

HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG
KHOA AN TOÀN THÔNG TIN



BÁO CÁO BÀI THỰC HÀNH
HỌC PHẦN: THỰC TẬP CƠ SỞ
MÃ HỌC PHẦN: INT13147

BÀI THỰC HÀNH 2.2
CÀI ĐẶT CẤU HÌNH HIDS/NIDS

Sinh viên thực hiện:

B22DCAT206 PHẠM ĐỨC NAM

Giảng viên hướng dẫn: Đỗ Xuân Chợt

HỌC KỲ 2 NĂM HỌC 2024-2025

Mục lục

1.	Mục đích.....	3
2.	Nội dung thực hành	3
2.1.	Cơ sở lý thuyết	3
2.1.1.	Tìm hiểu khái quát về các hệ thống phát hiện tấn công, xâm nhập, phân loại các hệ thống phát hiện xâm nhập, các kỹ thuật phát hiện xâm nhập. 3	
a.	Giới thiệu về hệ thống phát hiện tấn công, xâm nhập	3
b.	Phân loại hệ thống phát hiện tấn công, xâm nhập	4
c.	Các kỹ thuật phát hiện xâm nhập	5
2.1.2.	Tìm hiểu về kiến trúc và tính năng của một số hệ thống phát hiện tấn công, xâm nhập: Snort, OSSEC.....	7
2.1.2.1.	Snort.....	7
2.1.2.2.	Ossec.....	9
2.2.	Nội dung thực hành	12
2.2.1.	Chuẩn bị môi trường.....	12
2.2.2.	Các bước thực hiện	13
3.	Kết luận	22
4.	Tài liệu tham khảo.....	22

Danh mục hình ảnh

Hình 1 cấu hình ip	15
Hình 2 Kiểm tra phiên bản Snort	15
Hình 3 kiểm tra trạng thái Snort.....	16
Hình 4 Kiểm tra phiên bản Snort	17
Hình 5 chỉnh sửa rule	18
Hình 6 Kiểm tra địa chỉ IP máy Snort.....	19
Hình 7 Trên máy Kali, thực hiện Ping đến máy cài Snort	19
Hình 8 Trên máy Snort hiện các cảnh báo	20
Hình 9 Kiểm tra địa chỉ IP máy Snort.....	20
Hình 10 Trên máy Kali, sử dụng công cụ nmap để rà quét máy Snort: nmap -sV	21
Hình 11 Trên máy Snort, hiện cảnh báo	22
Hình 12 Kiểm tra IP máy Snort	22
Hình 13 Từ máy Kali, sử dụng công cụ hping3 để tấn công TCP SYN Flood máy Snort (dùng lệnh: hping3 -c 15000 -d 120 -S -w 64 -p 80 --flood --rand-source 192.168.17.176).....	23
Hình 14 Trên máy Snort hiện các thông báo	23

1. Mục đích

- Luyện tập việc cài đặt và vận hành hệ thống phát hiện xâm nhập cho host (HIDS) và cho mạng (NIDS)
- Luyện tập việc tạo và chỉnh sửa các luật phát hiện tấn công, xâm nhập cho các hệ thống phát hiện xâm nhập thông dụng

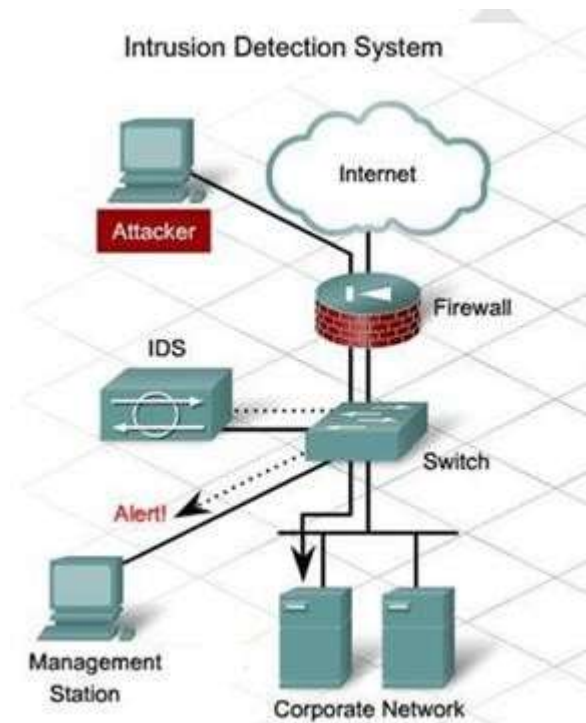
2. Nội dung thực hành

2.1. Cơ sở lý thuyết

2.2. Tìm hiểu khái quát về các hệ thống phát hiện tấn công, xâm nhập, phân loại các hệ thống phát hiện xâm nhập, các kỹ thuật phát hiện xâm nhập.

a. Giới thiệu về hệ thống phát hiện tấn công, xâm nhập

Hệ thống phát hiện xâm nhập (IDS – Intrusion Detection System) đóng vai trò thiết yếu trong các giải pháp bảo mật theo mô hình phòng thủ đa tầng (defense in depth), giúp bảo vệ hệ thống thông tin và mạng. Tùy thuộc vào mục đích triển khai, IDS có thể được đặt trước hoặc sau tường lửa trong sơ đồ mạng. Thông thường, IDS được kết nối với bộ chuyển mạch (switch) nằm phía sau tường lửa để giám sát lưu lượng mạng hiệu quả.



Hình 2.1.1.a.1. Vị trí hệ thống IDS trong sơ đồ mạng

Nhiệm vụ chính của các hệ thống IDS bao gồm:

- Giám sát lưu lượng mạng hoặc các hành vi trên một hệ thống để nhận dạng các dấu hiệu của

tấn công, xâm nhập;

- Khi phát hiện các hành vi tấn công, xâm nhập, thì ghi logs các hành vi này cho phân tích bổ sung sau này;

- Gửi thông báo cho người quản trị về các hành vi tấn công, xâm nhập đã phát hiện được.

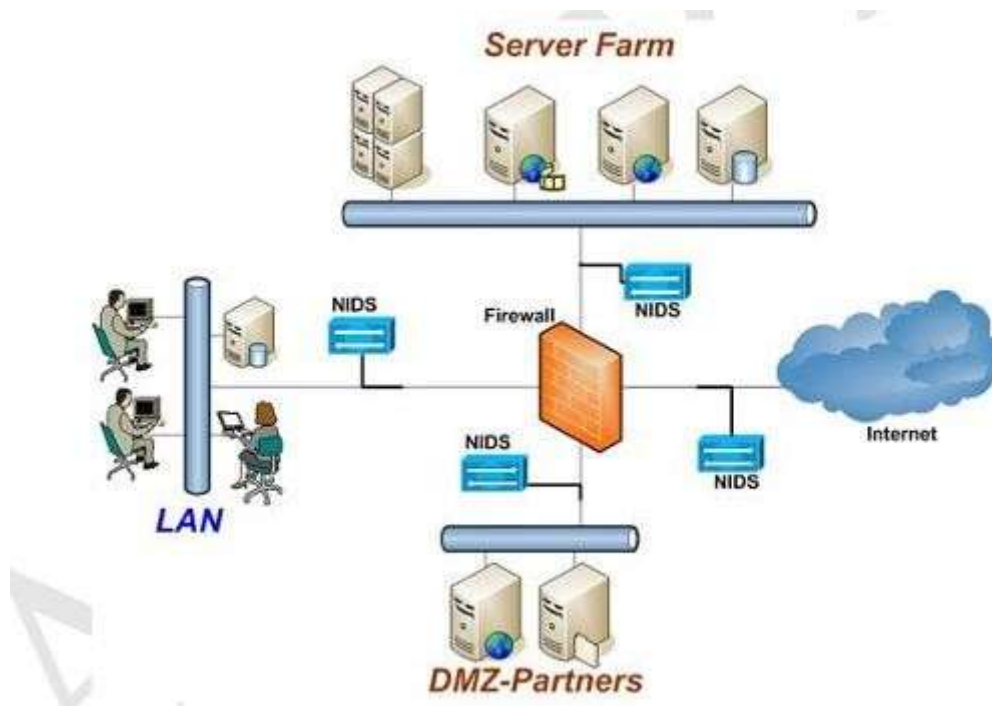
Nói tóm lại, IDS thường được kết nối vào các bộ định tuyến, switch, card mạng và chủ yếu làm nhiệm vụ giám sát và cảnh báo, không có khả năng chủ động ngăn chặn tấn công, xâm nhập.

b. Phân loại hệ thống phát hiện tấn công, xâm nhập

Có 2 phương pháp phân loại chính các hệ thống IDS gồm (1) phân loại theo nguồn dữ liệu và (2) phân loại theo phương pháp phân tích dữ liệu.

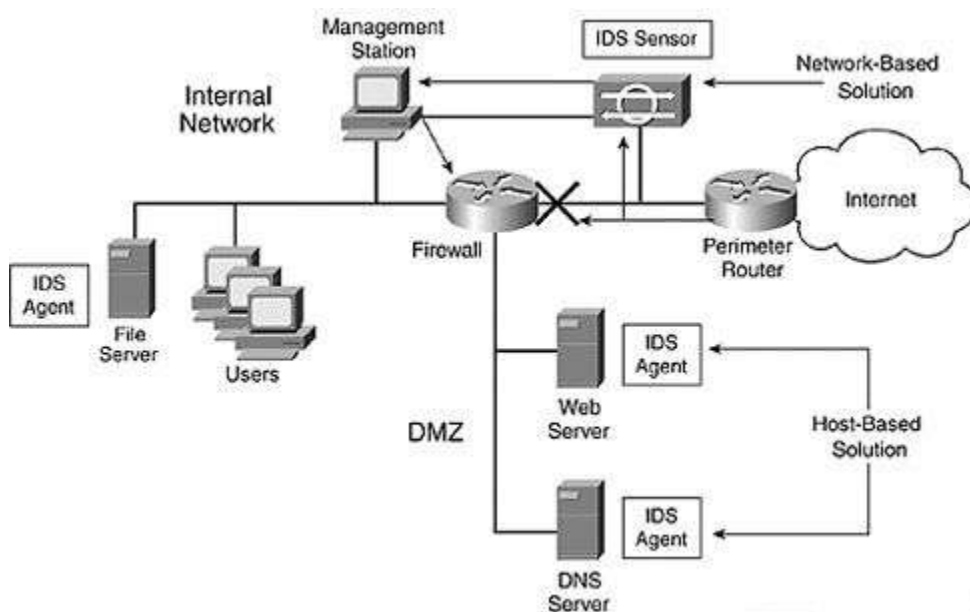
Theo nguồn dữ liệu, có 2 loại hệ thống phát hiện xâm nhập:

- Hệ thống phát hiện xâm nhập mạng (NIDS – Network-based IDS): NIDS phân tích lưu lượng mạng để phát hiện tấn công, xâm nhập cho cả mạng hoặc một phần mạng. Hình dưới đây biểu diễn một sơ đồ mạng, trong đó các NIDS được bố trí để giám sát phát hiện xâm nhập tại cổng vào và cho từng phân đoạn mạng.



Hình 2.1.1.b.1. Các NIDS được bố trí để giám sát phát hiện xâm nhập tại cổng vào và cho từng phân đoạn mạng

- HIDS giám sát các sự kiện xảy ra trên một hệ thống hoặc dịch vụ cụ thể để phát hiện các hành vi tấn công hoặc xâm nhập nhắm vào host đó. Trong sơ đồ mạng, **NIDS** được sử dụng để theo dõi lưu lượng tại cổng mạng, trong khi **HIDS** được triển khai trên các host thông qua các tác tử IDS (IDS agents). Một **trạm quản lý (Management Station)** được thiết lập để thu thập dữ liệu từ cả NIDS và HIDS, phân tích và đưa ra quyết định cuối cùng dựa trên thông tin thu thập được.



Hình 2.1.1.b.2. Sử dụng kết hợp NIDS và HIDS để giám sát lưu lượng mạng và các host

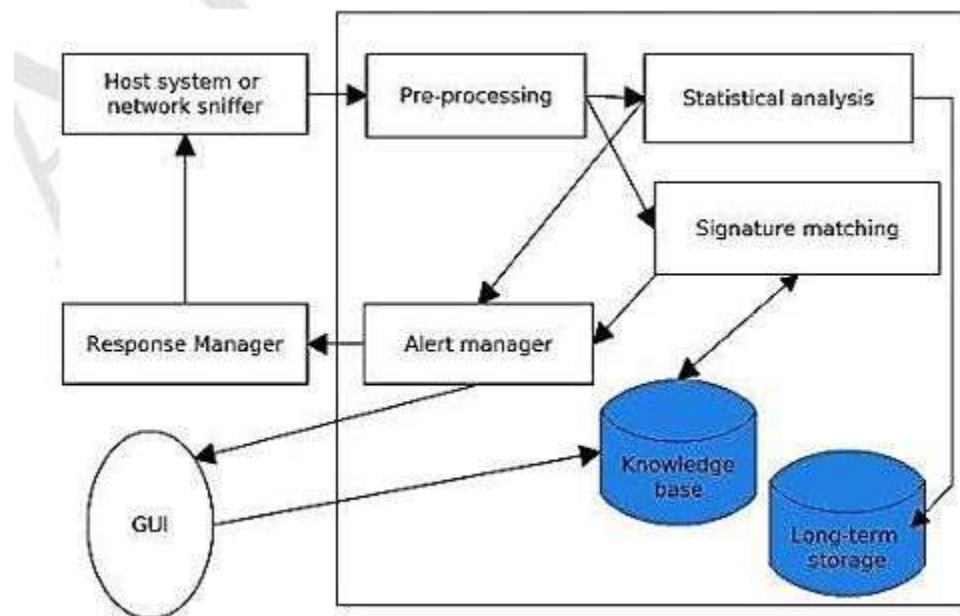
Theo phương pháp phân tích dữ liệu, có 2 kỹ thuật phân tích chính, gồm:

- Phát hiện xâm nhập dựa trên chữ ký, hoặc phát hiện sự lạm dụng (Signature-based / misuse intrusion detection)
- Phát hiện xâm nhập dựa trên các bất thường (Anomaly intrusion detection).

c. Các kỹ thuật phát hiện xâm nhập

c.1. Phát hiện xâm nhập dựa trên chữ ký

- Phương pháp phát hiện xâm nhập dựa trên chữ ký bắt đầu bằng việc xây dựng một cơ sở dữ liệu chữ ký (Knowledge base), chứa các dấu hiệu hoặc mẫu đặc trưng của các cuộc tấn công và xâm nhập đã biết. Các chữ ký này thường được tạo và mã hóa thủ công dưới dạng luật phát hiện (detection rules).
- Quá trình tiếp theo bao gồm việc sử dụng cơ sở dữ liệu chữ ký để theo dõi hành vi của hệ thống hoặc mạng. Nếu phát hiện bất kỳ hành vi nào khớp với chữ ký trong cơ sở dữ liệu, hệ thống sẽ đưa ra cảnh báo về khả năng tấn công hoặc xâm nhập.
- Sơ đồ quy trình điển hình của phương pháp này bao gồm Knowledge base, nơi lưu trữ các chữ ký tấn công và xâm nhập, được sử dụng để so sánh và phát hiện các mối đe dọa.



Hình 2.1.1.c.1. Lưu đồ giám sát phát hiện tấn công, xâm nhập dựa trên chữ ký

- Ưu điểm:

Phương pháp phát hiện xâm nhập dựa trên chữ ký nổi bật với khả năng phát hiện hiệu quả các cuộc tấn công và xâm nhập đã biết. Phương pháp này có tốc độ xử lý nhanh và chỉ yêu cầu tài nguyên tính toán thấp, giúp nó được ứng dụng rộng rãi trong thực tế.

- Nhược điểm:

Tuy nhiên, hạn chế lớn nhất là phương pháp này không thể phát hiện các cuộc tấn công hoặc xâm nhập mới, vì chữ ký của chúng chưa được lưu trong cơ sở dữ liệu. Ngoài ra, việc xây dựng và cập nhật cơ sở dữ liệu chữ ký đòi hỏi nhiều công sức và thời gian để duy trì tính chính xác và hiệu quả.

c.2. Phát hiện xâm nhập dựa trên bất thường

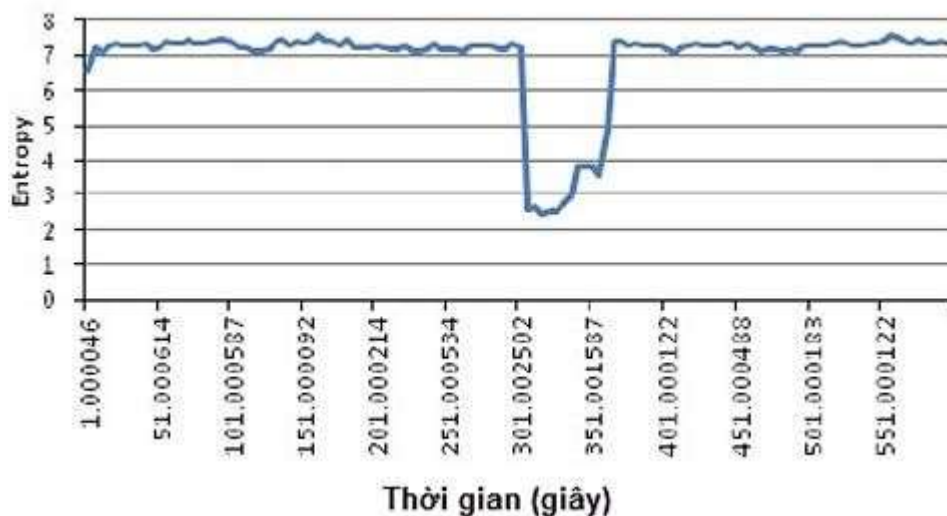
Phương pháp phát hiện xâm nhập dựa trên bất thường dựa trên giả định rằng các hành vi tấn công hoặc xâm nhập thường đi kèm với những hành vi bất thường. Quá trình triển khai hệ thống này bao gồm hai giai đoạn chính: huấn luyện và phát hiện.

- Giai đoạn huấn luyện:

Trong giai đoạn này, hệ thống xây dựng một hồ sơ (profile) mô tả hành vi bình thường của đối tượng (hệ thống hoặc mạng). Để làm được điều này, cần giám sát đối tượng trong một khoảng thời gian đủ dài để thu thập dữ liệu toàn diện về hành vi trong điều kiện bình thường. Dữ liệu này được sử dụng để huấn luyện và tạo ra một mô hình phát hiện, tức là hồ sơ đặc trưng của đối tượng.

- Giai đoạn phát hiện:

Hệ thống theo dõi các hành vi hiện tại của đối tượng và so sánh với hồ sơ đã được xây dựng. Nếu phát hiện sự khác biệt đáng kể giữa hành vi hiện tại và hành vi bình thường trong hồ sơ, hệ thống sẽ đưa ra cảnh báo về khả năng xảy ra tấn công hoặc xâm nhập.



Hình 2.1.1.c.2. Giá trị entropy của IP nguồn của các gói tin từ lưu lượng hợp pháp (phần giá trị cao, đều) và entropy của IP nguồn của các gói tin từ lưu lượng tấn công DDoS (phần giá trị thấp)

Hình trên biểu diễn giá trị entropy của IP nguồn của các gói tin theo cửa sổ trượt từ lưu lượng bình thường và entropy của IP nguồn của các gói tin từ lưu lượng tấn công DDoS. Có thể thấy sự khác biệt rõ nét giữa giá trị entropy của lưu lượng bình thường và lưu lượng tấn công và như vậy nếu một ngưỡng entropy được chọn phù hợp ta hoàn toàn có thể phát hiện sự xuất hiện của cuộc tấn công DDoS dựa trên sự thay đổi đột biến của giá trị entropy. Ưu điểm của phát hiện xâm nhập dựa trên bất thường là có tiềm năng phát hiện các loại tấn công, xâm nhập mới mà không yêu cầu biết trước thông tin về chúng. Tuy nhiên, phương pháp này thường có tỷ lệ cảnh báo sai tương đối cao so với phương pháp phát hiện dựa trên chữ ký. Điều này làm giảm khả năng ứng dụng thực tế của phát hiện xâm nhập dựa trên bất thường. Ngoài ra, phương pháp này cũng tiêu tốn nhiều tài nguyên hệ thống cho việc xây dựng hồ sơ đối tượng và phân tích hành vi hiện tại.

2.2.1. Tìm hiểu về kiến trúc và tính năng của một số hệ thống phát hiện tấn công, xâm nhập: Snort, OSSEC

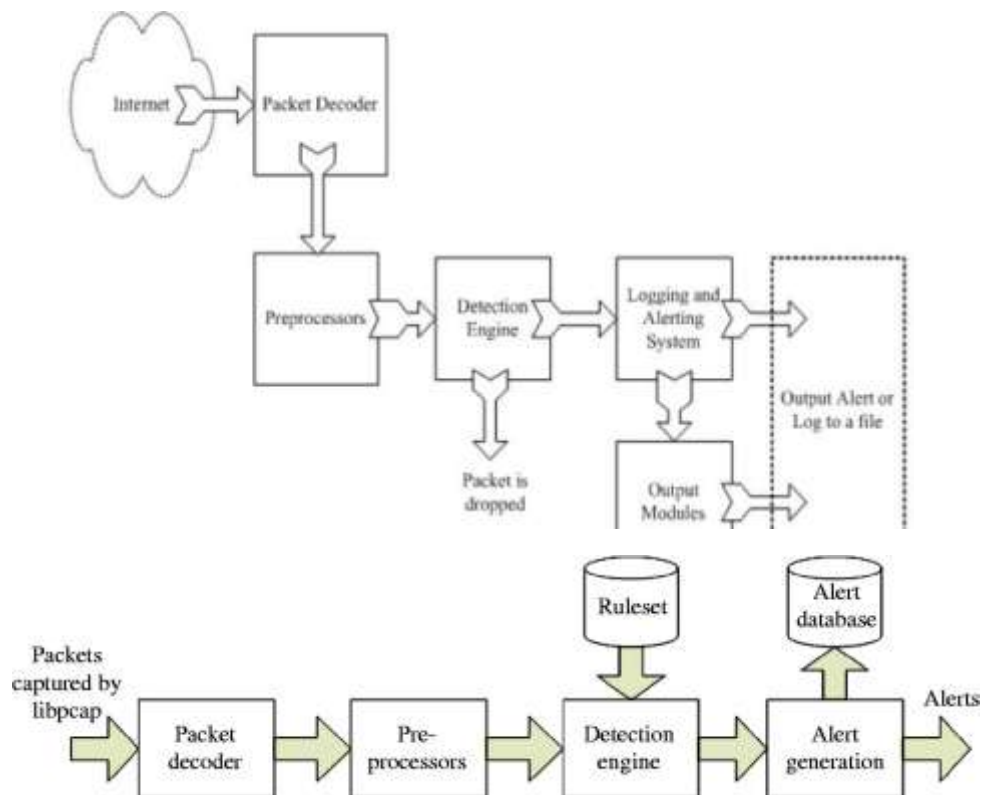
2.2.1.1. Snort

a. Giới thiệu

Snort là một công cụ IDS/IPS, thực hiện giám sát các gói tin ra vào hệ thống.

- Snort là một mã nguồn mở miễn phí với nhiều tính năng trong việc bảo vệ hệ thống bên trong, phát hiện sự tấn công từ bên ngoài vào hệ thống.
- Snort được viết bởi Martin Roesch vào năm 1998. Hiện tại, Snort được phát triển bởi Sourcefire, nơi mà Roesch đang là người sáng lập và CTO, và được sở hữu bởi Cisco từ năm 2013.

b. Kiến trúc của Snort



Trong mô hình kiến trúc trên, hệ thống Snort được chia thành 4 phần:

- Module Decoder: Xử lý giải mã các gói tin
- Module Preprocessors: Tiền xử lý
- Module Detection Engine: Phát hiện
- Module Logging and Alerting System: Lưu log và cảnh báo

c. Các luật của Snort

Cấu trúc của một rule được chia thành 02 phần: **[Rule header]****[Rule Option]**

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

Cấu trúc phần Header: **[Action]****[Protocol]****[Address]****[port]****[Direction]****[Address]****[Port]**

- Action: Thể hiện hành động sẽ được thực hiện khi một gói tin kích hoạt quy tắc. Trong đó:
 - + alert: Tạo một cảnh báo và ghi lại gói tin.
 - + log: Chỉ ghi lại gói tin mà không tạo cảnh báo.
 - + pass: Bỏ qua gói tin, không thực hiện hành động nào.

- + activate: Tạo ra cảnh báo và kích hoạt thêm các luật khác để kiểm tra thêm điều kiện của gói tin
- + dynamic: Đây là luật được gọi bởi các luật khác có Action khai báo là Activate
- Protocol: Xác định loại giao thức của gói tin, ví dụ: TCP, UDP, ICMP, hoặc any (tất cả).
- Source IP Address: Địa chỉ IP nguồn của gói tin.
- Source Port: Cổng nguồn của gói tin. Có thể là một số cụ thể hoặc từ khoảng cụ thể.
- Direction Operator: Thể hiện hướng của gói tin. Có thể là (đích tới (nguồn tới đích) hoặc nguồn). <- ->
- Destination IP Address: Địa chỉ IP đích của gói tin.
- Destination Port: Cổng đích của gói tin. Cũng có thể là một số cụ thể hoặc từ khoảng cụ thể.

Cấu trúc phần Option:

Phần Option nằm ngay sau phần Header và được bao bọc trong dấu ngoặc đơn. Nếu có nhiều Option thì sẽ phân biệt bởi dấu chấm phẩy ";". Một Option gồm có 2 phần: một là từ khóa và một là tham số. 02 phần này sẽ phân cách nhau bằng dấu hai chấm ":"

Các option có thể là: **msg** (tin nhắn cảnh báo), **content** (nội dung gói tin), **sid** (số nhận dạng duy nhất), **rev** (số phiên bản quy tắc), **content:** Chứa một chuỗi hoặc byte pattern để so khớp với dữ liệu gói tin ...

Ví dụ về cấu trúc một quy tắc Snort:

```
alert tcp any any -> any 80 (msg:"Potential Web Attack"; content:"/bin/bash"; sid:100001;)
```

2.2.1.2. Ossec

a. Ossec là gì?

OSSEC là phần mềm mã nguồn mở giúp phát hiện xâm nhập dựa trên host (HIDS) Nó đa nền tảng, có thể mở rộng và có nhiều cơ chế bảo mật khác nhau.

b. Các tính năng của Ossec

- Log based Intrusion Detection (LIDs) and Log Monitoring:
- + Chủ động theo dõi và phân tích dữ liệu real-time từ nhiều nguồn sinh log.
- + Ngoài ra, Ossec sẽ thu thập, phân tích và kiểm tra mối tương quan các log và cho ta biết những điều đáng ngờ đang xảy ra trong hệ thống (bị tấn công, lỗi, sử dụng sai,...), các phần mềm được cài đặt thêm, các rule firewall bị đổi.
- Compliance Auditing:

- + Kiểm soát các ứng dụng và hệ thống nhằm tuân thủ các yêu cầu, tiêu chuẩn về bảo mật như PCI-DSS và CIS.
- Rootkit and Malware Detection:
 - + Tin tặc thường muốn che dấu hành động và quay lại hệ thống đã xâm nhập được
 - + Ossec phân tích ở cấp độ file và tiến trình nhằm phát hiện các ứng dụng độc hại, các rootkit hay các file hệ thống bị sửa đổi theo cách phổ biến với rootkit
- File Integrity Monitoring (FIM):
 - + Phát hiện các thay đổi đối với hệ thống.
- Active Response:
 - + Các hành vi ứng phó lại các cuộc tấn công vào hệ thống trong thời gian thực.
 - + Giúp ngăn sự cố lan rộng trước khi admin có thể hành động
- System Inventory:
 - + Thu thập các thông tin hệ thống như phần mềm được cài đặt, hardware,...

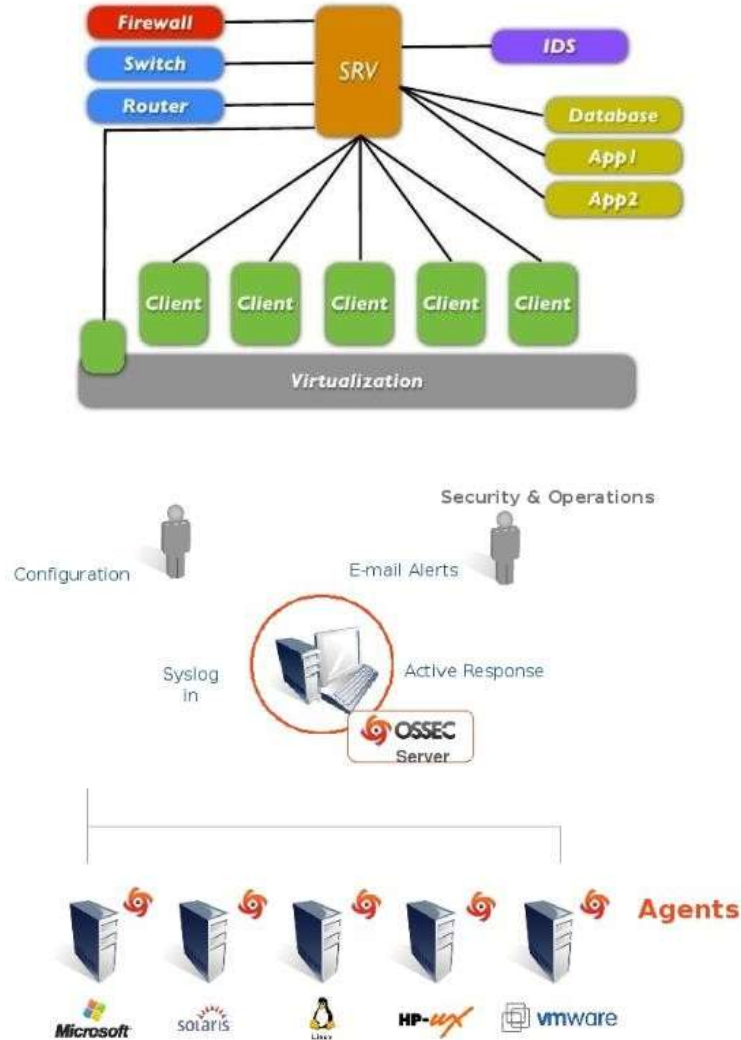
c. Điểm nổi trội của Ossec

- Đa nền tảng (Linux, Mac OS, Window, Solaris)
- Real-time Alert (Cảnh báo thời gian thực)
- + Kết hợp với smtp, sms, syslog sẽ cho phép người dùng nhận cảnh báo trên các thiết bị có hỗ trợ email
- + Ngoài ra tính năng Active-response có thể giúp block 1 cuộc tấn công ngay lập tức.
- Có thể tích hợp với các hệ thống hiện đại (SIM/SEM)
- Mô hình Server – Agent/Agentless, cho phép Server dễ dàng quản lý tập trung các chính sách trên nhiều OS.
- Giám sát trên agent, agentless (Client không cài đặt được gói agent) như router, firewall

d. Kiến trúc và mô hình hoạt động của Ossec

Ossec hoạt động theo mô hình Server-Agent/Agentless

OSSEC Architecture



Hình 2.1.2.2.1. Kiến trúc của OSSEC

❖ Manager (Server)

- Lưu trữ cơ sở dữ liệu của việc kiểm tra tính toàn vẹn file Kiểm tra các log, event.
- Quản lý, lưu tất cả các rule, decoder (bộ giải mã), cấu hình chính. Điều này giúp dễ dàng quản lý, dù cho có lượng lớn Agent
- Server không chạy trên Windows OS.

❖ Agent

Bản chất thì là 1 phần mềm được cài đặt trên máy client giúp thu thập các thông tin và gửi cho Server để phân tích, thống kê.

- Chiếm lượng memory và CPU nhỏ, không đáng kể
- 1 số thông tin được thu thập theo thời gian thực
- 1 số thông tin thì lại được thu thập định kỳ
- Nhưng khi nói Agent thì là để chỉ máy Client được cài gói Ossec-agent.

Chú ý: Windows OS chỉ có thể làm Agent chứ không làm Server được.

❖ Agentless

Là các hệ thống không cài được gói agent

Trên các Agentless này có thể thực hiện việc kiểm tra tính toàn vẹn Giúp monitor firewall, router hay thậm chí cả hệ thống Unix

❖ Ảo hóa/ VMware

- Cho phép cài đặt agent trên các guest OS (Máy ảo)
- Ngoài ra cũng được cài đặt trong VMware ESX nhưng có thể dẫn đến sự cố không hỗ trợ.
- Khi cài đặt trong VMware ESX giúp nhận được thời điểm các VM guest được khởi tạo, xóa đi, khởi động,... Ossec cũng giám sát việc login, logouts và các lỗi bên trong ESX server

Ngoài ra nó cũng cảnh báo nếu bất kỳ tùy chọn cấu hình không an toàn nào được bật.

❖ Firewalls, switches and routers

- Chính là các Agentless
- Ossec có thể nhận và phân tích nhật ký hệ thống từ nhiều firewall, switch, router.
- Nó support tất cả Cisco routers, Cisco PIX, Cisco FWSM, Cisco ASA, Juniper Routers, Netscreen firewall, Checkpoint và nhiều thiết bị khác.

2.3. Nội dung thực hành

2.3.1. Chuẩn bị môi trường

- 01 máy tính (máy thật hoặc máy ảo) chạy Linux với RAM tối thiểu 2GB, 10GB đĩa cứng có kết nối mạng (LAN hoặc Internet): IP 192.168.17.176
- 01 máy tính (máy thật hoặc máy ảo) chạy Kali Linux (bản 2021 trở lên): IP 192.168.17.175
- Bộ phần mềm Snort

2.3.2. Các bước thực hiện

- a. Bước 1:** Chuẩn bị các máy tính như mô tả trong mục 2.2.1. Các máy có địa chỉ IP và kết nối mạng LAN.

```
rtt min/avg/max/mdev = 0.369/0.499/0.601/0.096 ms
(ducnam@B22DCAT206-PhamDucNam-Kali)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.100.3 netmask 255.255.255.0 broadcast 192.168.100.255
    inet6 fe80::20c:29ff:fe44:1be3 prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:44:1b:e3 txqueuelen 1000 (Ethernet)
    RX packets 1369 bytes 86521 (84.4 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 3746 bytes 167989 (164.0 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
    device interrupt 19 base 0x2000

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 2422 bytes 244434 (238.7 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 2422 bytes 244434 (238.7 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```



```
192.168.100.147
05/20-23:57:56.930280  [**] [1:1000001:1] B22DCAT206-NamPD phat hien co cac goi ping den [**] [Priority: 0]
192.168.100.147
ducnam@B22DCAT206-PhamDucNam-Snort:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 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
        valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UNKNOWN group default qlen 1000
    link/ether 00:0c:29:91:e7:10 brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 192.168.100.147/24 brd 192.168.100.255 scope global noprefixroute ens33
        valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fe91:e710/64 scope link
        valid_lft forever preferred_lft forever
ducnam@B22DCAT206-PhamDucNam-Snort:~$
```

Hình 1 cấu hình ip

b. Bước 2: Tải, cài đặt Snort và chạy thử Snort. Kiểm tra log của Snort để đảm bảo Snort hoạt động bình thường.

- Tải snort:
- + sudo apt update
- + sudo apt install snort
- Kiểm tra phiên bản của snort

```
Snort configuration: interface default not set, using 'ens33'
Processing triggers for man-db (2.10.2-1) ...
Processing triggers for libc-bin (2.35-0ubuntu3.8) ...
ducnam@B22DCAT206-PhamDucNam-Snort:~$ snort --version

  ,,-_
o"  )~
  ' ' '

ved.

-*> Snort! <*-
Version 2.9.15.1 GRE (Build 15125)
By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
Copyright (C) 2014-2019 Cisco and/or its affiliates. All rights reserved.

Copyright (C) 1998-2013 Sourcefire, Inc., et al.
Using libpcap version 1.10.1 (with TPACKET_V3)
Using PCRE version: 8.39 2016-06-14
Using ZLIB version: 1.2.11

ducnam@B22DCAT206-PhamDucNam-Snort:~$
```

Hình 2 Kiểm tra phiên bản Snort

- Kiểm tra trạng thái của snort


```

ducnam@B22DCAT206-PhamDucNam-Snort:~$ sudo systemctl status snort
● snort.service - LSB: Lightweight network intrusion detection system
   Loaded: loaded (/etc/init.d/snort; generated)
   Active: active (running) since Tue 2025-05-20 23:01:49 +07; 44s ago
     Docs: man:systemd-sysv-generator(8)
  Process: 4525 ExecStart=/etc/init.d/snort start (code=exited, status=0/SUCCESS)
    Tasks: 2 (limit: 4551)
   Memory: 78.9M
      CPU: 683ms
    CGroup: /system.slice/snort.service
            └─4545 /usr/sbin/snort -m 027 -D -d -l /var/log/snort -u snort -g >

Thg 5 20 23:01:50 B22DCAT206-PhamDucNam-Snort snort[4545]:      Preproces>
Thg 5 20 23:01:50 B22DCAT206-PhamDucNam-Snort snort[4545]:      Preproces>
Thg 5 20 23:01:50 B22DCAT206-PhamDucNam-Snort snort[4545]:      Preproces>
Thg 5 20 23:01:50 B22DCAT206-PhamDucNam-Snort snort[4545]:      Preproces>
Thg 5 20 23:01:50 B22DCAT206-PhamDucNam-Snort snort[4545]:      Preproces>
Thg 5 20 23:01:50 B22DCAT206-PhamDucNam-Snort snort[4545]:      Preproces>
Thg 5 20 23:01:50 B22DCAT206-PhamDucNam-Snort snort[4545]:      Preproces>
Thg 5 20 23:01:50 B22DCAT206-PhamDucNam-Snort snort[4545]:      Preproces>

```

Hình 3 kiểm tra trạng thái Snort

- **Chỉnh sửa cấu hình snort**

```

60 # Note to Debian users: this value is overridden when starting
61 # up the Snort daemon through the init.d script by the
62 # value of DEBIAN_SNORT_HOME_NET s defined in the
63 # /etc/snort/snort.debian.conf configuration file
64 #
65 ipvar HOME_NET 192.168.100.147
66
67 # Set up the external network addresses. Leave as "any" in most situations
68 ipvar EXTERNAL_NET any
69 # If HOME_NET is defined as something other than "any", alternative, you can
70 # use this definition if you do not want to detect attacks from your internal
71 # IP addresses:
72 #ipvar EXTERNAL_NET !$HOME_NET
73
74 # List of DNS servers on your network
75 ipvar DNS_SERVERS $HOME_NET
76
77 # List of SMTP servers on your network
78 ipvar SMTP_SERVERS $HOME_NET
79
80 # List of web servers on your network
81 ipvar HTTP_SERVERS $HOME_NET

```

– Kiểm tra cấu hình snort: `sudo snort -T -i ens33 -c /etc/snort/snort.conf`

```

ducham@B22DCAT206-PhamDucNam-Snort: ~
|
| Patterns      : 0.51
| Match Lists   : 1.01
| DFA
|   1 byte states : 1.02
|   2 byte states : 13.96
|   4 byte states : 0.00
|
+-----+
[ Number of patterns truncated to 20 bytes: 1038 ]

--== Initialization Complete ==--

o" )~  -> Snort! <*-
'""'  Version 2.9.15.1 GRE (Build 15125)
      By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
      Copyright (C) 2014-2019 Cisco and/or its affiliates. All rights reserved.
      Copyright (C) 1998-2013 Sourcefire, Inc., et al.
      Using libpcap version 1.10.1 (with TPACKET_V3)
      Using PCRE version: 8.39 2016-06-14
      Using ZLIB version: 1.2.11

Rules Engine: SF_SNORT_DETECTION_ENGINE Version 3.1 <Build 1>
Preprocessor Object: SF_REPUTATION Version 1.1 <Build 1>
Preprocessor Object: SF_SSLPP Version 1.1 <Build 4>
Preprocessor Object: SF_FTPTELNET Version 1.2 <Build 13>
Preprocessor Object: SF_POP Version 1.0 <Build 1>
Preprocessor Object: SF_GTP Version 1.1 <Build 1>
Preprocessor Object: SF_DCERPC2 Version 1.0 <Build 3>
Preprocessor Object: SF_SIP Version 1.1 <Build 1>
Preprocessor Object: SF_SMTP Version 1.1 <Build 9>
Preprocessor Object: SF_SDF Version 1.1 <Build 1>
Preprocessor Object: SF_IMAP Version 1.0 <Build 1>
Preprocessor Object: SF_DNP3 Version 1.1 <Build 1>
Preprocessor Object: appid Version 1.1 <Build 5>
Preprocessor Object: SF_MODBUS Version 1.1 <Build 1>
Preprocessor Object: SF_DNS Version 1.1 <Build 4>
Preprocessor Object: SF_SSH Version 1.1 <Build 3>

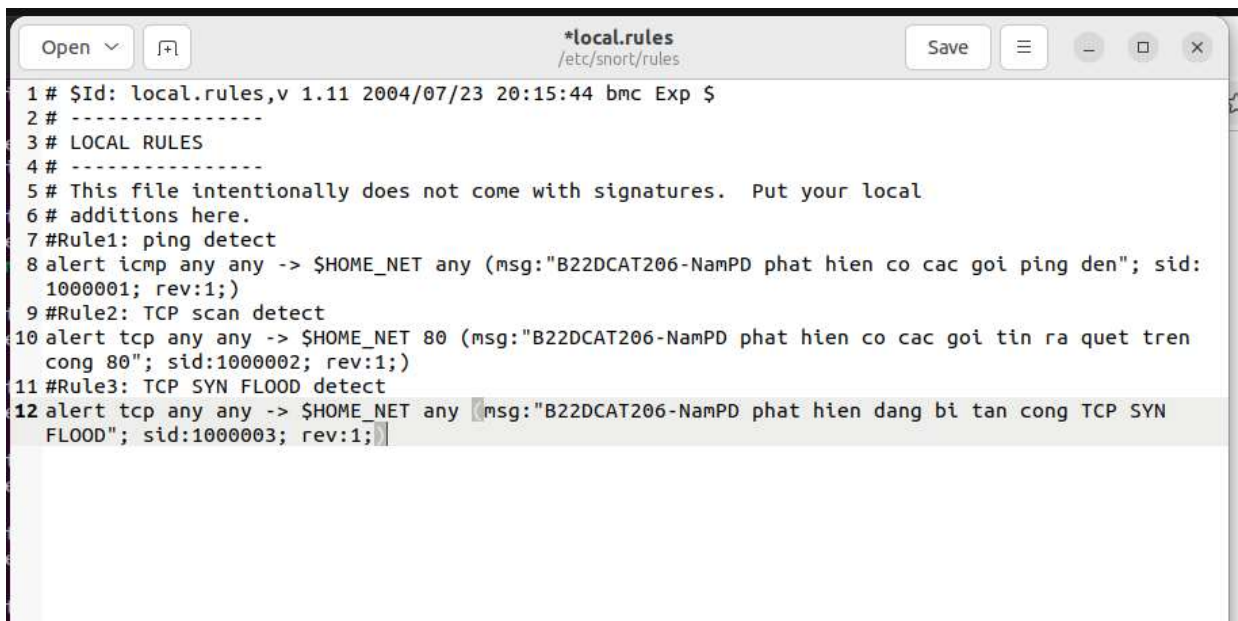
Snort successfully validated the configuration!
Snort exiting
ducham@B22DCAT206-PhamDucNam-Snort: ~$

```

Hình 4 Kiểm tra phiên bản Snort

c. Bước 3: Tạo các luật Snort để phát hiện 3 dạng rà quét, tấn công hệ thống

- Yêu cầu:
 - + Phát hiện các gói tin ping từ bất kỳ một máy nào gửi đến máy chạy Snort. Hiện thị thông điệp khi phát hiện: “B22DCAT206-PhamDucNam-Snort phát hiện có các gói Ping gửi đến.”
 - + Phát hiện các gói tin rà quét từ bất kỳ một máy nào gửi đến máy chạy Snort trên cổng 80. Hiện thị thông điệp khi phát hiện: “ B22DCAT206- PhamDucNam-Snort phát hiện có các gói tin rà quét trên cổng 80.”
 - + Phát hiện tấn công TCP SYN Flood từ bất kỳ một máy nào gửi đến máy chạy Snort. Hiện thị thông điệp khi phát hiện: “B22DCAT206-PhamDucNam- Snort phát hiện đang bị tấn công TCP SYN Flood.”
- Mở file để tạo thêm luật: *sudo gedit /etc/snort/rules/local.rules*



```
1 # $Id: local.rules,v 1.11 2004/07/23 20:15:44 bmc Exp $
2 # -----
3 # LOCAL RULES
4 # -----
5 # This file intentionally does not come with signatures. Put your local
6 # additions here.
7 #Rule1: ping detect
8 alert icmp any any -> $HOME_NET any (msg:"B22DCAT206-NamPD phat hien co cac goi ping den"; sid:
  1000001; rev:1;)
9 #Rule2: TCP scan detect
10 alert tcp any any -> $HOME_NET 80 (msg:"B22DCAT206-NamPD phat hien co cac goi tin ra quet tren
   cong 80"; sid:1000002; rev:1;)
11 #Rule3: TCP SYN FLOOD detect
12 alert tcp any any -> $HOME_NET any (msg:"B22DCAT206-NamPD phat hien dang bi tan cong TCP SYN
   FLOOD"; sid:1000003; rev:1;)
```

Hình 5 chỉnh sửa rule

d. Bước 4: Thực thi tấn công và phát hiện sử dụng Snort.

- Từ máy Kali, sử dụng lệnh ping để ping máy Snort. Trên máy Snort kiểm tra kết quả phát hiện trên giao diện terminal hoặc log của Snort.


```

Snort successfully validated the configuration!
Snort exiting
ducnam@B22DCAT206-PhamDucNam-Snort:~$ ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.100.147 netmask 255.255.255.0 broadcast 192.168.100.255
    inet6 fe80::20c:29ff:fe91:e710 prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:91:e7:10 txqueuelen 1000 (Ethernet)
    RX packets 16280 bytes 18074709 (18.0 MB)
    RX errors 17 dropped 0 overruns 0 frame 0
    TX packets 7128 bytes 514253 (514.2 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
    device interrupt 19 base 0x2000

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 3026 bytes 268156 (268.1 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 3026 bytes 268156 (268.1 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

ducnam@B22DCAT206-PhamDucNam-Snort:~$

```

Hình 6 Kiểm tra địa chỉ IP máy Snort

```

2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 0.793/1.286/1.779/0.493 ms

(ducnam@ B22DCAT206-PhamDucNam-Kali)-[~]
$ ping 192.168.100.147
PING 192.168.100.147 (192.168.100.147) 56(84) bytes of data.
64 bytes from 192.168.100.147: icmp_seq=1 ttl=64 time=0.308 ms
64 bytes from 192.168.100.147: icmp_seq=2 ttl=64 time=0.410 ms
64 bytes from 192.168.100.147: icmp_seq=3 ttl=64 time=0.248 ms
64 bytes from 192.168.100.147: icmp_seq=4 ttl=64 time=0.284 ms
64 bytes from 192.168.100.147: icmp_seq=5 ttl=64 time=1.01 ms
64 bytes from 192.168.100.147: icmp_seq=6 ttl=64 time=1.24 ms
64 bytes from 192.168.100.147: icmp_seq=7 ttl=64 time=0.882 ms
64 bytes from 192.168.100.147: icmp_seq=8 ttl=64 time=0.502 ms
64 bytes from 192.168.100.147: icmp_seq=9 ttl=64 time=0.723 ms
64 bytes from 192.168.100.147: icmp_seq=10 ttl=64 time=0.979 ms
^Z
zsh: suspended ping 192.168.100.147

(ducnam@ B22DCAT206-PhamDucNam-Kali)-[~]
$

```

Hình 7 Trên máy Kali, thực hiện Ping đến máy cài Snort

Khởi động snort bằng lệnh: `sudo snort -A console -q -c /etc/snort/snort.conf -i ens33`

```
/20-23:26:15.859704  [**] [1:527:8] BAD-TRAFFIC same SRC/DST [**] [Classification: Potentially Bad Traffic]
} :: -> ff02::16
/20-23:26:15.886232  [**] [1:527:8] BAD-TRAFFIC same SRC/DST [**] [Classification: Potentially Bad Traffic]
} :: -> ff02::1:ff91:e710
/20-23:26:16.622293  [**] [1:527:8] BAD-TRAFFIC same SRC/DST [**] [Classification: Potentially Bad Traffic]
} :: -> ff02::16
/20-23:29:14.735527  [**] [1:527:8] BAD-TRAFFIC same SRC/DST [**] [Classification: Potentially Bad Traffic]
} :: -> ff02::16
/20-23:29:14.971848  [**] [1:527:8] BAD-TRAFFIC same SRC/DST [**] [Classification: Potentially Bad Traffic]
} :: -> ff02::16
/20-23:29:15.035478  [**] [1:527:8] BAD-TRAFFIC same SRC/DST [**] [Classification: Potentially Bad Traffic]
} :: -> ff02::1:ff44:1be3
/20-23:57:48.900972  [**] [1:1000001:1] B22DCAT206-NamPD phat hien co cac goi ping den [**] [Priority: 0]
2.168.100.147
/20-23:57:49.901472  [**] [1:1000001:1] B22DCAT206-NamPD phat hien co cac goi ping den [**] [Priority: 0]
2.168.100.147
/20-23:57:50.903133  [**] [1:1000001:1] B22DCAT206-NamPD phat hien co cac goi ping den [**] [Priority: 0]
2.168.100.147
/20-23:57:51.904599  [**] [1:1000001:1] B22DCAT206-NamPD phat hien co cac goi ping den [**] [Priority: 0]
2.168.100.147
/20-23:57:52.905681  [**] [1:1000001:1] B22DCAT206-NamPD phat hien co cac goi ping den [**] [Priority: 0]
2.168.100.147
/20-23:57:53.907518  [**] [1:1000001:1] B22DCAT206-NamPD phat hien co cac goi ping den [**] [Priority: 0]
2.168.100.147
/20-23:57:54.927784  [**] [1:1000001:1] B22DCAT206-NamPD phat hien co cac goi ping den [**] [Priority: 0]
2.168.100.147
/20-23:57:55.928683  [**] [1:1000001:1] B22DCAT206-NamPD phat hien co cac goi ping den [**] [Priority: 0]
2.168.100.147
/20-23:57:56.930280  [**] [1:1000001:1] B22DCAT206-NamPD phat hien co cac goi ping den [**] [Priority: 0]
2.168.100.147
```

Hình 8 Trên máy Snort hiện các cảnh báo

- Từ máy Kali, sử dụng công cụ nmap để rà quét máy Snort (dùng lệnh: `nmap -sV -p80 -A 192.168.17.176`). Trên máy Snort kiểm tra kết quả phát hiện trên giao diện terminal hoặc log của Snort.

```
192.168.100.147
05/20-23:57:56.930280  [**] [1:1000001:1] B22DCAT206-NamPD phat hien co cac goi ping den [**] [Priority: 0]
192.168.100.147
ducnam@B22DCAT206-PhamDucNam-Snort:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 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
        valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UNKNOWN group default qlen 1000
    link/ether 00:0c:29:91:e7:10 brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 192.168.100.147/24 brd 192.168.100.255 scope global noprefixroute ens33
        valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fe91:e710/64 scope link
        valid_lft forever preferred_lft forever
ducnam@B22DCAT206-PhamDucNam-Snort:~$
```

Hình 9 Kiểm tra địa chỉ IP máy Snort


```
ducnam@B22DCAT206-PhamDucNam-Kali: ~  
File Actions Edit View Help  
  
(ducnam@ B22DCAT206-PhamDucNam-Kali)-[~]  
$ nmap -sV -p80 -A 192.168.100.147  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-05-20 10:01 PDT  
Nmap scan report for 192.168.100.147  
Host is up (0.00072s latency).  
  
PORT      STATE SERVICE VERSION  
80/tcp    open  http    Apache httpd 2.4.52 ((Ubuntu))  
|_http-title: Apache2 Ubuntu Default Page: It works  
|_http-server-header: Apache/2.4.52 (Ubuntu)  
MAC Address: 00:0C:29:91:E7:10 (VMware)  
Warning: OSScan results may be unreliable because we could not find at least  
1 open and 1 closed port  
Device type: general purpose  
Running: Linux 4.X|5.X  
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5  
OS details: Linux 4.15 - 5.8  
Network Distance: 1 hop  
  
TRACEROUTE  
HOP RTT      ADDRESS  
1 0.72 ms 192.168.100.147  
  
OS and Service detection performed. Please report any incorrect results at ht  
tps://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 21.13 seconds
```

Hình 10 Trên máy Kali, sử dụng công cụ nmap để rà quét máy Snort: nmap -sV

```

21-00:01:21.299607  [**] [1:1000003:1] B22DCAT206-NamPD phát hiện đang bị tấn công TCP SYN FLOOD [**] [P
00.3:41470 -> 192.168.100.147:80
/21-00:01:21.299607  [**] [1:1000002:1] B22DCAT206-NamPD phát hiện có các gói tin ra quét trên cổng 80 [
168.100.3:41470 -> 192.168.100.147:80
/21-00:01:21.299608  [**] [1:1000003:1] B22DCAT206-NamPD phát hiện đang bị tấn công TCP SYN FLOOD [**] [P
00.3:41470 -> 192.168.100.147:80
/21-00:01:21.299608  [**] [1:1000002:1] B22DCAT206-NamPD phát hiện có các gói tin ra quét trên cổng 80 [
168.100.3:41470 -> 192.168.100.147:80
/21-00:01:21.301039  [**] [1:1000003:1] B22DCAT206-NamPD phát hiện đang bị tấn công TCP SYN FLOOD [**] [P
00.3:41470 -> 192.168.100.147:80
/21-00:01:21.301039  [**] [1:1000002:1] B22DCAT206-NamPD phát hiện có các gói tin ra quét trên cổng 80 [
168.100.3:41470 -> 192.168.100.147:80
/21-00:01:21.301378  [**] [1:1000003:1] B22DCAT206-NamPD phát hiện đang bị tấn công TCP SYN FLOOD [**] [P
00.3:41470 -> 192.168.100.147:80
/21-00:01:21.301378  [**] [1:1000002:1] B22DCAT206-NamPD phát hiện có các gói tin ra quét trên cổng 80 [
168.100.3:41470 -> 192.168.100.147:80
ducnam@B22DCAT206-PhamDucNam-Snort:~$

```

Hình 11 Trên máy Snort, hiện cảnh báo

- Từ máy Kali, sử dụng công cụ hping3 để tấn công TCP SYN Flood máy Snort (dùng lệnh: hping3 -c 15000 -d 120 -S -w 64 -p 80 --flood --rand-source 192.168.17.176). Trên máy Snort kiểm tra kết quả phát hiện trên giao diện terminal hoặc log của Snort.

```

05/20-23:57:56.930280  [**] [1:1000001:1] B22DCAT206-NamPD phát hiện có các gói ping đen [**] [Priority: 0]
192.168.100.147
ducnam@B22DCAT206-PhamDucNam-Snort:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 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
        valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UNKNOWN group default qlen 1000
    link/ether 00:0c:29:91:e7:10 brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 192.168.100.147/24 brd 192.168.100.255 scope global noprefixroute ens33
        valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fe91:e710/64 scope link
        valid_lft forever preferred_lft forever
ducnam@B22DCAT206-PhamDucNam-Snort:~$

```

Hình 12 Kiểm tra IP máy Snort

```
command 'sudo' from deb sudo-ldap
Try: sudo apt install <deb name>

(ducnam@B22DCAT206-PhamDucNam-Kali)-[~]
$ sudo hping3 -c 15000 -d 120 -S -w 64 -p 80 --flood --rand-source 192.168.100.147
sudo: unable to resolve host B22DCAT206-PhamDucNam-Kali: Temporary failure in name resolution
[sudo] password for ducnam:
HPING 192.168.100.147 (eth0 192.168.100.147): S set, 40 headers + 120 data bytes
hping in flood mode, no replies will be shown
```

Hình 13 Từ máy Kali, sử dụng công cụ hping3 để tấn công TCP SYN Flood máy Snort (dùng lệnh: hping3 -c 15000 -d 120 -S -w 64 -p 80 --flood --rand-source 192.168.17.176).

```
05/21-00:07:19.987303  [**] [1:1000003:1] B22DCAT206-NamPD phát hiện đang bị tấn công TCP SYN FLOOD [**] [P
.107.243:23167 -> 192.168.100.147:80
05/21-00:07:19.987303  [**] [1:1000002:1] B22DCAT206-NamPD phát hiện có các gói tin ra quét trên cổng 80 [P
3.142.107.243:23167 -> 192.168.100.147:80
05/21-00:07:19.987308  [**] [1:1000003:1] B22DCAT206-NamPD phát hiện đang bị tấn công TCP SYN FLOOD [**] [P
61.187:23168 -> 192.168.100.147:80
05/21-00:07:19.987308  [**] [1:1000002:1] B22DCAT206-NamPD phát hiện có các gói tin ra quét trên cổng 80 [P
.76.161.187:23168 -> 192.168.100.147:80
05/21-00:07:19.987313  [**] [1:1000003:1] B22DCAT206-NamPD phát hiện đang bị tấn công TCP SYN FLOOD [**] [P
.188.124:23169 -> 192.168.100.147:80
05/21-00:07:19.987313  [**] [1:1000002:1] B22DCAT206-NamPD phát hiện có các gói tin ra quét trên cổng 80 [P
3.164.188.124:23169 -> 192.168.100.147:80
05/21-00:07:19.987319  [**] [1:1000003:1] B22DCAT206-NamPD phát hiện đang bị tấn công TCP SYN FLOOD [**] [P
160.107:23170 -> 192.168.100.147:80
05/21-00:07:19.987319  [**] [1:1000002:1] B22DCAT206-NamPD phát hiện có các gói tin ra quét trên cổng 80 [P
.182.160.107:23170 -> 192.168.100.147:80
05/21-00:07:19.987323  [**] [1:1000003:1] B22DCAT206-NamPD phát hiện đang bị tấn công TCP SYN FLOOD [**] [P
225.79:23171 -> 192.168.100.147:80
05/21-00:07:19.987323  [**] [1:1000002:1] B22DCAT206-NamPD phát hiện có các gói tin ra quét trên cổng 80 [P
.234.225.79:23171 -> 192.168.100.147:80
05/21-00:07:19.987328  [**] [1:1000003:1] B22DCAT206-NamPD phát hiện đang bị tấn công TCP SYN FLOOD [**] [P
176.204:23172 -> 192.168.100.147:80
05/
```

Hình 14 Trên máy Snort hiện các thông báo

3. Kết luận

- Hệ thống phát hiện xâm nhập Snort hoạt động ổn định.
- Các luật mới được tạo và lưu vào trong file luật của Snort.
- Snort phát hiện thành công các rà quét tấn công kẻ trên.

4. Tài liệu tham khảo

- [1]. Chương 5, Giáo trình Cơ sở an toàn thông tin, Học viện Công nghệ BVCT, 2020. [2].
Suricata: <https://suricata.io/documentation/>
[3]. Snort: <https://www.snort.org/#documents>
[4]. OSSEC: <https://www.ossec.net/docs/>
[5]. Wazuh: <https://documentation.wazuh.com/current/index.html>