort của mình bằng việc cài đặt hoặc viết thêm mới vào các module.

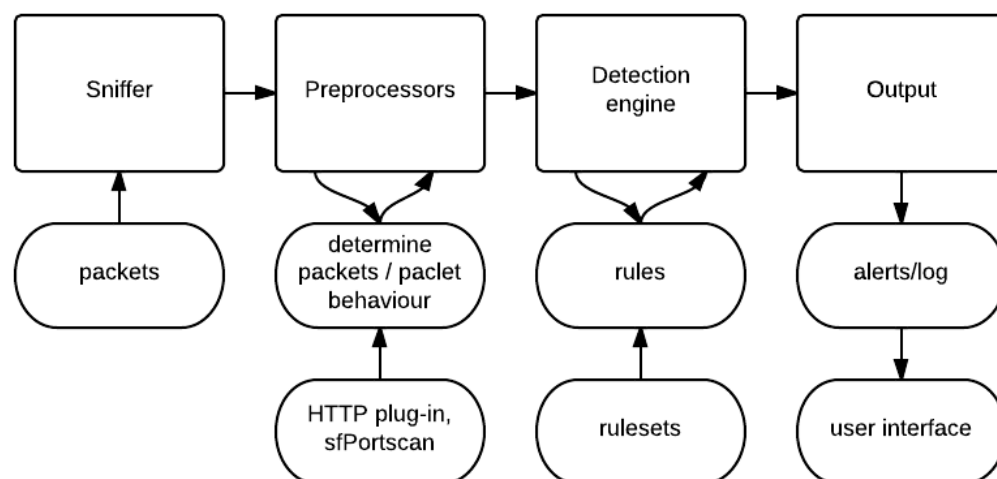
2. Kiến trúc của SNORT

Kiến trúc của Snort gồm nhiều phần, mỗi phần có các chức năng khác nhau, gọi là module:

- Module giải mã gói tin (Packet Decoder).
- Module tiền xử lý (Preprocessor).
- Module phát hiện (Detection Engine).
- Module log và cảnh báo (Logging and Alerting System).
- Module kết xuất thông tin (Output Modules).



Hình 5: Kiến trúc của Snort (1)



Hình 6: Kiến trúc của Snort (2)

Trong quá trình hoạt động, Snort sẽ giám sát tất cả các gói tin di chuyển qua nó. Tất cả các gói tin sau khi bị bắt sẽ được đưa vào module giải mã. Tiếp theo sẽ vào module tiền xử lý và đưa qua module phát hiện. Tại đây, tùy thuộc vào các gói tin có bị phát hiện xâm nhập hay không mà các gói tin có thể bỏ qua để lưu thông tin hoặc đưa vào module log và cảnh báo để xử lý, module kết xuất thông tin sẽ thực hiện việc đưa ra cảnh báo theo đúng định dạng mong muốn.

- Chức năng cụ thể của từng thành phần:
 - **Module giải mã gói:** bộ giải mã gói tin của Snort hỗ trợ các phương tiện Ethernet, SLIP và PPP. Snort dùng thư viện pcap để thực hiện bắt tất cả gói tin trên mạng lưu thông qua hệ thống. Nhiệm vụ của bộ giải mã là phân tích các gói dữ liệu thô bắt được trên mạng và khôi phục chúng thành các gói dữ liệu hoàn chỉnh ở lớp ứng dụng và làm đầu vào cho hệ thống phát hiện. Các gói tin sau khi giải mã sẽ được đưa sang bộ tiền xử lý.
 - **Module tiền xử lý:** Bộ tiền xử lý này rất quan trọng đối với bất kỳ hệ thống nào để có thể chuẩn bị gói dữ liệu đưa vào cho bộ phát hiện gói tin. Bộ tiền xử lý thực hiện 3 chức năng sau:
 - Kết hợp các gói tin: Khi dữ liệu lớn được gửi đi, thông tin sẽ không đóng gói toàn bộ vào một gói mà thực hiện phân mảnh, chia thành nhiều gói tin rồi gửi đi. Khi Snort nhận được các gói tin này, nó phải thực hiện kết nối lại để có gói tin ban đầu. Bộ tiền xử lý giúp Snort có thể hiểu được các phiên làm việc khác nhau.
 - Giải mã và chuẩn hóa giao thức (Decode/normalize): Công việc phát hiện xâm nhập dựa trên dấu hiệu nhận dạng thường xuyên thất bại khi kiểm tra các giao thức có dữ liệu có thể được biểu diễn dưới nhiều dạng khác nhau. Ví dụ: Một Web server có thể nhận nhiều dạng URL: URL viết dưới dạng hexa/Unicode hay URL

chấp nhận / hay \. Nếu Snort chỉ thực hiện đơn thuần việc so sánh dữ liệu với dấu hiệu nhận dạng sẽ xảy ra tình trạng bỏ sót hành vi xâm nhập. Do vậy, một số module tiền xử lý của Snort phải có nhiều vụ giải mã và chỉnh sửa, sắp xếp lại các thông tin đầu vào.

- Phát hiện các xâm nhập bất thường (nonruled/anormal: Các plugin dạng này thường xử lý với các xâm nhập không thể hoặc rất khó phát hiện bằng các luật thông thường. Phiên bản hiện tại của Snort có đi kèm 2 plugin giúp phát hiện xâm nhập bất thường đó là portscan và bo (backoffice). Portscan dùng để đưa ra cảnh báo khi kẻ tấn công thực hiện quét cổng để tìm lỗ hổng. Bo dùng để đưa ra cảnh báo hệ thống nhiễm trojan backoffice.
- **Module phát hiện:** Đây là module quan trọng nhất của Snort. Nó chịu trách nhiệm phát hiện các dấu hiệu xâm nhập. Module phát hiện sử dụng các luật (rules) được định nghĩa trước để so sánh với dữ liệu thu thập được, từ đó xác định xem có xâm nhập xảy ra hay không. Module phát hiện có khả năng tách các phần của gói tin và áp dụng luật lên từng phần của gói tin như là IP header; Header ở tầng transport: TCP, UDP; Header ở tầng application: DNS, HTTP, FTP, ...; Phần tải của gói tin. Do các luật trong Snort được đánh số thứ tự ưu tiên nên một gói tin khi bị phát hiện bởi nhiều luật khác nhau, cảnh báo được đưa ra theo luật có mức ưu tiên cao nhất. Các thành phần chính của module phát hiện là các module plugin như module quét cổng, các module plugin nâng cấp chức năng của Snort bằng cách thêm vào khả năng phân tích. Một vấn đề quan trọng đối với module phát hiện là vấn đề thời gian xử lý gói tin: một IDS thường nhận rất nhiều gói tin và bản thân nó cũng có rất nhiều luật xử lý. Khi lưu lượng mạng quá lớn, có thể xảy ra việc bỏ sót hoặc không phản hồi đúng lúc. Khả năng xử lý của nó phụ thuộc vào nhiều yếu tố: số lượng các luật, tốc độ hệ thống, băng thông mạng, ...
- **Module log và cảnh báo (Logger / Alerter):** Ghi nhật ký và cảnh báo là hai thành phần con riêng biệt. Ghi nhật ký cho phép người dùng ghi lại thông tin được bộ giải mã gói tin thu thập ở định dạng con người có thể đọc được hoặc tcpdump. Cảnh báo được cấu hình bởi người dùng, có thể cấu hình cảnh báo gửi đến nhật ký hệ thống, tệp phẳng, ổ cứng UNIX hoặc cơ sở dữ liệu. Tùy theo tùy chọn, người dùng có thể tắt hoàn toàn cảnh báo trong quá trình thử nghiệm hoặc nghiên cứu xâm nhập. Theo mặc định, tất cả nhật ký được ghi trong thư mục /var/log/Snort và tất cả các cảnh báo được ghi vào tệp /var/log/Snort/alerts.
- **Module kết xuất thông tin:** Module này thực hiện các thao tác tùy thuộc vào việc cấu hình lưu kết quả xuất ra như thế nào.
 - Ghi log file
 - Ghi syslog

- Ghi cảnh báo vào cơ sở dữ liệu
- Tạo file log XML
- Cấu hình lại Router, Firewall
- Gửi các cảnh báo được gói trong gói tin sử dụng giao thức SNMP

IV. SNORT'S RULES

Một trong những chức năng được đánh giá cao nhất của Snort là cho phép người sử dụng tự viết các rule của chính mình. Ngoài số lượng các rule đi kèm với Snort, người quản trị có thể vận dụng khả năng của mình để phát triển ra các rule riêng thay vì phụ thuộc vào các cơ quan, tổ chức bên ngoài.

1. Cấu trúc:

Rule Header: chứa thông tin về hành động mà luật đó sẽ thực hiện khi phát hiện ra có xâm nhập nằm trong gói tin và nó cũng chứa tiêu chuẩn để áp dụng luật với gói tin đó.

Rule Option: chứa thông điệp cảnh báo và các thông tin về các phần của gói tin dùng để tạo nên cảnh báo. Phần Option chứa các tiêu chuẩn phụ thêm để đối sánh với gói tin.

2. Rule Header

Rule header chứa thông tin để xác định một packet cũng như tất cả những gì cần thực hiện với tất cả các thuộc tính chỉ định trong rule. Rule header bao gồm những phần sau: Rule actions, protocol, IP address, port number, Direction operator.

a. Rule Action (5 basic action)

Alert -> Tạo cảnh báo khi bắt được gói tin đáng ngờ.

Block -> Khóa gói tin hiện tại và tất cả gói tin tiếp theo trong luồng.

Drop -> Bỏ gói tin ngay khi được cảnh báo.

Log -> Ghi lại thông tin ngay khi được cảnh báo.

Pass -> Bỏ qua gói tin đáng ngờ và đánh dấu thông qua.

b. Protocol (IP, ICMP, UDP, TCP)

c. Source/Destination IP (IP address)

Chỉ đến địa chỉ IP cần áp dụng rule

- 4 cách khai báo:
 - Numeric IP addresss (e.g., 192.168.0.5, 192.168.1.0/24)
 - Variable defined in Snort (e.g., \$EXTERNAL_NET, \$HOME_NET)
 - Keyword: any

- List of IP address (e.g., [192.168.1.0/24,10.1.1.0/24])

d. Port (Direction of traffic)

Cách khai báo:

Any -> any

Static port (e.g., 80, 445, 21)

Variable defined in Snort (e.g., \$HTTP_PORTS)

Range operator (e.g., 1:1024, 500:)

A list port (e.g., [1:1024,4444,5555, \$HTTP_PORTS])

e. Điều hướng (Direction Operator)

“->”: được sử dụng nhiều nhất

IP và port bên trái là của source

IP và port bên phải là của đích

VD: **alert** **tcp** \$EXTERNAL_NET 80 -> \$HOME_NET any (

“<>”: Là toán tử 2 chiều, nó coi IP cả 2 về như nguồn hoặc đích

VD: **log** **tcp** !192.168.1.0/24 any <> 192.168.1.0/24 23 (

3. Rule Options

Là trung tâm phát hiện, chứa dấu hiệu phát hiện xâm nhập và là trái tim chính của Snort. Phần Option nằm ngay sau phần Header và được bao bọc trong dấu ngoặc đơn. Nếu có nhiều option thì sẽ phân biệt nhau bởi dấu “;”. Một option gồm 2 phần: một từ khóa và một tham số, 2 phần này sẽ phân cách nhau bằng dấu hai chấm.

a. 4 loại:

- General
 - Cung cấp thông tin về rule nhưng không gây ra bất kì ảnh hưởng nào đến quá trình phát hiện packet
- Payload
 - Tìm kiếm thông tin trong phần Payload của packet
 - Gồm các từ khóa như: content, nocase, rawbytes, depth, offset, distance, within, http client body, http cookie,...
- Non-Payload
 - Tìm kiếm thông tin trong phần Non-payload của packet
 - Gồm các từ khóa như: frag, offset, ttl, tos, id, ipotps, fragbits,...
- Post-detection
 - Xảy ra khi 1 rule được kích hoạt
 - Gồm các từ khóa: logto, session, resp, react, tag, activated hy, count

b. Rule Option syntax Key

Chữ in nghiêng: thay thế bằng 1 giá trị khác phù hợp

VD: food *food* -> food pizza

Ngoặc vuông: []: Tạo tùy chọn (có thể không chọn)

VD: [pizza|cookies] -> có thể chọn 1 trong 2 hoặc không

[, nocase] -> Người viết tùy ý thêm

Ngoặc nhọn: {}: Tạo tùy chọn bắt buộc

VD: {pizza|cookies} -> phải chọn 1 trong 2

Dấu 3 chấm: ...: Áp dụng cho toàn bộ nhóm như trong [], {}, ...

VD: food *food* [, *food*] ... -> người viết sẽ thay *food* [, *food*] bằng những items được cách nhau bằng dấu phẩy -> food pizza, cake, bacon

V. Cơ chế hoạt động của Plugin SNORTSAM [10] [11]

Để trở Snort trở thành một hệ thống ngăn chặn xâm nhập (IPS), một phần mềm do 1 bên thứ 3 phát triển là SnortSam, đây là 1 plugin của Snort sẽ hỗ trợ việc block các IP do Snort phát hiện là đang thực hiện hành vi trái phép đối với hệ thống.

SnortSam sẽ giúp Snort gửi thông tin tương tác với Firewall để chặn các IP tấn công, hiện đang hỗ trợ các Firewall: Iptables, Checkpoint Firewall-1, CISCO ASA, PIX, Netscreen...

SnortSam bao gồm hai phần riêng biệt:

Một phần là một tập hợp của các sửa đổi trong tập tin mã nguồn, mở rộng Snort bằng cách thêm một mô-đun mới đó là: alert_fwsam

Hai là một tác nhân sẽ giao tiếp trực tiếp với tường lửa gọi là agent. Tác nhân này có thể đặt ngay trên chính tường lửa nếu tường lửa đó là iptables, hoặc trên pf nếu hệ thống là BDS hoặc trên Checkpoint's Firewall-1 nếu hệ thống đó là Windows. Đối với các tường lửa phần cứng như Cisco PIX thì tác nhân này của SnortSam phải đặt trên một máy riêng biệt dành riêng để giao tiếp với PIX.

Phương thức hoạt động: Snort sẽ giám sát các luồng lưu lượng trên mạng, và khi một luật của Snort được kích hoạt hay một chữ ký xảy ra (gặp một traffic phù hợp), Snort sẽ gửi đầu ra cho mô-đun fwsam (hay cho SnortSam). Mô-đun fwsam sau đó sẽ gửi một tin nhắn mã hóa tới cho agent được đặt trên tường lửa. Agent này sẽ kiểm tra xem tin nhắn đó có phải được gửi tới từ một nguồn có thẩm quyền hay không, nếu đúng nó sẽ giải mã thông điệp vừa nhận được và kiểm tra xem các địa chỉ IP nào được yêu cầu chặn. SnortSam sẽ rà soát xem các địa chỉ đó có nằm trong danh sách trắng (white-list) hay không. Nếu IP đó không nằm trong danh sách trắng,

SnortSam sẽ yêu cầu tường lửa chặn địa chỉ IP đó trong một khoảng thời gian đã được định nghĩa từ trước. Cơ chế này giúp tăng cường an ninh mạng bằng cách phản ứng nhanh chóng với các mối đe dọa và ngăn chặn chúng trước khi chúng gây hại cho hệ thống.

CÀI ĐẶT HỆ THỐNG

VI. Cài đặt SNORT, thiết lập rules

1. Cài đặt Snort

- Tiến hành cài đặt các thư viện tiên quyết: *build-essential, autotools-dev, libdumbnet-dev, liblua5.1-dev, libpcap-dev, zlib1g-dev, pkg-config, libhwloc-dev, cmake liblzma-dev, openssl libssl-dev, cpputest libsqlite3-dev, libtool, uuid-dev, git, autoconf, bison, flex, libcmocka-dev, libnetfilter-queue-dev, libunwind-dev, libmnl-dev, ethtool, libjemalloc-dev.*

```
quangkha@quangkha-virtual-machine:~$ sudo apt-get install -y build-essential autotools-dev libdumbnet-dev liblua5.1-dev libpcap-dev zlib1g-dev pkg-config libhwloc-dev cmake liblzma-dev openssl libssl-dev cpputest libsqlite3-dev libtool uuid-dev git autoconf bison flex libcmocka-dev libnetfilter-queue-dev libunwind-dev libmnl-dev ethtool libjemalloc-dev
```

Hình 7: Tiến hành cài đặt các thư viện

- Tải và tiến hành giải nén các gói: *pcre, gperftools, Rangel, Hyperscan, flatbuffers, Data Acquisition (DAQ) from Snort, Boost C++ Libraries.*

Ví dụ cài đặt pcre:

```
quangkha@quangkha-virtual-machine:~/snort$ wget https://sourceforge.net/projects/pcr/files/pcr/8.45/pcr-8.45.tar.gz
--2024-03-28 10:54:56-- https://sourceforge.net/projects/pcr/files/pcr/8.45/pcr-8.45.tar.gz
Resolving sourceforge.net (sourceforge.net)... 172.64.150.145, 104.18.37.111, 2606:4700:4400::6812:256f, ...
Connecting to sourceforge.net (sourceforge.net)|172.64.150.145|:443... connected
.
```

Hình 8: Tải và giải nén các gói (1)

```
quangkha@quangkha-virtual-machine:~/snort$ tar -xzf pcr-8.45.tar.gz

quangkha@quangkha-virtual-machine:~/snort$ cd pcr-8.45/
quangkha@quangkha-virtual-machine:~/snort/pcr-8.45$ ./configure
checking for a BSD-compatible install... /usr/bin/install -c
checking whether build environment is sane... yes
checking for a race-free mkdir -p... /usr/bin/mkdir -p
checking for gawk... no
checking for mawk... mawk
checking whether make sets $(MAKE)... yes
checking whether make supports nested variables... yes
checking whether make supports nested variables... (cached) yes
```

Hình 9: Tải và giải nén các gói (2)

```
checking whether make supports nested variables... no
Code coverage ..... : no

quangkha@quangkha-virtual-machine:~/snort/pcr-8.45$ make
rm -f pcr_chartables.c
ln -s ./pcr_chartables.c.dist pcr_chartables.c
make all-am
make[1]: Entering directory '/home/quangkha/snort/pcr-8.45'
CC      pcretest-pcretest.o
CC      pcretest-pcre printint.o
```

Hình 10: Tải và giải nén các gói (3)

```
quangkha@quangkha-virtual-machine:~/snort/pcr-8.45$ sudo make install
[sudo] password for quangkha:
make install-am
make[1]: Entering directory '/home/quangkha/snort/pcr-8.45'
CC      libpcr_la-pcr_study.lo
CC      libpcr_la-pcr_tables.lo
CC      libpcr_la-pcr_ucd.lo
```

Hình 11: Tải và giải nén các gói (4)

Libraries	Source
Pcre	https://sourceforge.net/projects/pcre/files/pcre/8.45/pcre-8.45.tar.gz
Gperftools	https://github.com/gperftools/gperftools/releases/download/gperftools-2.9.1/gperftools-2.9.1.tar.gz
Rangel	http://www.colm.net/files/rangel/rangel-6.10.tar.gz
Hyperscan	https://github.com/intel/hyperscan/archive/refs/tags/v5.4.2.tar.gz
Flatbuffer	https://github.com/google/flatbuffers/archive/refs/tags/v2.0.0.tar.gz
DAQ	https://github.com/snort3/libdaq/archive/refs/tags/v3.0.13.tar.gz
Boost C++ Libraries	https://boostorg.jfrog.io/artifactory/main/release/1.77.0/source/boost_1_77_0.tar.gz

- Cập nhật các thư viện chia sẻ: `sudo ldconfig`

```
quangkha@quangkha-virtual-machine:~/snort$ sudo ldconfig
quangkha@quangkha-virtual-machine:~/snort$
```

Hình 12: Cập nhật các thư viện chia sẻ

- Cài đặt phiên bản Snort3 gần nhất:

Tải mã nguồn từ Github	\$wget https://github.com/snort3/snort3/archive/refs/tags/3.1.74.0.tar.gz -O snort3-3.1.74.0.tar.gz
Giải nén	\$tar -xzf snort3-3.1.74.0.tar.gz
Điều hướng đến thư mục snort3-3.1.74.0	\$cd snort3-3.1.74.0

Cấu hình Cmake	<code>\$/./configure_cmake.sh --prefix=/usr/local --enable-tcmalloc</code>
Điều hướng tới thư mục build	<code>\$cd build</code>
Biên dịch	<code>\$make</code>
Cài đặt Snort3	<code>\$sudo make install</code>

```

quangkha@quangkha-virtual-machine:~/snort$ snort -V

  _,-
 o" )~
  '""

ved.

-*> Snort++ <*-
Version 3.1.74.0
By Martin Roesch & The Snort Team
http://snort.org/contact#team
Copyright (C) 2014-2023 Cisco and/or its affiliates. All rights reserved.

Copyright (C) 1998-2013 Sourcefire, Inc., et al.
Using DAQ version 3.0.13
Using LuaJIT version 2.1.0-beta3
Using OpenSSL 3.0.2 15 Mar 2022
Using libpcap version 1.10.1 (with TPACKET_V3)
Using PCRE version 8.45 2021-06-15
Using ZLIB version 1.2.11
Using Hyperscan version 5.4.2 2024-03-13
Using LZMA version 5.2.5

quangkha@quangkha-virtual-machine:~/snort$

```

Hình 13: Cài đặt Snort 3 thành công

Để Snort3 có thể chạy như một dịch vụ bình thường, ta vô hiệu hóa LRO & GRO bằng dịch vụ, sau đó thực hiện các thao tác:

- `$sudo nano /lib/systemd/system/ethtool.service`

```

quangkha@quangkha-virtual-machine: ~/snort
quangkha@quangkha-virtual-machine: /... x  quangkha@quangkha-virtual-machine: ~... x
GNU nano 6.2 /lib/systemd/system/ethtool.service
[Unit]
Description=Ethtool Configuration for Network Interface
[Service]
Requires=network.target
Type=oneshot
ExecStart=/sbin/ethtool -K ens3 gro off
ExecStart=/sbin/ethtool -K ens3 lro off
[Install]
WantedBy=multi-user.target

Read 9 lines
^G Help      ^O Write Out ^W Where Is  ^K Cut       ^T Execute  ^C Location
^X Exit      ^R Read File ^\ Replace   ^U Paste     ^J Justify  ^_ Go To Line

```

Hình 14: Vô hiệu hóa LRO & GRO

- \$sudo systemctl enable ethtool
- **Restart lại service:** \$sudo service ethtool start

```
quangkha@quangkha-virtual-machine:~/snort$ sudo ethtool -k ens33 | grep receive-
offload
generic-receive-offload: off
large-receive-offload: off [fixed]
quangkha@quangkha-virtual-machine:~/snort$
```

Hình 15: LRO & GRO đã bị vô hiệu hóa

2. Thiết lập rules

- **Tạo thư mục rules:**

```
$sudo mkdir /usr/local/etc/rules
```

- **Tạo file local.rules:**

```
$sudo nano /usr/local/etc/rules/local.rules
```

Nội dung file: alert icmp nay nay -> any any (msg:"Phat hien ICMP";
sid:1000001;)

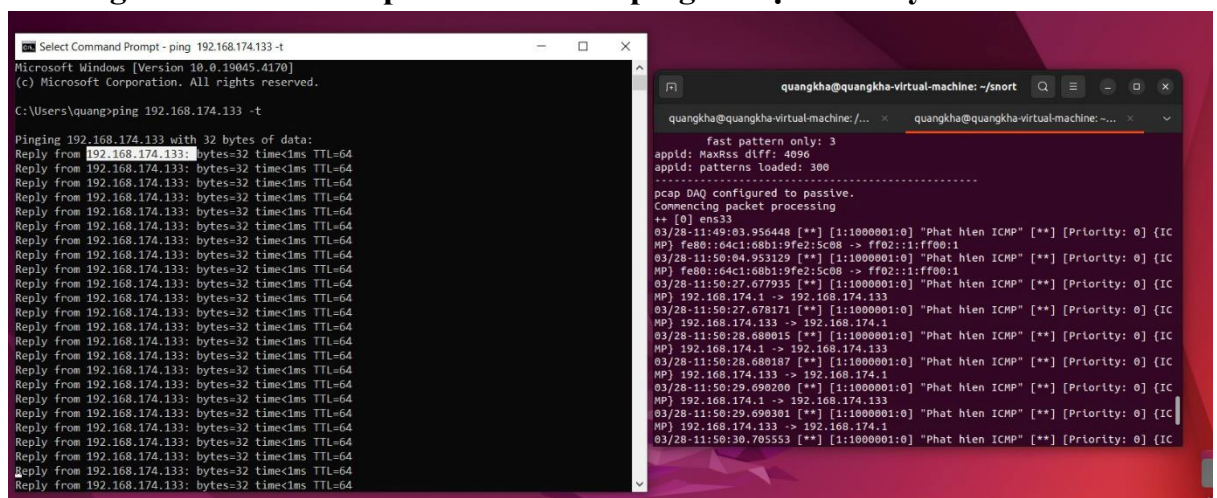
- **Cấu hình Snort3 nhận rules từ local.rules:**

```
$snort -c /usr/local/etc/snort/snort.lua -R /usr/local/etc/rules/local.rules
```

- **Khởi chạy Snort3:**

```
$sudo snort -c /usr/etc/snort/snort.lua --plugin-path/usr/local/etc/so_rules/ -i
ens33 -A alert_fast
```

- **Dùng Command Prompt của Windows ping tới địa chỉ máy ảo Ubuntu**



Hình 16: Snort3 đã phát hiện ICMP

- **Đọc hiểu thông báo:**

03/28-11:51:54.662604 [**] [1:1000001:0] "Phat hien ICMP" [**]
[Priority: 0] {ICMP} 192.168.174.1 -> 192.168.174.133

Đỏ: thời điểm bắt sự kiện

Xanh lam: sid sự kiện

Xanh lục: thông điệp sự kiện

Đen: độ ưu tiên

Nâu: giao thức sự kiện

Tím: IP nguồn

Hồng: IP đích

VII. Mô hình mạng

1. Mô hình mạng



Hình 17: Mô hình mạng

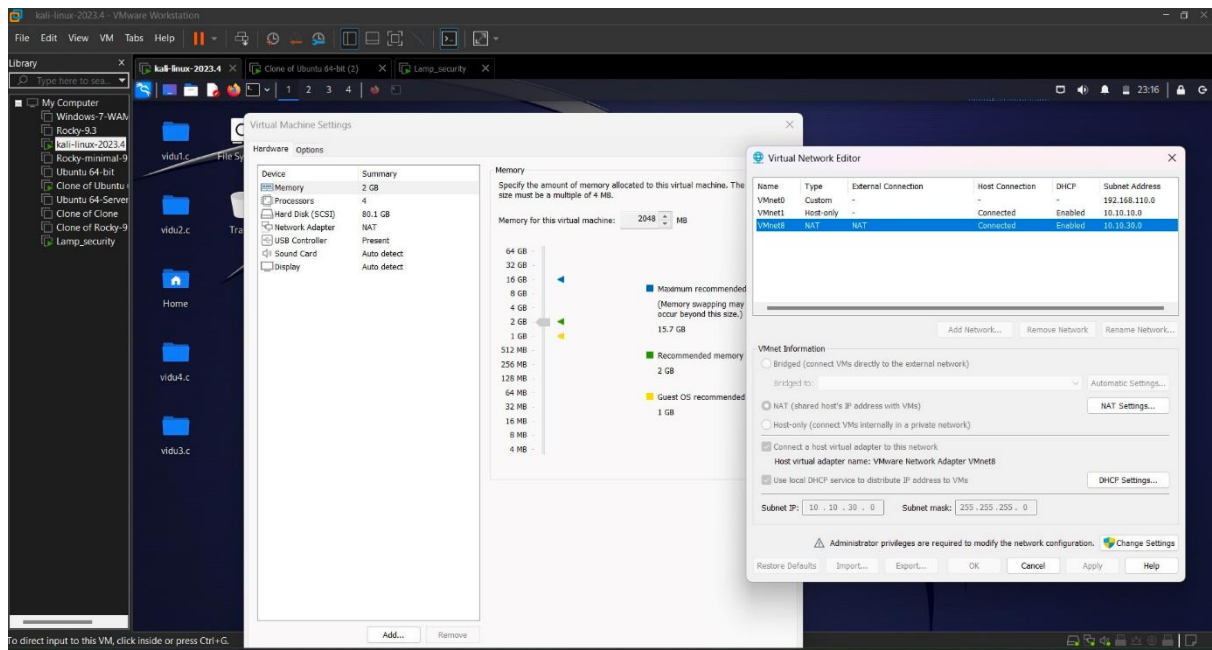
Mô tả kịch bản:

- Sử dụng một máy attacker chạy hệ điều hành Kali Linux (có các công cụ tấn công vào mạng) để tấn công vào một máy web server.
- Khi ấy chúng ta dùng máy IDS/IPS đưa tập luật đã xây dựng vào Snort để phát hiện có vụ tấn công mạng vào Server và ngăn chặn địa chỉ IP của máy Attacker.

Máy Attacker:

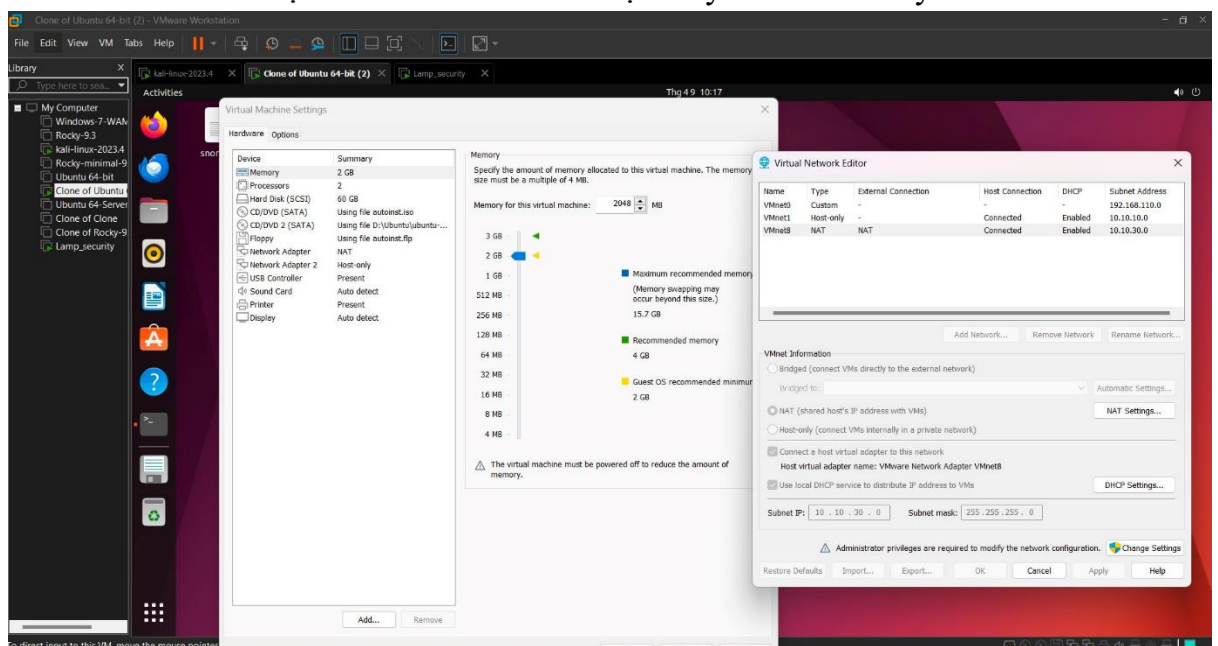
- Sử dụng hệ điều hành Kali Linux.
- Có 1 card mạng eth0 địa chỉ IP 10.10.30.130/24, gateway 10.10.30.129 kết nối trực tiếp với card mạng ens33 của máy IDS/IPS server.

- Máy Attacker sử dụng các công cụ tấn công để tấn công vào máy WEB server.



Máy IDS/IPS:

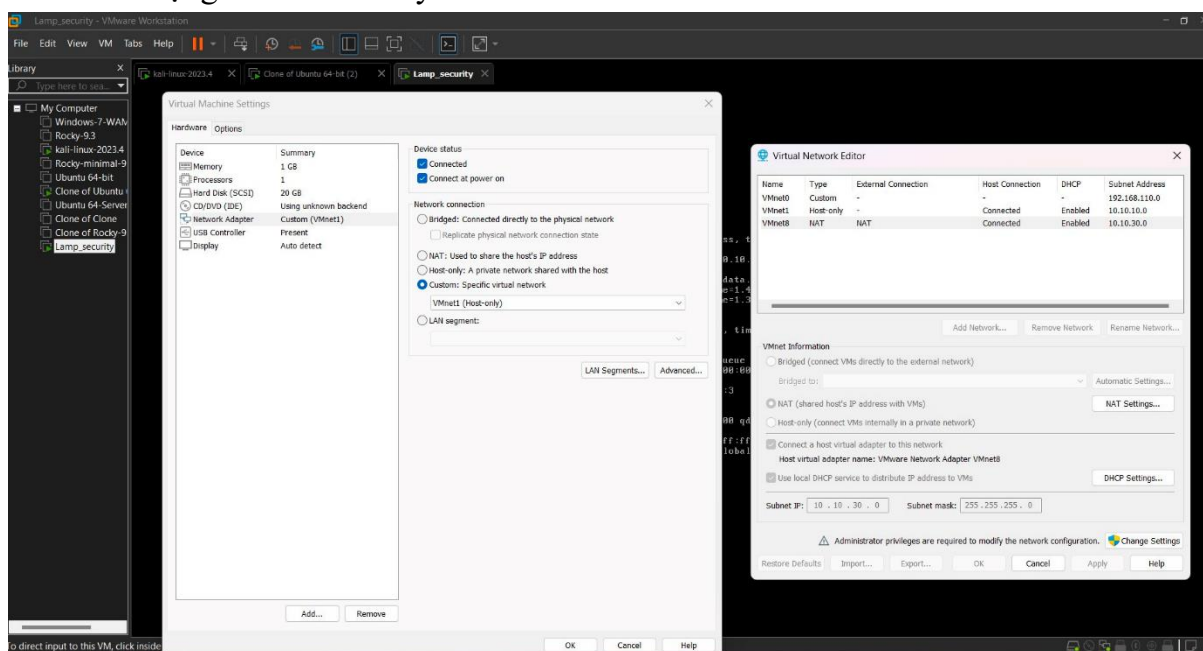
- Sử dụng hệ điều hành Ubuntu.
- Cài đặt Snort/SnortSam làm IDS, IPS.
- Cài đặt Iptables là Firewall.
- Card ens33 có địa chỉ IP 10.10.30.129/24 để máy Attacker định tuyến qua.
- Card ens33 có địa chỉ 10.10.10.129/24 định tuyến sau với máy WEB server.



Hình 19: Cấu hình của máy IDS/IPS

Máy WEB Server:

- Sử dụng hệ điều hành CentOS Linux.
- Có 1 card mạng eth4 IP 10.10.10.130/24, gateway 10.10.10.129 định tuyến với card mạng ens37 của máy IDS/IPS server.



Hình 20: Cấu hình của máy WEB Server

2. Cấu hình các phụ thuộc

2.1. Snort rules

- *Phát hiện DOS Attack:*
alert tcp any any -> any any (msg:"Phat hien DOS Attack"; flow:to_server; detection_filter:track by_src, count 500, seconds 5; sid: 1000001; rev: 004;)
- *Phát hiện XSS Attack:*
alert tcp any any -> any any (msg:"Attack XSS"; flow:to_server; pcre:"/((\%3C)|<)((\%2F)|\/)*[a-z0-9\%]+((\%3E)|>)/"; classtype:web-pplication-attack; sid:1000002; rev:5;)
- *Phát hiện SQL Injection:*
alert tcp any any -> any 80 (msg:"SQL Injection Attempt detected (OR operator)"; flow:to_server; content:"GET"; http_method; content:"or"; pcre:"\\Wor\\W/i"; sid:1000003;)
- *Phát hiện Brute Force:*
alert tcp 10.10.10.0/24 22 -> any any (msg:"thong bao Attack Brute Force"; sid:1000004;)

2.2. Cài đặt Web Server

2.2.1. Cài đặt Web Server:

- Cài đặt Web Server với công cụ LAMP (Linux, Apache, MySQL, và ngôn ngữ PHP hay Perl hay Python) để tạo nên một môi trường máy chủ Web có khả năng chứa và phân phối các trang website động.
- Thiết lập khả năng cung cấp các gói sau này:

`rpm --import /etc/pki/rpm-gpg/RPM-GPG-KEY*`

`yum -y install epel-release`

- Là một dự án repository từ Fedora team cung cấp nhiều gói add-on package mà chúng ta thường dùng cho các bản Linux. Repo này được tạo và duy trì bởi một người Pháp tên là Remi Collect.

2.2.2. Cài đặt các công cụ trong LAMP:

a. Cài đặt Apache2:

- `dnf -y update`
- `dnf install epel-release`
- `dnf install httpd mod_ssl openssl`
- `vim /etc/httpd/conf/httpd.conf`

#Dong 86

ServerAdmin admin@vmware.lab

#Dong 95

ServerName srv.vmware.lab:80

#Dong 164

DirectoryIndex index.html index.php

#Them cuoi cung

ServerTokens Prod

KeepAlive On

- `systemctl restart httpd`
- `vim /etc/httpd/conf.d/vhost.conf`


```
GNU nano 2.8.9 File: vhost.conf

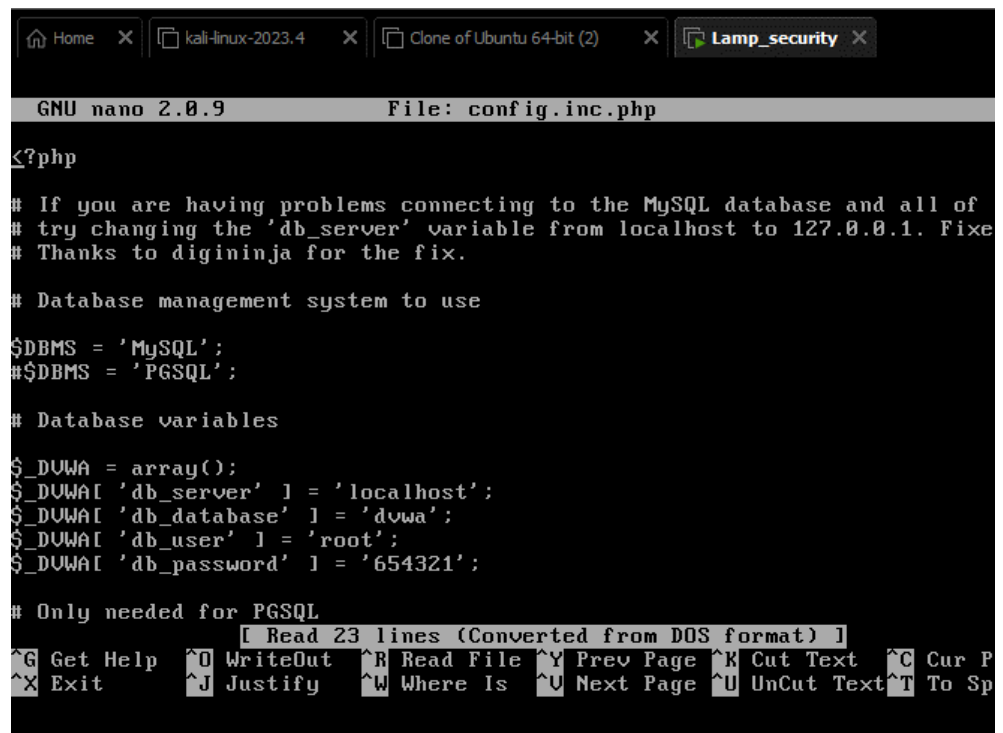
ServerAlias site3.vmware.lab
DocumentRoot /srv/www/site3.vmware.lab/public_html/
ErrorLog /srv/www/site3.vmware.lab/logs/error.log
CustomLog /srv/www/site3.vmware.lab/logs/access.log combined
</VirtualHost>

<VirtualHost *:80>
ServerAdmin site4@vmware.lab
ServerName site4.vmware.lab
ServerAlias site4.vmware.lab
DocumentRoot /srv/www/site4.vmware.lab/public_html/
ErrorLog /srv/www/site4.vmware.lab/logs/error.log
CustomLog /srv/www/site4.vmware.lab/logs/access.log combined
</VirtualHost>

<VirtualHost *:80>
ServerAdmin site5@vmware.lab
ServerName site5.vmware.lab

^G Get Help ^O WriteOut ^R Read File ^Y Prev Page ^K Cut Text ^C Cur P
^X Exit ^J Justify ^W Where Is ^U Next Page ^U UnCut Text ^T To Sp
```

- mkdir -p /srv/www/site4.vmware.lab/public_html
- mkdir -p /srv/www/site4.vmware.lab/logs/
- touch /srv/www/ site4.vmware.lab /virtual.host-error_log
- touch /srv/www/ site4.vmware.lab /virtual.host-access_log combined
- cd /srv/www/
- chown -R apache:apache vmware.lab/
- cd ~
- sudo git clone <https://github.com/digininja/DVWA.git>
- cd DVWA
- mv * /srv/www/site4.vmware.lab/public_html
- cd /srv/www/site4.vmware.lab/public_html
- cp config.inc.php.dist config.inc.php



```
GNU nano 2.0.9 File: config.inc.php
<?php
# If you are having problems connecting to the MySQL database and all of
# try changing the 'db_server' variable from localhost to 127.0.0.1. Fixe
# Thanks to digininja for the fix.

# Database management system to use

$DBMS = 'MySQL';
#$DBMS = 'PGSQL';

# Database variables

$_DVWA = array();
$_DVWA['db_server'] = 'localhost';
$_DVWA['db_database'] = 'dvwa';
$_DVWA['db_user'] = 'root';
$_DVWA['db_password'] = '654321';

# Only needed for PGSQL
[ Read 23 lines (Converted from DOS format) ]
^G Get Help ^O WriteOut ^R Read File ^Y Prev Page ^K Cut Text ^C Cur P
^X Exit ^J Justify ^W Where Is ^U Next Page ^U UnCut Text ^T To Sp
```

- systemctl restart httpd

b. Cài đặt MySQL/MariaDB:

- dnf install mariadb-server mariadb
- systemctl enable mariadb
- systemctl restart mariadb
- mysql_secure_install
- mysql -u root -p

c. Cài đặt PHP:

- dnf install <https://dl.fedoraproject.org/pub/epel/epel-release-latest-8.noarch.rpm>
- dnf install <https://rpms.remirepo.net/enterprise/remi-release-8.rpm>
- dnf module list
- dnf module install php:remi-7.2
- dnf install php-mysql php-xml php-soap php-xmllrpc php-mbstring php-json php-gd php-mcrypt php-gd php-ldap php-odbc php-pear php-xml php-xmllrpc php-mbstring php-soap curl curl-devel
- dnf install php-opcache php-pecl-apcu php-pecl-memcached
- Cài đặt phpMyAdmin:
yum install phpMyAdmin

Cung cấp khả năng truy cập đến phpmyadmin từ ip bên ngoài internet bằng lệnh sau:

vi /etc/httpd/conf.d/phpMyAdmin.conf

d. Cài đặt Wordpress:

- Xóa đi nội dung web tĩnh:
 - `cd /srv/www/vmware.lab/public_html`
 - `rm -rf *`
- Download mã nguồn Wordpress
 - `wget https://wordpress.org/latest.tar.gz`
 - `tar xf latest.tar.gz`
 - `cd wordpress`
 - `cp -R */srv/www/vmware.lab/public_html/`
- Phân loại quyền lại source web wordpress
 - `chown -R apache:apache public_html/`
 - `mv wp-config-sample.php wp-config.php`

vi wp-config.php

```
// ** MySQL settings - You can get this info from your web host ** //  
/** The name of the database for WordPress */  
define('DB_NAME', 'wordpress');  
  
/** MySQL database username */  
define('DB_USER', 'wordpressuser');  
  
/** MySQL database password */  
define('DB_PASSWORD', 'password');
```

2.3. Cấu hình Iptables

2.3.1. Cài đặt iptables: \$ sudo apt-get install iptables

```
quangkha@quangkha-virtual-machine: ~/Desktop
quangkha@quangkha-virtual-machine:~/Desktop$ sudo apt-get install iptables
[sudo] password for quangkha:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
iptables is already the newest version (1.8.7-1ubuntu5.2).
iptables set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 2 not upgraded.
quangkha@quangkha-virtual-machine:~/Desktop$ iptables -L
iptables v1.8.7 (nf_tables): Could not fetch rule set generation id: Permission
denied (you must be root)

quangkha@quangkha-virtual-machine:~/Desktop$ sudo iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source                destination

Chain FORWARD (policy ACCEPT)
target     prot opt source                destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination
quangkha@quangkha-virtual-machine:~/Desktop$ sudo systemctl start iptables
Failed to start iptables.service: Unit iptables.service not found.
quangkha@quangkha-virtual-machine:~/Desktop$
```

Hình 21: Cài đặt Iptable

2.3.2. Thiết lập iptables

Thiết lập ban đầu iptables: **\$sudo iptables -F**

```
quangkha@quangkha-virtual-machine:~/Desktop$ sudo iptables -F
quangkha@quangkha-virtual-machine:~/Desktop$ sudo iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source                destination

Chain FORWARD (policy ACCEPT)
target     prot opt source                destination

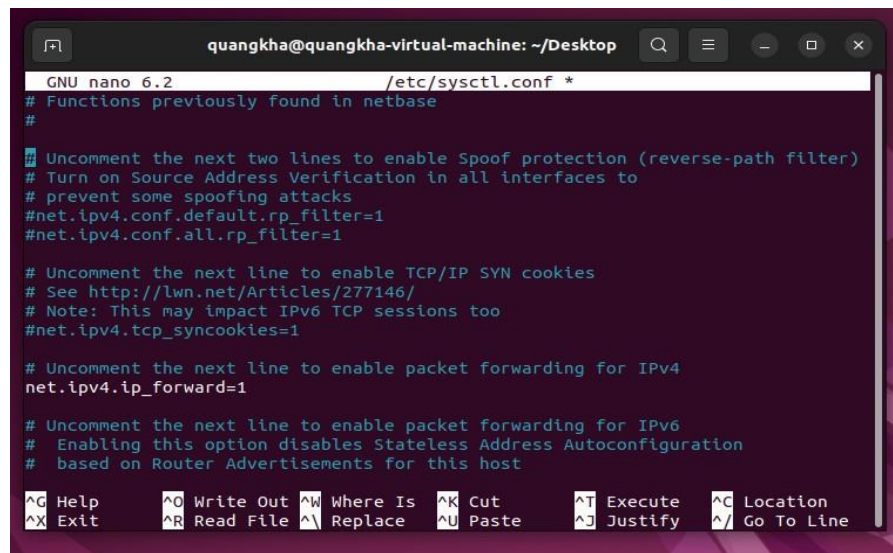
Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination
quangkha@quangkha-virtual-machine:~/Desktop$
```

Hình 22: Thiết lập ban đầu cho iptables

Kích hoạt khả năng định tuyến: **\$sudo sysctl -w net.ipv4.ip_forward=1**

```
quangkha@quangkha-virtual-machine:~/Desktop$ whereis iptables.service
iptables.service:
quangkha@quangkha-virtual-machine:~/Desktop$ sudo sysctl -w net.ipv4.ip_forward=
1
[sudo] password for quangkha:
net.ipv4.ip_forward = 1
quangkha@quangkha-virtual-machine:~/Desktop$
```

Hình 23: Kích hoạt khả năng định tuyến (1)



```
quangkha@quangkha-virtual-machine: ~/Desktop
GNU nano 6.2 /etc/sysctl.conf
# Functions previously found in netbase
#
# Uncomment the next two lines to enable Spoof protection (reverse-path filter)
# Turn on Source Address Verification in all interfaces to
# prevent some spoofing attacks
#net.ipv4.conf.default.rp_filter=1
#net.ipv4.conf.all.rp_filter=1
#
# Uncomment the next line to enable TCP/IP SYN cookies
# See http://lwn.net/Articles/277146/
# Note: This may impact IPv6 TCP sessions too
#net.ipv4.tcp_syncookies=1
#
# Uncomment the next line to enable packet forwarding for IPv4
net.ipv4.ip_forward=1
#
# Uncomment the next line to enable packet forwarding for IPv6
# Enabling this option disables Stateless Address Autoconfiguration
# based on Router Advertisements for this host

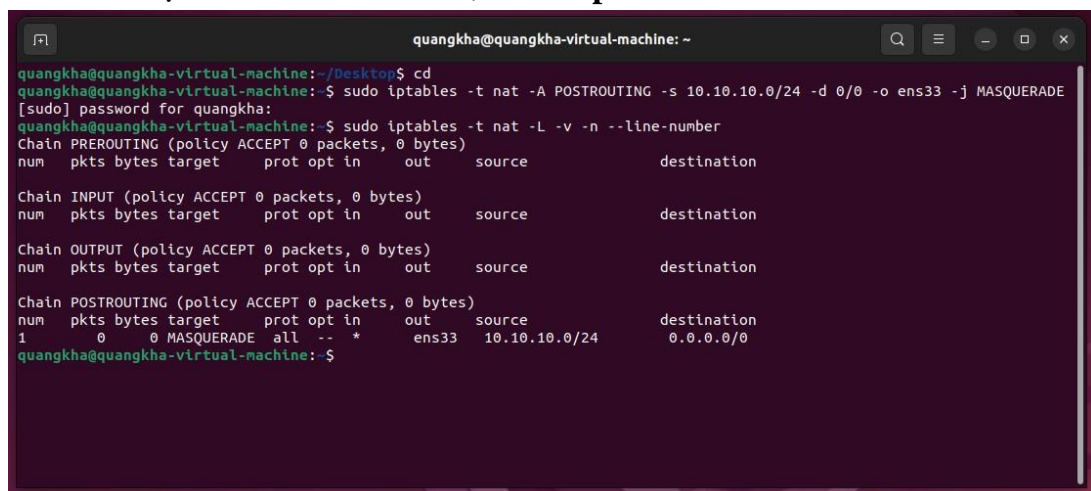
^G Help      ^O Write Out ^W Where Is  ^K Cut       ^T Execute  ^C Location
^X Exit      ^R Read File ^\ Replace   ^U Paste     ^J Justify  ^_ Go To Line
```

Hình 24: Kích hoạt khả năng định tuyến (2)

Cho phép post routing đến card mạng ens33:

\$sudo iptables -t nat -A POSTROUTING -s 10.10.10.0/24 -d 0/0 -o ens33 -j MASQUERADE

Kiểm tra lại trên Chain NAT: **\$ sudo iptables -t nat -L -v -n --line-number**



```
quangkha@quangkha-virtual-machine: ~
quangkha@quangkha-virtual-machine:~/Desktop$ cd
quangkha@quangkha-virtual-machine:~$ sudo iptables -t nat -A POSTROUTING -s 10.10.10.0/24 -d 0/0 -o ens33 -j MASQUERADE
[sudo] password for quangkha:
quangkha@quangkha-virtual-machine:~$ sudo iptables -t nat -L -v -n --line-number
Chain PREROUTING (policy ACCEPT 0 packets, 0 bytes)
num  pkts bytes target    prot opt in     out     source destination
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
num  pkts bytes target    prot opt in     out     source destination
Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
num  pkts bytes target    prot opt in     out     source destination
Chain POSTROUTING (policy ACCEPT 0 packets, 0 bytes)
num  pkts bytes target    prot opt in     out     source destination
1    0    0 MASQUERADE all  --  *      ens33   10.10.10.0/24  0.0.0.0/0
quangkha@quangkha-virtual-machine:~$
```

Hình 25: Kiểm tra trong Chain NAT

VIII. Thiết lập các luồng trong Iptables:

- Cho phép Chain FORWARD ACCEPT:
\$ sudo iptables -P FORWARD ACCEPT
- Cho phép Chain INPUT ACCEPT:
\$ sudo iptables -P INPUT ACCEPT
- Cho phép Chain OUTPUT ACCEPT:
\$ sudo iptables -P OUTPUT ACCEPT

2.4. Thiết lập IP tĩnh trên CentOS

- Xin địa chỉ IP: **\$ dhclient**

```
[root@vmware ~]# dhclient
[root@vmware ~]# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet 31.13.95.36/24 brd 31.13.95.255 scope global lo:1
    inet 216.58.199.101/24 brd 216.58.199.255 scope global lo:2
    inet 8.8.8.8/24 brd 8.8.8.255 scope global lo:3
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth4: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UNKNOW
    link/ether 00:0c:29:d4:bd:fe brd ff:ff:ff:ff:ff:ff
    inet 10.10.10.130/24 brd 10.10.10.255 scope global eth4
    inet6 fe80::20c:29ff:fed4:bdf6/64 scope link
        valid_lft forever preferred_lft forever
[root@vmware ~]#
```

Hình 26: Xin địa chỉ

- Tạo một tệp cấu hình mới trong thư mục:
\$ nano /etc/sysconfig/network-scripts/ifcfg-eth4

```
GNU nano 2.0.9 File: ifcfg-eth4

DEVICE=eth4
HWADDR=00:0c:29:d4:bd:fe
NM_CONTROLLED=yes
ONBOOT=yes

IPADDR=10.10.10.130
NETMASK=255.255.255.0
BROADCAST=10.10.10.255
GATEWAY=10.10.10.129

TYPE=Ethernet
BOOTPROTO=static

[ Read 12 lines ]
^G Get Help  ^O WriteOut  ^R Read File ^Y Prev Page ^K Cut Text   ^C Cur Pos
^X Exit      ^J Justify   ^W Where Is  ^U Next Page ^_ UnCut Text ^T To Spell
```

Hình 27: Tạo tệp cấu hình

- Khởi động lại dịch vụ mạng: **\$ service network restart**

```
[root@vmware network-scripts]# service network restart
Shutting down interface eth4: [ OK ]
Shutting down loopback interface: [ OK ]
Bringing up loopback interface: [ OK ]
Bringing up interface eth1: Device eth1 does not seem to be present, delaying i
nitialization. [FAILED]
Bringing up interface eth3: Device eth3 does not seem to be present, delaying i
nitialization. [FAILED]
Bringing up interface eth4: Determining if ip address 10.10.10.130 is already i
n use for device eth4... [ OK ]
[root@vmware network-scripts]#
```

Hình 28: Khởi động lại dịch vụ mạng

THỰC NGHIỆM

IX. Tiến hành kịch bản

1. Rules Snort3 các kịch bản:

- DOS Attack: alert tcp any any -> any any (msg:"Phat hien DOS Attack"; flow:to_server; detection_filter:track by_src, count 500, seconds 5; sid: 1000001; rev: 004;)
- XSS Attack: alert tcp any any -> any any (msg:"Phat hien DOS Attack"; flow:to_server; detection_filter:track by_src, count 500, seconds 5; sid: 1000001; rev: 004;)
- SQL Injection Attack:
 - alert tcp any any -> any 80 (content:"or", nocase; msg:"Phat hien OR tren url"; sid:1000004;)
 - alert tcp any any -> any 80 (content:"and", nocase; msg:"Phat hien AND tren url"; sid:1000005;)
- Brute force Attack: alert tcp 10.10.10.0/24 22 -> any any (msg:"thong bao Attack Brute Force";sid:1000009;)

2. Kịch bản DOS

2.1. Khái niệm:

DoS (Denial of Service) là hình thức tấn công dựa trên hình thức đánh sập tạm thời 1 hệ thống mạng bằng cách gửi lượng lớn yêu cầu truy cập đến 1 trang web cụ thể.[7]

2.2. Tấn công thực nghiệm:

2.2.1. Sử dụng Pentmenu tiến hành tấn công DOS


```
root@khaks: ~/pentmenu
File Actions Edit View Help
root@khaks: ~/pentmenu x khaks@khaks: ~ x

PENTMENU

Welcome to pentmenu!
Please report all bugs, improvements and suggestions to https://github.com/GinjaChris/pentmenu/issues
This software is only for responsible, authorised use.
YOU are responsible for your own actions!
Please review the readme at https://raw.githubusercontent.com/GinjaChris/pentmenu/master/README.md before proceeding

1) Recon
2) DOS
3) Extraction
4) View Readme
5) Quit
Pentmenu>2
1) ICMP Echo Flood 5) TCP RST Flood 9) Slowloris 13) Go back
2) ICMP Blacknurse 6) TCP XMAS Flood 10) IPsec DOS
3) TCP SYN Flood 7) UDP Flood 11) Distraction Scan
4) TCP ACK Flood 8) SSL DOS 12) DNS NXDOMAIN Flood
Pentmenu>9
Using netcat for Slowloris attack....
Enter target:
10.10.10.130
Target is set to 10.10.10.130
Enter target port (defaults to 80):
80
Using Port 80
Enter number of connections to open (default 2000):
5000
Choose interval between sending headers.
Default is [r]andom, between 5 and 15 seconds, or enter interval in seconds:
5
use SSL/TLS? [y]es or [n]o (default):
```

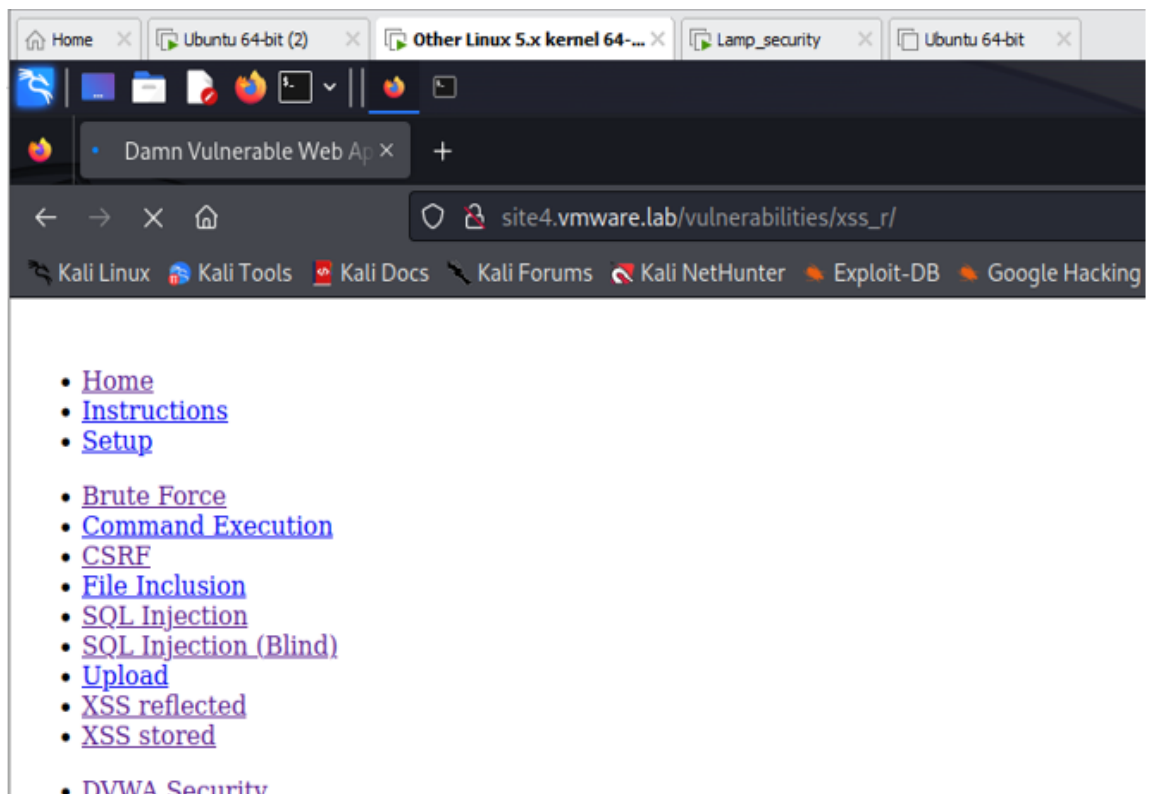
Hình 29: Tấn công Slowloris vào Web Server port 80

```
root@khaks: ~/pentmenu
File Actions Edit View Help
root@khaks: ~/pentmenu x khaks@khaks: ~ x

Default is [r]andom, between 5 and 15 seconds, or enter interval in seconds:
r
use SSL/TLS? [y]es or [n]o (default):

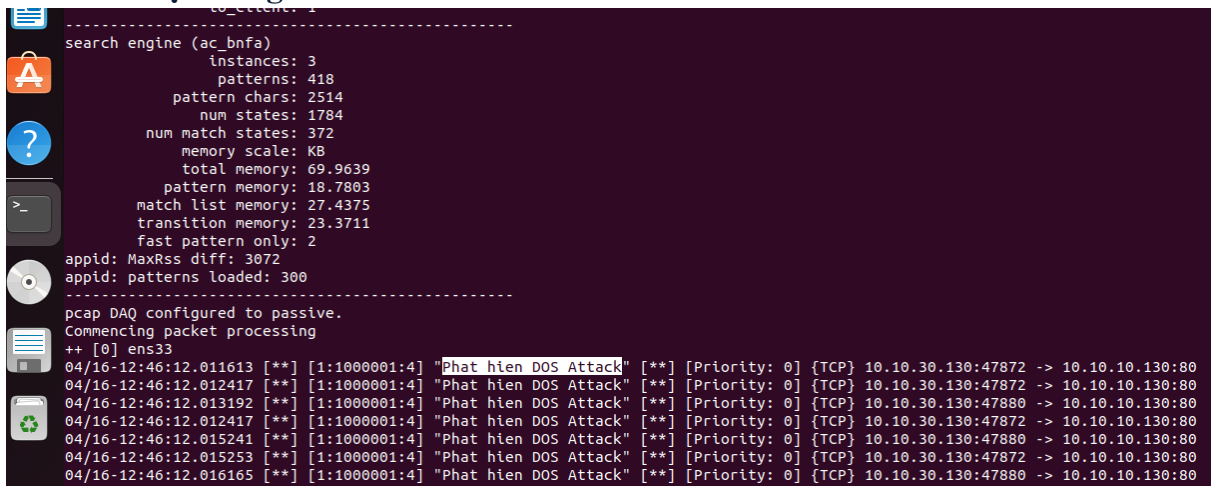
Launching Slowloris...Use 'Ctrl c' to exit prematurely
Slowloris attack ongoing...this is connection 1, interval is 13 seconds
Slowloris attack ongoing...this is connection 2, interval is 13 seconds
Slowloris attack ongoing...this is connection 3, interval is 13 seconds
Slowloris attack ongoing...this is connection 4, interval is 13 seconds
Slowloris attack ongoing...this is connection 5, interval is 13 seconds
Slowloris attack ongoing...this is connection 6, interval is 13 seconds
Slowloris attack ongoing...this is connection 7, interval is 13 seconds
Slowloris attack ongoing...this is connection 8, interval is 13 seconds
Slowloris attack ongoing...this is connection 9, interval is 13 seconds
Slowloris attack ongoing...this is connection 10, interval is 13 seconds
Slowloris attack ongoing...this is connection 11, interval is 13 seconds
Slowloris attack ongoing...this is connection 12, interval is 13 seconds
Slowloris attack ongoing...this is connection 13, interval is 13 seconds
Slowloris attack ongoing...this is connection 14, interval is 13 seconds
Slowloris attack ongoing...this is connection 15, interval is 13 seconds
Slowloris attack ongoing...this is connection 16, interval is 13 seconds
Slowloris attack ongoing...this is connection 17, interval is 13 seconds
Slowloris attack ongoing...this is connection 18, interval is 13 seconds
Slowloris attack ongoing...this is connection 19, interval is 13 seconds
Slowloris attack ongoing...this is connection 20, interval is 13 seconds
Slowloris attack ongoing...this is connection 21, interval is 13 seconds
Slowloris attack ongoing...this is connection 22, interval is 13 seconds
Slowloris attack ongoing...this is connection 23, interval is 13 seconds
Slowloris attack ongoing...this is connection 24, interval is 13 seconds
Slowloris attack ongoing...this is connection 25, interval is 13 seconds
Slowloris attack ongoing...this is connection 26, interval is 13 seconds
Slowloris attack ongoing...this is connection 27, interval is 13 seconds
Slowloris attack ongoing...this is connection 28, interval is 13 seconds
Slowloris attack ongoing...this is connection 29, interval is 13 seconds
Slowloris attack ongoing...this is connection 30, interval is 13 seconds
```

Hình 30: Attacker gửi hàng loạt request đến Web Server



Hình 31: Kết quả

2.2.2. Phát hiện bằng Snort



Hình 32: Snort nghe trên mạng ens33 phát hiện DOS

3. Kịch bản XSS

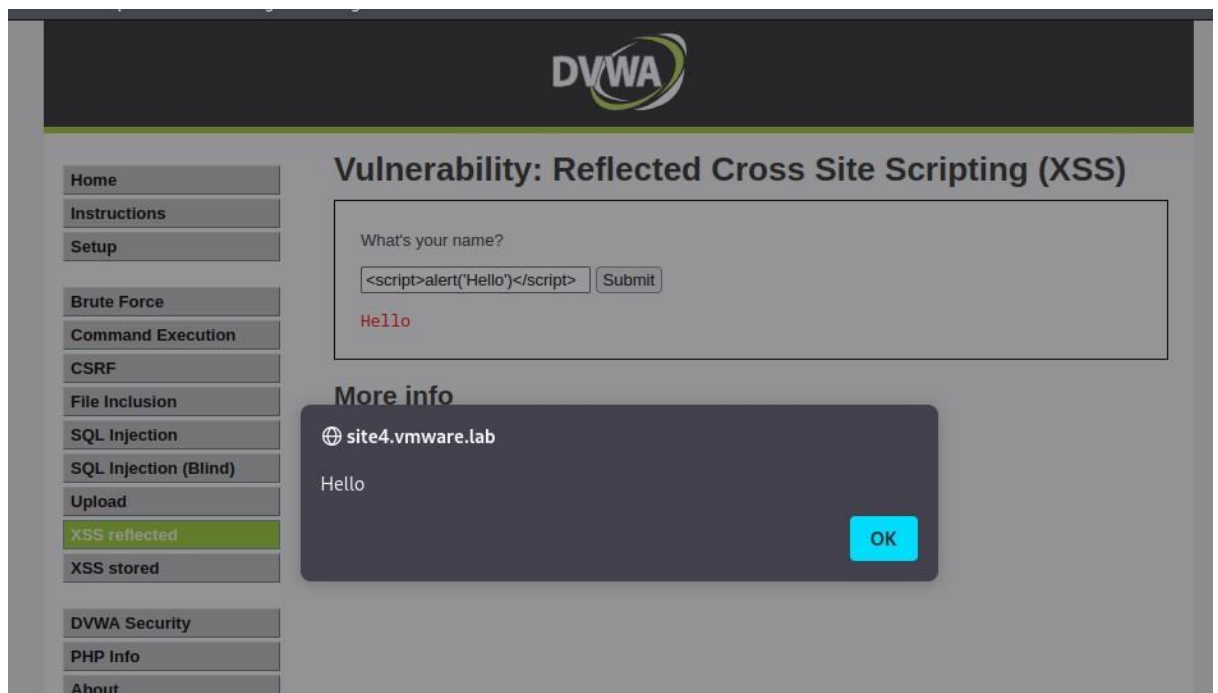
3.1. Khái niệm:

XSS là kiểu tấn công chèn mã độc Script vào các trang web hoặc ứng dụng web khiến cho người dùng cuối thực thi mã trong trình duyệt của họ.

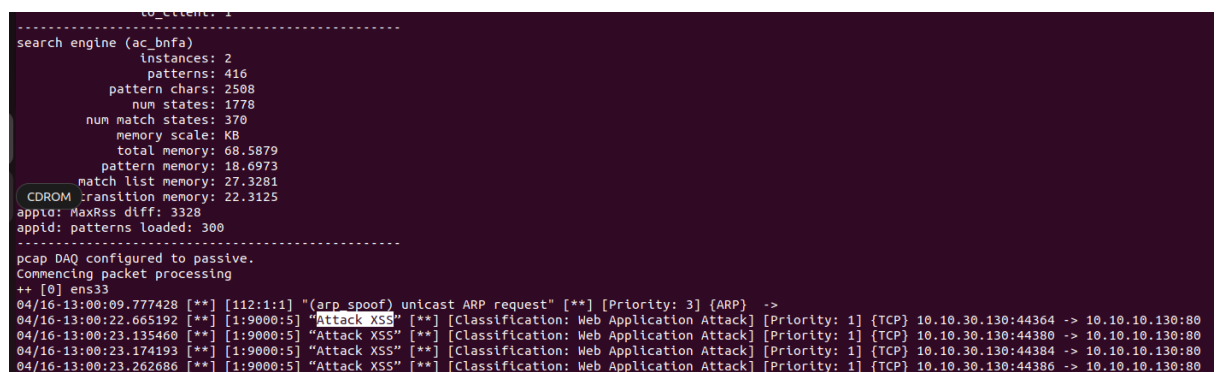
Ví dụ: Reflected XSS, Stored XSS, DOM XSS.

3.2. Tấn công thực nghiệm:

- `<script>alert('Hello')</script>` : Tấn công XSS Reflected



Hình 33: Tấn công XSS



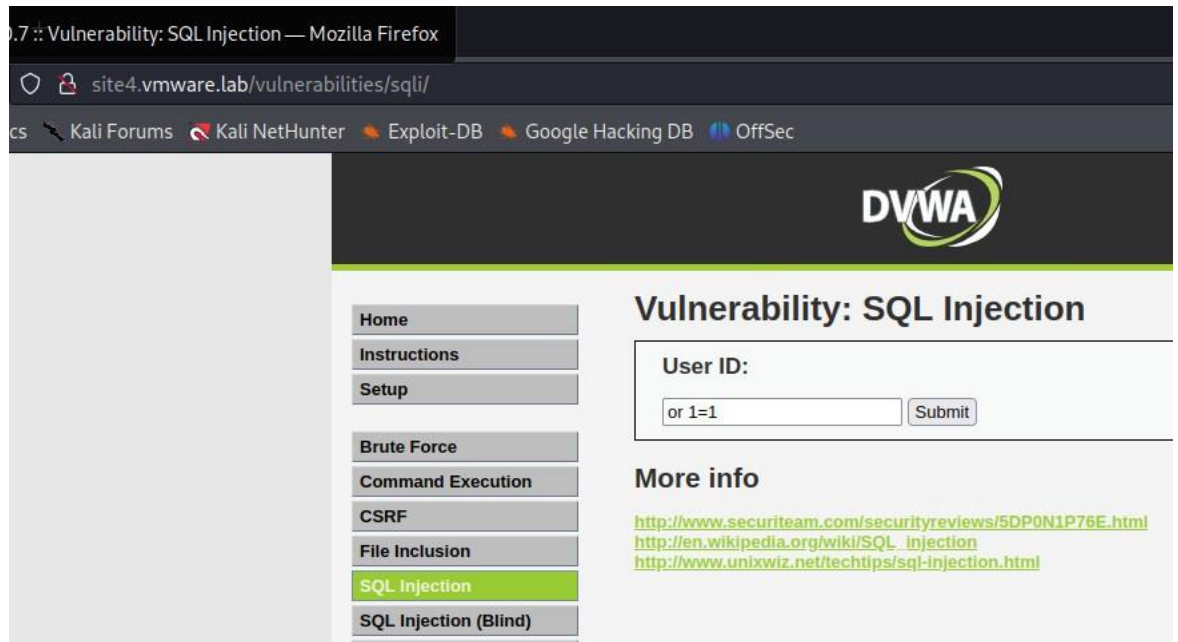
Hình 34: Snort nghe trên mạng ens33 phát hiện tấn công XSS

4. Kịch bản SQL Injection

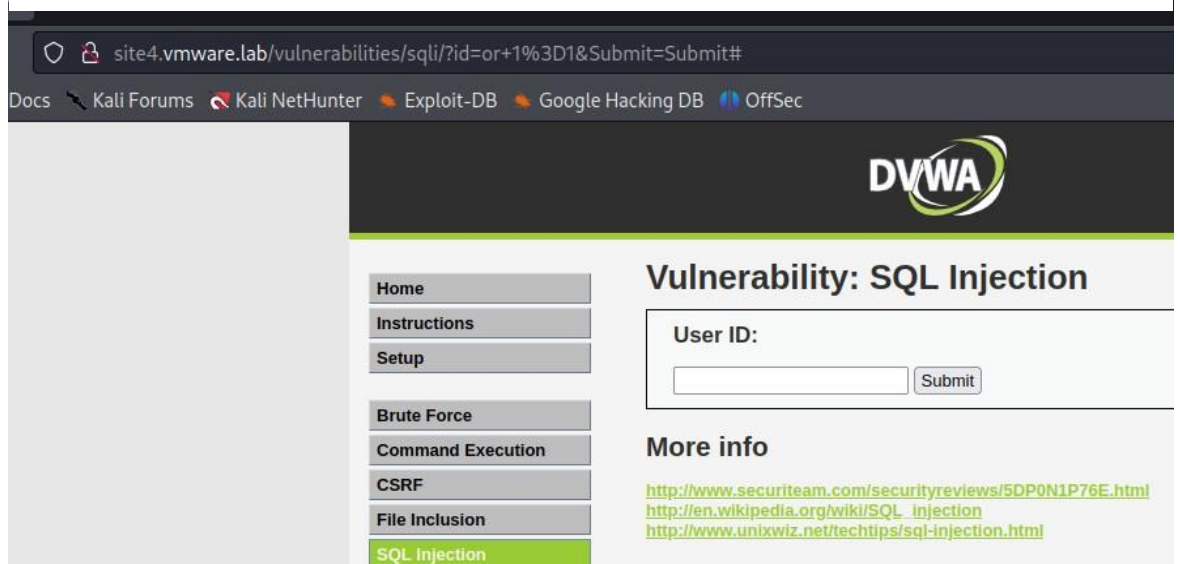
4.1. Khái niệm:

- SQL Injection là một loại tấn công mà kẻ tấn công chèn các câu lệnh SQL độc hại vào trường dữ liệu của ứng dụng web, từ đó có thể thực thi có các lệnh SQL không mong muốn.

4.2. Tấn công thực nghiệm:



Hình 36: Tấn công SQL Injection (1)



Hình 35: Tấn công SQL Injection (2)

```
Ubuntu Software Center
ac_bnf)
instances: 3
patterns: 418
pattern chars: 2514
num states: 1784
num match states: 372
memory scale: KB
total memory: 69.9639
pattern memory: 18.7803
match list memory: 27.4375
transition memory: 23.3711
fast pattern only: 2
appid: MaxRss diff: 3456
appid: patterns loaded: 300

pcap DAQ configured to passive.
Commencing packet processing
++ [0] ens33
04/16-13:04:10.008826 [**] [112:1:1] "(arp_spoof) unicast ARP request" [**] [Priority: 3] {ARP} ->
04/16-13:04:10.244647 [**] [1:1000004:0] "Phat hien OR tren url" [**] [Priority: 0] {TCP} 10.10.30.130:50786 -> 10.10.10.130:80
04/16-13:04:10.742890 [**] [1:1000004:0] "Phat hien OR tren url" [**] [Priority: 0] {TCP} 10.10.30.130:50802 -> 10.10.10.130:80
04/16-13:04:10.804011 [**] [1:1000004:0] "Phat hien OR tren url" [**] [Priority: 0] {TCP} 10.10.30.130:50814 -> 10.10.10.130:80
04/16-13:04:10.849254 [**] [1:1000004:0] "Phat hien OR tren url" [**] [Priority: 0] {TCP} 10.10.30.130:50820 -> 10.10.10.130:80
04/16-13:04:12.368286 [**] [1:1000004:0] "Phat hien OR tren url" [**] [Priority: 0] {TCP} 10.10.30.130:50826 -> 10.10.10.130:80
04/16-13:04:16.050068 [**] [1:1000005:0] "Phat hien AND trn url" [**] [Priority: 0] {TCP} 10.10.30.130:36686 -> 10.10.10.130:80
04/16-13:04:16.595543 [**] [1:1000005:0] "Phat hien AND trn url" [**] [Priority: 0] {TCP} 10.10.30.130:36694 -> 10.10.10.130:80
04/16-13:04:16.665636 [**] [1:1000005:0] "Phat hien AND trn url" [**] [Priority: 0] {TCP} 10.10.30.130:36702 -> 10.10.10.130:80
```

Hình 37: Snort nghe trên mạng ens33 phát hiện tấn công SQL Injection

5. Kịch bản tấn công Brute Force:

5.1. Khái niệm:

Brute Force Attack là hình thức tấn công mạng, trong đó tin tặc sử dụng phần mềm để “trộn” các ký tự khác nhau thành mật khẩu hợp lệ. Lúc này, chúng sẽ gửi các truy vấn đăng nhập vào file wp-login.php và thử mật khẩu. Quá trình này sẽ diễn ra liên tục cho đến khi tin tặc có thể đăng nhập thành công.

5.2. Tấn công thực nghiệm:

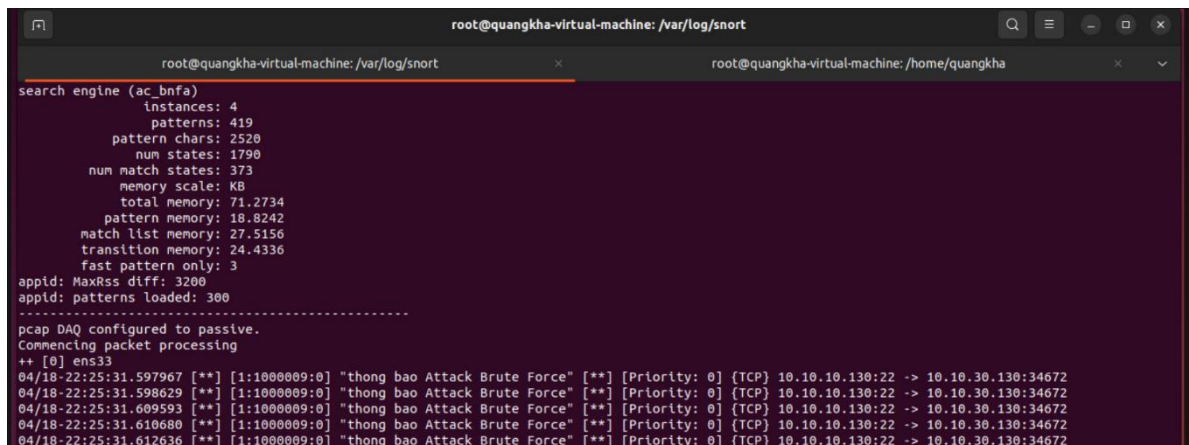
```
(kali@kali)-[~]
$ hydra -L username.txt -P pwd.txt 10.10.30.129 ssh
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-04-18 11:45:34
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 49 login tries (l:7/p:7), ~4 tries per task
[DATA] attacking ssh://10.10.30.129:22/
[ERROR] could not connect to ssh://10.10.30.129:22 - Connection refused
```

Hình 38: Tấn công Brute force tài khoản người dùng bằng Hydra

X. Ngăn chặn xâm nhập bằng IPTABLES

Các bước thực hiện:



```
root@quangkha-virtual-machine: /var/log/snort
search engine (ac_bnf)
  instances: 4
  patterns: 419
  pattern chars: 2520
  num states: 1790
  num match states: 373
  memory scale: KB
  total memory: 71.2734
  pattern memory: 18.8242
  match list memory: 27.5156
  transition memory: 24.4336
  fast pattern only: 3
  apid: MaxRss diff: 3200
  apid: patterns loaded: 300
-----
pcap DAQ configured to passive.
Commencing packet processing
++ [0] ens33
04/18-22:25:31.597967 [**] [1:1000009:0] "thong bao Attack Brute Force" [**] [Priority: 0] [TCP] 10.10.10.130:22 -> 10.10.30.130:34672
04/18-22:25:31.598629 [**] [1:1000009:0] "thong bao Attack Brute Force" [**] [Priority: 0] [TCP] 10.10.10.130:22 -> 10.10.30.130:34672
04/18-22:25:31.609593 [**] [1:1000009:0] "thong bao Attack Brute Force" [**] [Priority: 0] [TCP] 10.10.10.130:22 -> 10.10.30.130:34672
04/18-22:25:31.610680 [**] [1:1000009:0] "thong bao Attack Brute Force" [**] [Priority: 0] [TCP] 10.10.10.130:22 -> 10.10.30.130:34672
04/18-22:25:31.612636 [**] [1:1000009:0] "thong bao Attack Brute Force" [**] [Priority: 0] [TCP] 10.10.10.130:22 -> 10.10.30.130:34672
```

Hình 39: Chống xâm nhập bằng IPTABLE

1. Cấu hình file log dưới dạng JSON:

- Thêm dòng lệnh trong tệp cấu hình snort.lua của Snort3:

```
alert_json = {
    file = true, -- Kích hoạt ghi vào file
    limit = 500, -- Giới hạn số lượng bản ghi trong file 0log
    fields = 'msg src_addr', --Các trường cần ghi vào file log (message và ip nguồn)
}
```

2. Chạy Snort dưới dạng ghi vào log

```
sudo /usr/local/bin/snort -c /usr/local/etc/snort/snort.lua -s 65535 -k none -l /var/log/snort -i ens33 -m 0x1b
```

3. Tạo file ghi log và đọc log

- Tạo một thư mục chứa log: `$sudo mkdir /var/log/snort/`
- Trong thư mục snort, tạo các file: `alert_json.txt`, `blockip.sh`, `blocklist.txt`
- Trong file `blockip.sh`:

```
#!/bin/bash
# Đường dẫn đến file log của Snort
LOG_FILE="alert_json.txt"
# File chứa danh sách IP cần block
BLOCK_LIST="blocklist.txt"
# Trích xuất IP từ cấu trúc JSON và thêm vào danh sách block
```

```
jq '.src_addr' $LOG_FILE | sed 's///g' | sort | uniq >> $BLOCK_LIST
# Đọc từng dòng trong file danh sách block và thực hiện block bằng iptables
while IFS= read -r ip; do
    # Kiểm tra xem IP đã có trong danh sách block hay chưa
    if ! iptables -C INPUT -s $ip -j DROP 2>/dev/null; then
        iptables -A INPUT -s $ip -j DROP
    fi
    #them quy tac cho chain FORWARD
    if ! iptables -C FORWARD -s $ip -j DROP 2>/dev/null; then
        iptables -A FORWARD -s $ip -j DROP
    fi
done < $BLOCK_LIST
# Lưu lại cấu hình iptables
iptables-save > /etc/iptables/rules.v4
```

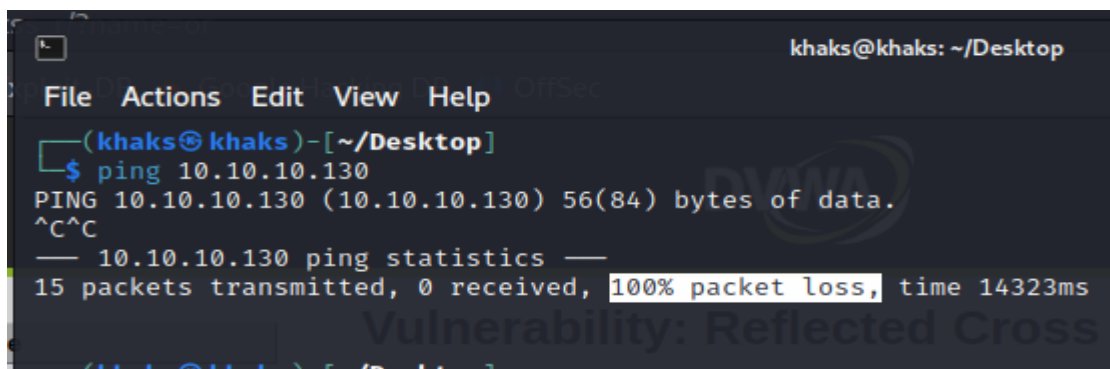
4. Cấp cho blockip.sh quyền execute: \$sudo chmod +x blockip.sh
5. Khởi chạy file blockip.sh: \$sudo ./blockip.sh

```
quangkha@quangkha-virtual-machine:/var/log/snort$ ls
alert_json.txt  blockip.sh  blocklist.txt
quangkha@quangkha-virtual-machine:/var/log/snort$ sudo ./blockip.sh
DROP all opt -- in * out * 10.10.30.1 -> 0.0.0.0/0
DROP all opt -- in * out * 10.10.30.1 -> 0.0.0.0/0
DROP all opt -- in * out * 10.10.30.130 -> 0.0.0.0/0
DROP all opt -- in * out * 10.10.30.130 -> 0.0.0.0/0
DROP all opt -- in * out * 10.10.30.1 -> 0.0.0.0/0
DROP all opt -- in * out * 10.10.30.1 -> 0.0.0.0/0
DROP all opt -- in * out * 10.10.30.130 -> 0.0.0.0/0
DROP all opt -- in * out * 10.10.30.130 -> 0.0.0.0/0
quangkha@quangkha-virtual-machine:/var/log/snort$ sudo iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source                destination
DROP       all  --  10.10.30.1             anywhere
DROP       all  --  10.10.30.130           anywhere

Chain FORWARD (policy ACCEPT)
target     prot opt source                destination
DROP       all  --  10.10.30.1             anywhere
DROP       all  --  10.10.30.130           anywhere

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination
quangkha@quangkha-virtual-machine:/var/log/snort$
```

Hình 40: Máy attacker đã được đưa vào iptables



```
khaks@khaks: ~/Desktop
File Actions Edit View Help
(khaks@khaks)-[~/Desktop]
$ ping 10.10.10.130
PING 10.10.10.130 (10.10.10.130) 56(84) bytes of data.
^C^C
— 10.10.10.130 ping statistics —
15 packets transmitted, 0 received, 100% packet loss, time 14323ms
```

Hình 41: Máy attacker không còn ping được đến máy chủ sau khi bị chặn

XI. Gửi thông báo tấn công về email với sSMTP

A. Các bước cài đặt sSMTP cơ bản:

1. Cập nhật hệ thống và cài đặt các thư viện phụ thuộc:

```
$sudo apt-get update
```

```
$sudo apt-get install ssmtp
```

2. Cấu hình ssmtp trên Ubuntu

```
$sudo -s
```

```
cat >> /etc/ssmtp/ssmtp.conf << EOF
```

```
AuthUser=abc@domain.com
```

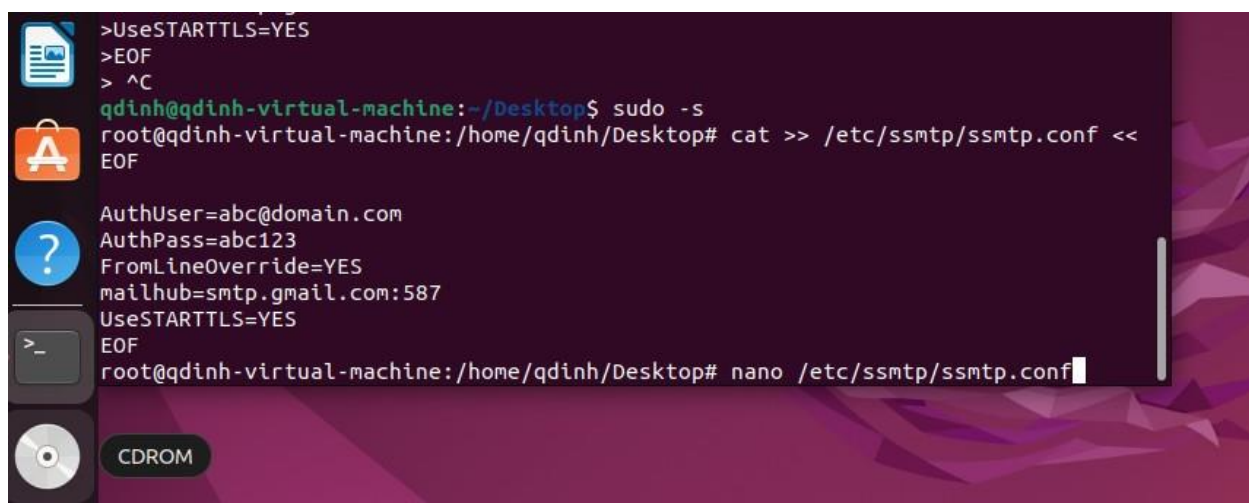
```
AuthPass=abc123
```

```
FromLineOverride=YES
```

```
mailhub=smtp.gmail.com:587
```

```
UseSTARTTLS=YES
```

```
EOF
```

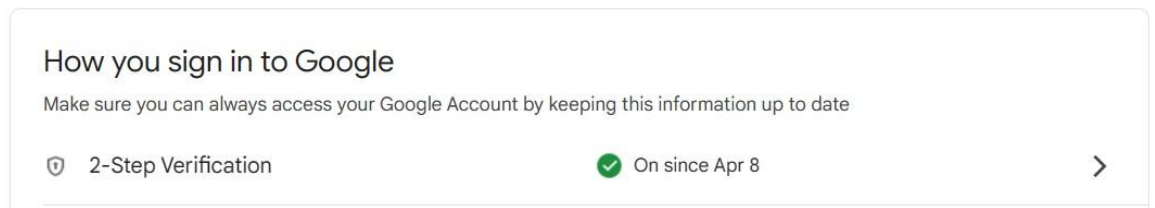


```
>UseSTARTTLS=YES
>EOF
> ^C
qđinh@qđinh-virtual-machine:~/Desktop$ sudo -s
root@qđinh-virtual-machine:/home/qđinh/Desktop# cat >> /etc/ssmtp/ssmtp.conf <<
EOF
AuthUser=abc@domain.com
AuthPass=abc123
FromLineOverride=YES
mailhub=smtp.gmail.com:587
UseSTARTTLS=YES
EOF
root@qđinh-virtual-machine:/home/qđinh/Desktop# nano /etc/ssmtp/ssmtp.conf
```

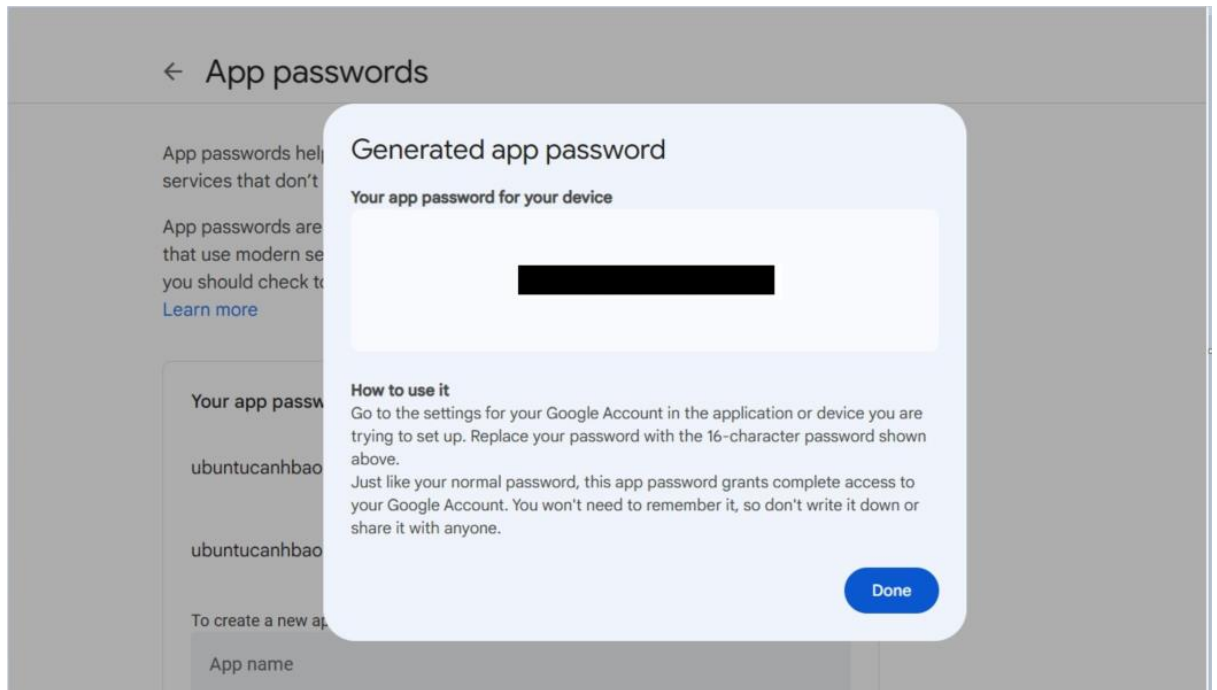
Hình 42: Cấu hình sSMTP

3. Tạo mật khẩu ứng dụng Gmail để sử dụng SMTP

- **Bật xác minh 2 bước:**



Hình 43: Bật xác minh 2 bước

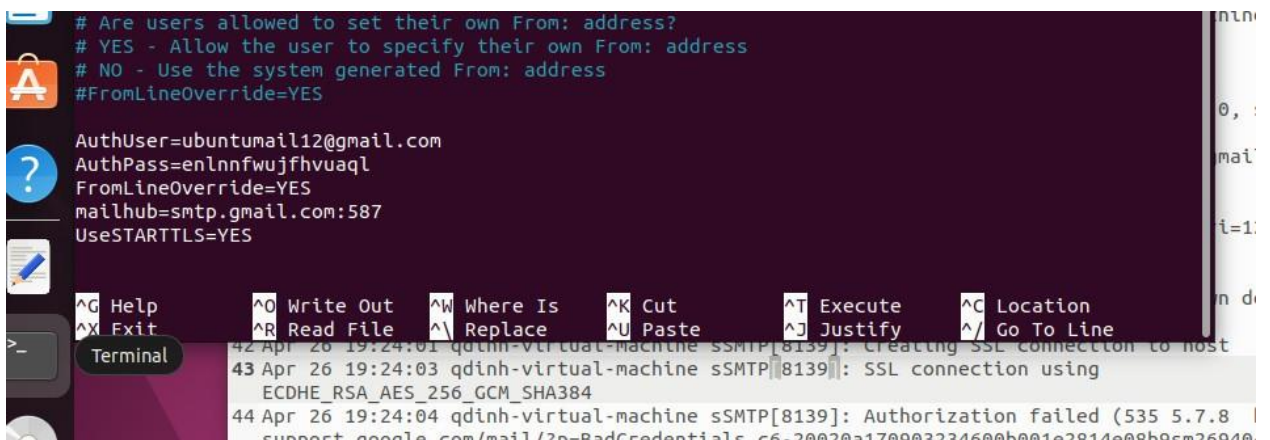


Hình 44: Tạo mật khẩu ứng dụng

- **Tạo mật khẩu ứng dụng:**

4. Thiết lập ứng dụng liên kết với Mail Server

nano /etc/ssmtp/ssmtp.conf



Hình 45: Cấu hình sSMTP liên kết với mật khẩu ứng dụng

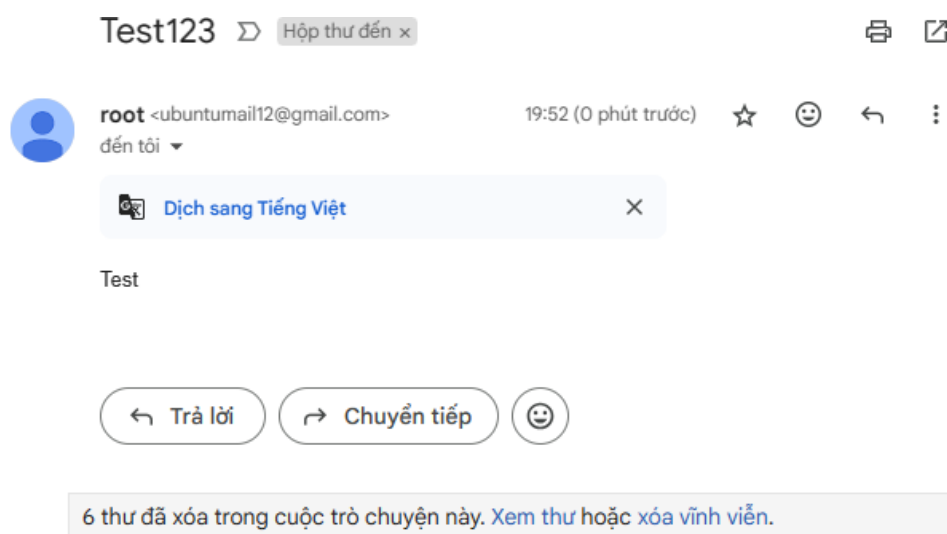
- Tạo backup cho sendmail và cấu hình bằng liên kết tượng trưng
`mkdir /root/.backup`
`mv /usr/sbin/sendmail /root/.backup`
`ln -s /usr/sbin/ssmtp /usr/sbin/sendmail`
- Kiểm tra liên kết:
`ls -l /usr/sbin/sendmail`
- Cài đặt mailutils để gửi mail qua PHP
`apt install mailutils`

```
root@qđinh-virtual-machine:/home/qđinh/Desktop# apt install mailutils
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  db-util db5.3-util liblockfile-bin liblockfile1 libsigsegv2 lockfile-progs m4 procmail
  liblockfile1 libsigsegv2 lockfile-progs m4 procmail
Use 'dpkg --get-selections' to configure these defaults. Use 'apt autoremove' to remove them.
```

Hình 46: Cài đặt mailutils

5. Test gửi email

\$ echo "TEST" | mail -s "123" lequangdinh0609@gmail.com



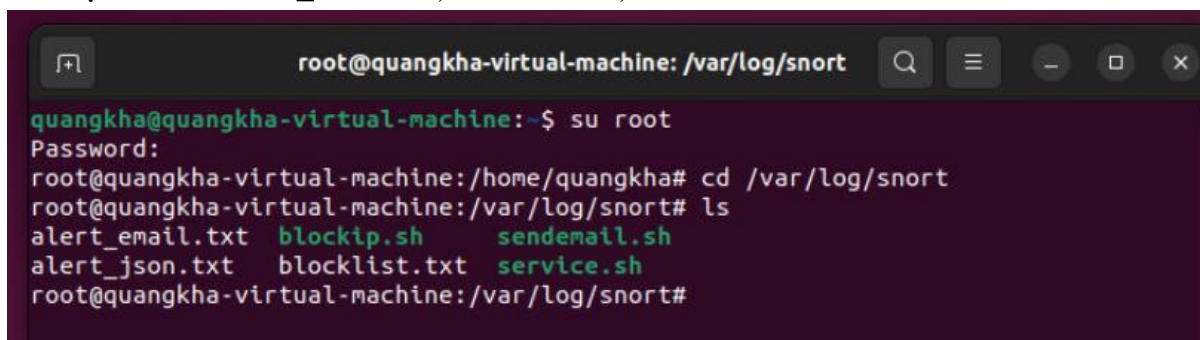
Hình 47: Test gửi email

B. Kết hợp với Snort3

1. Điều hướng đến thư mục chứa log:

```
$cd /var/log/snort
```

2. Tạo các file alert_email.txt, sendmail.sh, service.sh



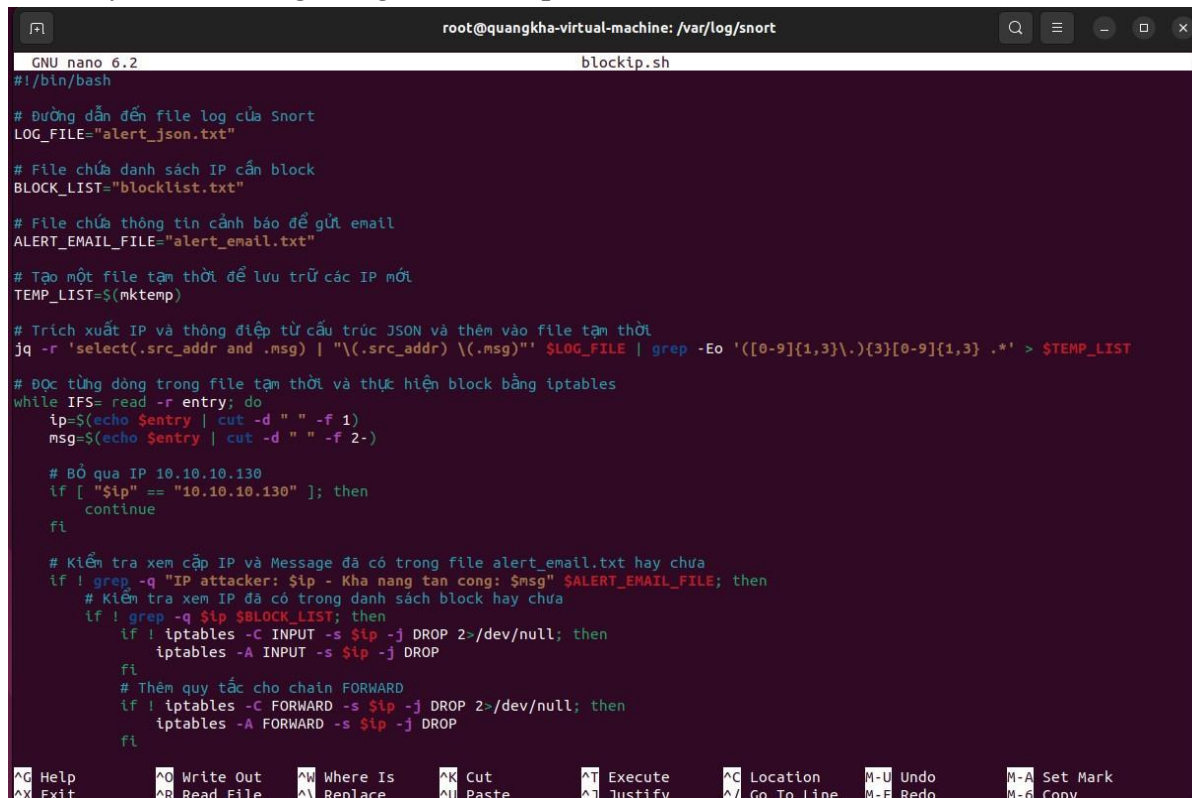
```
root@quangkha-virtual-machine: /var/log/snort
quangkha@quangkha-virtual-machine:~$ su root
Password:
root@quangkha-virtual-machine:/home/quangkha# cd /var/log/snort
root@quangkha-virtual-machine:/var/log/snort# ls
alert_email.txt  blockip.sh  sendmail.sh
alert_json.txt  blocklist.txt  service.sh
root@quangkha-virtual-machine:/var/log/snort#
```

Hình 48: Tạo các file .txt để điều hướng

3. Kịch bản:

- alert_email.txt sẽ trống, alert_json sẽ đọc trong file lua, blockip sẽ đọc file alert_json và block vào iptable và ghi lại vào blocklist.txt và ghi cảnh báo vào file alert_email.txt.
- service.sh sẽ luôn thực thi file sendmail.sh, file sendmail.sh sẽ tự động gửi mail cảnh báo nếu có nội dung trong file alert_email.txt.

4. Thay đổi nội dung trong file blockip.sh:



```
GNU nano 6.2 blockip.sh
#!/bin/bash

# Đường dẫn đến file log của Snort
LOG_FILE="alert_json.txt"

# File chứa danh sách IP cần block
BLOCK_LIST="blocklist.txt"

# File chứa thông tin cảnh báo để gửi email
ALERT_EMAIL_FILE="alert_email.txt"

# Tạo một file tạm thời để lưu trữ các IP mới
TEMP_LIST=$(mktemp)

# Trích xuất IP và thông điệp từ cấu trúc JSON và thêm vào file tạm thời
jq -r 'select(.src_addr and .msg) | "{src_addr: \(.src_addr) | \(.msg)}"' $LOG_FILE | grep -Eo '([0-9]{1,3}\.){3}[0-9]{1,3} .*' > $TEMP_LIST

# Đọc từng dòng trong file tạm thời và thực hiện block bằng iptables
while IFS= read -r entry; do
    ip=$(echo $entry | cut -d " " -f 1)
    msg=$(echo $entry | cut -d " " -f 2-)

    # Bỏ qua IP 10.10.10.130
    if [ "$ip" == "10.10.10.130" ]; then
        continue
    fi

    # Kiểm tra xem cặp IP và Message đã có trong file alert_email.txt hay chưa
    if ! grep -q "IP attacker: $ip - Khả năng tấn công: $msg" $ALERT_EMAIL_FILE; then
        # Kiểm tra xem IP đã có trong danh sách block hay chưa
        if ! grep -q $ip $BLOCK_LIST; then
            if ! iptables -C INPUT -s $ip -j DROP 2>/dev/null; then
                iptables -A INPUT -s $ip -j DROP
            fi
            # Thêm quy tắc cho chain FORWARD
            if ! iptables -C FORWARD -s $ip -j DROP 2>/dev/null; then
                iptables -A FORWARD -s $ip -j DROP
            fi
        fi
    fi
done
```

Hình 49: Thay đổi nội dung file blockip.sh (1)

```
# Ghi thông tin vào file alert_email.txt
echo "IP attacker: $ip - Khả năng tấn công: $msg" >> $ALERT_EMAIL_FILE
fi
done < $TEMP_LIST
# Xóa file tạm thời
rm $TEMP_LIST
# Lưu lại cấu hình iptables
iptables-save > /etc/iptables/rules.v4
```

Help Write Out Where Is Cut Execute Location Undo Set Mark
Exit Read File Replace Paste Justify Go To Line Redo Redo Copy

Hình 50: Thay đổi nội dung file blockip.sh (2)

5. Nội dung file sendmail.sh

```
GNU nano 6.2 sendmail.sh
#!/bin/bash

# File chứa thông tin cảnh báo để gửi email
ALERT_EMAIL_FILE="/var/log/snort/alert_email.txt"
ALERT_JAYSON_FILE="/var/log/snort/alert_json.txt"
BLOCKIP_SCRIPT="/var/log/snort/blockip.sh"

# Đọc nội dung cảnh báo từ file

# Địa chỉ email người gửi và người nhận
from_email="info@yourdomain.com"
to_email="tranducthien285@gmail.com"
# Gửi email
run_blockip_script() {
    bash "$BLOCKIP_SCRIPT"
}
run_blockip_script
sleep 10
email_content=$(cat "$ALERT_EMAIL_FILE")
if [ -s "$ALERT_EMAIL_FILE" ]; then
    # Nếu file không rỗng, gửi email
    echo "$email_content" | mail -s "cảnh báo từ web server!" -a "From: $from_email" "$to_email"
    > "$ALERT_EMAIL_FILE"
fi
```

Hình 51: Nội dung file sendmail.sh

6. Nội dung file service.sh

```
GNU nano 6.2 service.sh
#!/bin/bash

SENDEMAIL="/var/log/snort/sendmail.sh"

run_sendemail_script() {
    bash "$SENDEMAIL"
}

while true; do
    run_sendemail_script
    sleep 30 # Chờ 30s
done
```

Hình 52: Nội dung file service.sh



Hình 53: Cảnh báo được gửi về mail

➔ Như vậy, khi Snort3 ở chế độ ghi vào log, khi ta chạy file service.sh thì sẽ gửi cảnh báo về mail nếu có phát hiện bất thường.

Tài liệu tham khảo

- [1] T. c. c. thương, “Thiệt hại do tấn công mạng toàn cầu lên tới 8 nghìn tỷ USD,” 07 03 2024. [Online]. Available: <https://tapchicongthuong.vn/bai-viet/thiet-hai-do-tan-cong-mang-toan-cau-len-toi-8-nghin-ty-usd-117368.htm>. [Accessed 2024].
- [2] tenten.vn, “IDS là gì? Phân tích so sánh IDS, IPS và tường lửa chi tiết,” 16 10 2023. [Online]. Available: <https://tenten.vn/tin-tuc/ids-la-gi/>. [Accessed 28 03 2024].
- [3] HUY-QA, “SNORT,” 09 03 2023. [Online]. Available: <https://huyqa-home.com/2023/03/09/snort/?fbclid=IwAR2yYnZrKiEE7tcLVffQP0itXErmI29XLDVdao5mM7EvWKRWNaJfXtbz-k>. [Accessed 07 03 2024].
- [4] John, “TOP 5 CÁCH TẤN CÔNG MẠNG PHỔ BIẾN VÀ CÁCH PHÒNG CHỐNG,” 14 07 2023. [Online]. Available: <https://vacif.com/blog/top-5-cach-tan-cong-mang-pho-bien-va-cach-phong-chong/>.
- [5] P. D. Thi, “Kỹ thuật tấn công XSS và cách ngăn chặn,” 24 06 2018. [Online]. Available: <https://viblo.asia/p/ky-thuat-tan-cong-xss-va-cach-ngan-chan-YWOZr0Py5Q0>.
- [6] T. Nguyen, “Tấn công SQL injection là gì? Nguy hiểm đến mức nào và làm sao để phòng tránh?,” 14 09 2023. [Online]. Available: <https://cystack.net/blog/tan-cong-sql-injection>.
- [7] tenten.vn, “DDos/Dos là gì? Giải pháp phòng chống tấn công DDos,” 22 03 2021. [Online]. Available: <https://tenten.vn/tin-tuc/ddos-dos-la-gi-giai-phap-phong-chong-tan-cong-ddos/>. [Accessed 28 03 2024].
- [8] T. V. Cường, “[Network] Tìm hiểu cơ chế, cách hoạt động của IDS (phần 2),” 25 03 2015. [Online]. Available: <https://viblo.asia/p/network-tim-hieu-co-che-cach-hoat-dong-cua-ids-phan-2-pDljMbe5RVZn>. [Accessed 28 03 2024].
- [9] N. V. Đường, “Luận văn thạc sĩ, Các giải pháp bảo mật mạng và Ứng dụng cho mạng máy tính tại các trường đại học/cao đẳng,” PTIT, 2020. [Online]. Available: <https://123docz.net/document/10389249-luan-van-thac>

si-cac-giai-phap-bao-mat-mang-va-ung-dung-cho-mang-may-tinh-tai-truong-cao-dang-ky-thuat-thong-tin.htm. [Accessed 28 03 2024].

- [10] phongtvc, “Hệ thống phát hiện và ngăn chặn xâm nhập,” WhiteHat, 05 02 2015. [Online]. Available: <https://whitehat.vn/threads/he-thong-phat-hien-va-ngan-chan-xam-nhap.3993/>. [Accessed 28 03 2024].
- [11] Huỳnh Thanh Tâm, Nguyễn Hoàng Nam Dương, “Báo cáo, tìm hiểu hệ thống xâm nhập Snort IDS,” PTIT, 10 2017. [Online]. Available: <https://123docz.net/document/4544345-bao-cao-tim-hieu-he-thong-phat-hien-xam-nhap-snort-ids.htm>. [Accessed 28 03 2024]. [1]