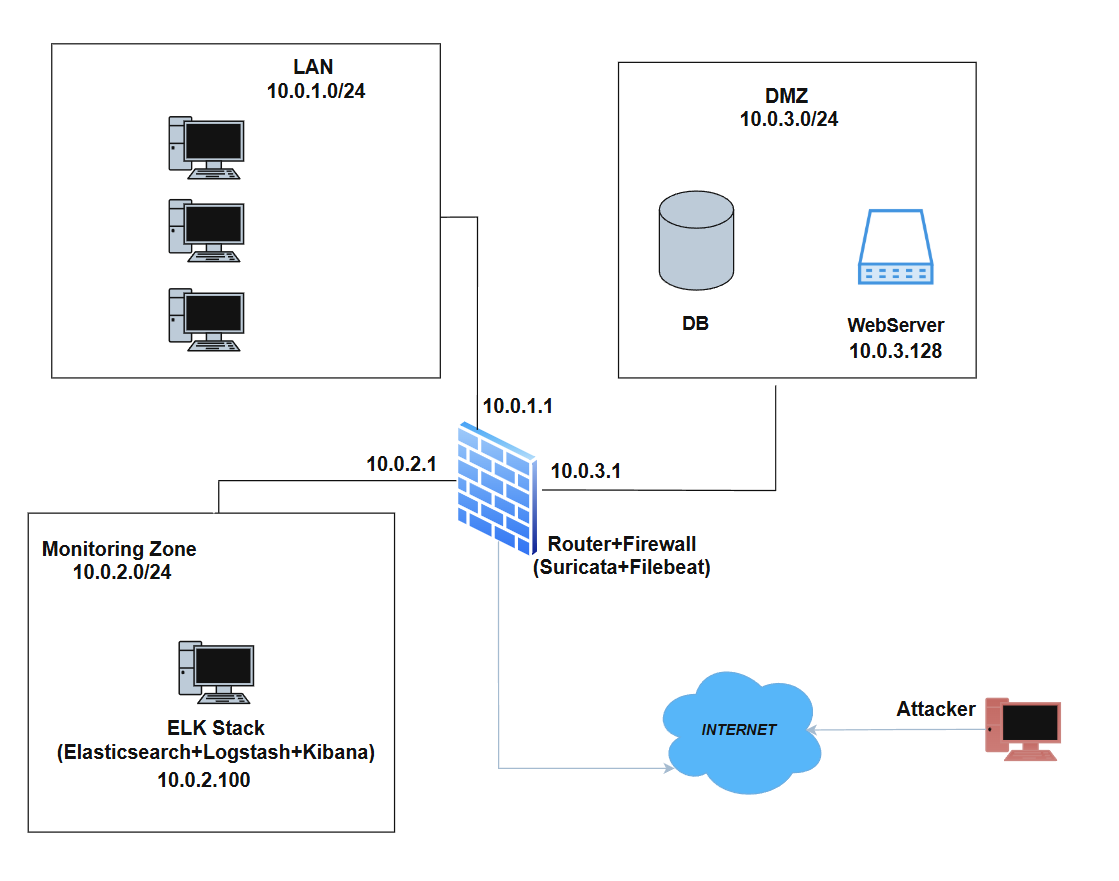
# **CHƯƠNG 3. TRIỂN KHAI HỆ THỐNG GIÁM SÁT VÀ PHÁT HIỆN XÂM NHẬP SỬ DỤNG SURICATA VÀ ELK STACK**

## 3.1. Mục tiêu thực nghiệm

Triển khai hệ thống giám sát và phát hiện xâm nhập mạng (NIDS/NIPS) sử dụng Suricata kết hợp với ELK Stack (Elasticsearch, Logstash, Kibana).Mô phỏng môi trường mạng có các phân vùng chức năng: LAN, DMZ (Webserver), Monitoring (ELK).Thực hiện ghi nhận log an ninh mạng theo thời gian thực, trực quan hóa qua Kibana.Phát hiện và phân tích các log tấn công thử nghiệm từ attacker (truy cập trái phép, scan, brute-force...) từ đó đưa ra các biện pháp xử lý thích hợp.

## 3.2. Xây dựng môi trường

### 3.2.1. Mô hình thực nghiệm

****

Hình 3.1 Sơ đồ mô hình hệ thống triển khai

**Mô hình gồm 3 vùng mạng độc lập:**

|  |  |
| --- | --- |
| **Khu vực** | **Vai trò chính** |
| **LAN (10.0.1.0/24)** | Máy trạm người dùng |
| **DMZ (10.0.3.0/24)** | Máy chủ Web (có thể bị tấn công từ bên ngoài) |
| **Monitoring (10.0.2.0/24)** | Máy ELK Stack (Logstash + Elasticsearch + Kibana) |
| **Router (4 NICs)** | Đóng vai trò định tuyến, NAT, Suricata IPS, Filebeat |

**Bảng 5**  Phân vùng mạng của mô hình.

**Và gồm 4 máy ảo chính:**

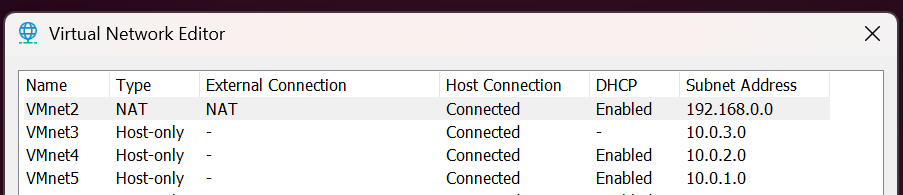
|  |  |  |
| --- | --- | --- |
| **Thiết bị** | **IP Address** | **Mô tả** |
| **Router/ Firewall/ Suricata** | **10.0.1.1 (LAN)** | Thiết bị trung tâm, cài Suricata (IPS mode) và Filebeat để thu log. |
| **10.0.2.1 (Monitoring)** | Giao tiếp với máy chủ ELK Stack trong vùng giám sát. |
| **10.0.3.1 (DMZ)** | Giao tiếp với các máy chủ dịch vụ trong vùng DMZ. |
| **192.168.xxx.xxx** | Giao tiếp với mạng internet bên ngoài. |
| **Máy Monitor/ ELK Stack** | **10.0.2.100** | Máy Ubuntu cài đặt bộ ELKStack giao tiếp với máy Suricata nhằm nhận log để phân tích, xử lý và biểu diễn trực quan. |
| **Web Server** | **10.0.3.128** | Máy Ubuntu giả lập máy chủ web và CSDL đặt trong vùng DMZ, mục tiêu tấn công giả lập. |
|  |
| **Attacker** | **192.168.xxx.xxx** | Máy Kali Linux mô phỏng kẻ tấn công từ Internet. |

**Bảng 6** Bảng cấu hình địa chỉ IP cho từng máy

### 3.2.2. Cài đặt và cấu hình

**a) Cấu hình mạng ảo bằng Virtual Network Editor.**

Để triển khai mô hình giám sát an ninh mạng sử dụng Suricata và ELK Stack, các mạng ảo đã được tạo và cấu hình thông qua công cụ Virtual Network Editor trong VMware Workstation như sau:



Hình 3.2 Cấu hình mạng ảo bằng virtual network editor

**Giải thích cấu hình:**

* VMnet2 (NAT): Dùng để mô phỏng mạng ngoài (Internet). Interface ens33 của router kết nối vào đây. DHCP bật để nhận IP tự động trong mạng.
* VMnet3 (Host-only): Dùng làm vùng DMZ, nơi đặt Web Server. DHCP bị tắt để đảm bảo địa chỉ tĩnh. Subnet: 10.0.3.0/24.
* VMnet4 (Host-only): Dùng làm vùng Monitoring, nơi router giao tiếp với máy ELK Stack. Subnet: 10.0.2.0/24.
* VMnet5 (Host-only): Dùng làm LAN nội bộ. DHCP được bật để máy người dùng nhận IP động trong mạng 10.0.1.0/24.

**b) Cấu hình iptables**

Nhằm đảm bảo chức năng định tuyến, NAT và giám sát lưu lượng mạng qua Suricata, hệ thống được cấu hình các luật iptables như sau:

***Đặt chính sách mặc định:*** Trước khi cấu hình mới, tất cả các luật và chuỗi cũ trong các bảng filter, nat, và mangle được xóa để tránh xung đột hoặc ảnh hưởng từ các cấu hình trước đó.Chính sách mặc định cho INPUT và OUTPUT là ACCEPT, nhưng FORWARD được đặt là DROP nhằm đảm bảo an toàn – chỉ cho phép các lưu lượng được xác định rõ ràng:

iptables -F

iptables -X

iptables -t nat -F

iptables -t nat -X

iptables -t mangle -F

iptables -t mangle -X  
iptables -P INPUT ACCEPT

iptables -P OUTPUT ACCEPT

iptables -P FORWARD DROP

***Kích hoạt chuyển tiếp IP (IP forwarding):***Để máy chủ có thể định tuyến các gói tin giữa các mạng khác nhau, chức năng chuyển tiếp IP được bật bằng cách thiết lập giá trị:

echo 1 > /proc/sys/net/ipv4/ip\_forward

* Điều này cho phép máy hoạt động như một router.

***Thiết lập NAT Masquerade:***Chức năng NAT được cấu hình trên bảng nat với luật masquerade nhằm cho phép các gói tin có nguồn từ các mạng nội bộ đi ra ngoài qua interface ens33 được thay đổi địa chỉ IP nguồn tương ứng với địa chỉ IP của interface này:

iptables -t nat -A POSTROUTING -s 10.0.1.0/24 -o ens33 -j MASQUERADE

iptables -t nat -A POSTROUTING -s 10.0.2.0/24 -o ens33 -j MASQUERADE

iptables -t nat -A POSTROUTING -s 10.0.3.0/24 -o ens33 -j MASQUERADE

***Cho phép các mạng LAN, Monitoring, DMZ ra Internet:*** Các interface nội bộ ens37, ens38, và ens39 tương ứng với mạng LAN, Monitoring, và DMZ được phép gửi dữ liệu ra ngoài qua ens33:

iptables -A FORWARD -i ens37 -o ens33 -j ACCEPT

iptables -A FORWARD -i ens38 -o ens33 -j ACCEPT

iptables -A FORWARD -i ens39 -o ens33 -j ACCEPT

***Cho phép gói trả lời từ Internet trở về:*** Lưu lượng từ Internet trả lời lại các kết nối nội bộ sẽ được chấp nhận nếu đã được thiết lập hoặc liên quan:

iptables -A FORWARD -i ens33 -m state --state ESTABLISHED,RELATED -j ACCEPT

***Chặn truy cập từ Internet vào mạng LAN:*** Ngăn không cho Internet truy cập trực tiếp vào mạng LAN:

iptables -A FORWARD -i ens33 -d 10.0.1.0/24 -j DROP

***Chặn DMZ truy cập LAN và Monitoring:*** Đảm bảo tính phân tách giữa DMZ với các vùng mạng còn lại để tăng cường bảo mật nội bộ:

iptables -A FORWARD -s 10.0.3.0/24 -d 10.0.1.0/24 -j DROP

iptables -A FORWARD -s 10.0.3.0/24 -d 10.0.2.0/24 -j DROP

***Cho phép Monitoring truy cập DMZ và nhận phản hồi:***

iptables -A FORWARD -i ens38 -o ens39 -s 10.0.2.0/24 -d 10.0.3.0/24 -j ACCEPT

iptables -A FORWARD -i ens39 -o ens38 -s 10.0.3.0/24 -d 10.0.2.0/24 -m state --state ESTABLISHED,RELATED -j ACCEPT

***Cho phép LAN truy cập DMZ và nhận phản hồi:***

iptables -A FORWARD -i ens37 -o ens39 -s 10.0.1.0/24 -d 10.0.3.0/24 -j ACCEPT

iptables -A FORWARD -i ens39 -o ens37 -s 10.0.3.0/24 -d 10.0.1.0/24 -m state --state ESTABLISHED,RELATED -j ACCEPT

***Chuyển tiếp toàn bộ lưu lượng từ Internet đến WebServer DMZ:*** Toàn bộ lưu lượng TCP từ ens33 của Router (Internet) được chuyển tiếp đến máy chủ Web trong DMZ (10.0.3.2). Luồng dữ liệu tương ứng cũng được cho phép đi qua:

iptables -t nat -A POSTROUTING -s 10.0.3.0/24 -o ens33 -j MASQUERADE  
iptables -t nat -A PREROUTING -i ens33 -p tcp -j DNAT --to-destination 10.0.3.2

iptables -A FORWARD -d 10.0.3.2 -p tcp -m state --state NEW,ESTABLISHED,RELATED -j ACCEPT

***Đưa lưu lượng vào hàng đợi NFQUEUE để Suricata xử lý:*** Tích hợp chức năng IPS bằng cách chuyển toàn bộ lưu lượng FORWARD vào hàng đợi NFQUEUE số 1 để Suricata xử lý:

iptables -I FORWARD -j NFQUEUE --queue-num 1

**c) Cấu hình suricata**

Để Suricata hoạt động đúng trong chế độ IPS sử dụng NFQUEUE, file cấu hình khởi động **/etc/default/suricata** cần được chỉnh sửa như sau:

RUN=yes

RUN\_AS\_USER=

CONF=/etc/suricata/suricata.yaml

LISTENMODE=nfqueue

NFQUEUE="-q 1"

CUSTOM\_NFQUEUE="-q 0 -q 1 -q 2 -q 3"

Trong mô hình triển khai Suricata theo chế độ IPS (Intrusion Prevention System), việc cấu hình chính xác phương thức bắt gói và hàng đợi xử lý là yếu tố then chốt để đảm bảo hệ thống hoạt động đúng chức năng.

***Thiết lập chế độ bắt gói là NFQUEUE****:* Suricata hỗ trợ nhiều chế độ bắt gói như pcap, af-packet, nfqueue, và custom\_nfqueue. Tuy nhiên, trong triển khai theo mô hình IPS, chỉ chế độ NFQUEUE mới cho phép Suricata tương tác chủ động với các gói tin để đưa ra quyết định chặn hoặc cho phép.Do đó, trong file cấu hình khởi động /etc/default/suricata, chế độ LISTENMODE được thiết lập như sau:

LISTENMODE=nfqueue

Việc chọn chế độ này đảm bảo rằng Suricata sẽ tiếp nhận các gói tin được định tuyến từ iptables thông qua cơ chế hàng đợi của Netfilter, thay vì bắt gói trực tiếp từ interface vật lý.

***Cấu hình hàng đợi xử lý gói tin:***Để Suricata có thể nhận đúng các gói tin được chuyển từ iptables, hàng đợi NFQUEUE phải được khai báo trùng khớp giữa hai thành phần. Trong trường hợp này, hàng đợi số **1** được sử dụng. Cấu hình được thiết lập như sau:

NFQUEUE="-q 1"