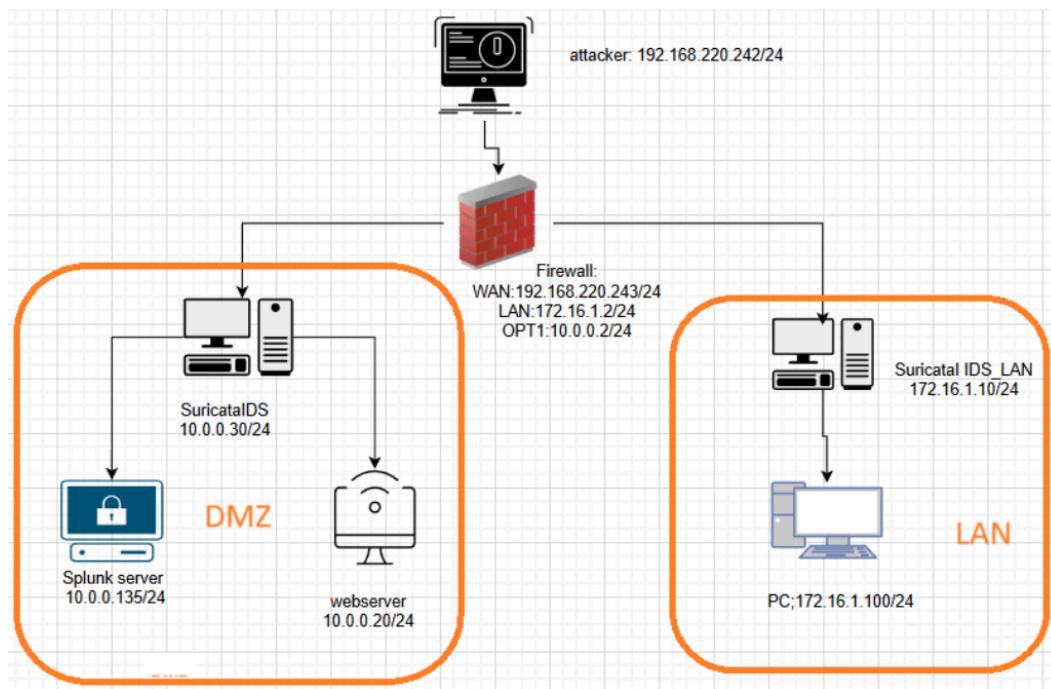


Suricata NIDS with Splunk SIEM

3.1. Mô hình triển khai thực nghiệm

3.1.1. Mô hình kiến trúc mạng



3.1.2. Chức năng các thành phần và cấu hình

Trong hệ thống mô phỏng được triển khai, các thành phần chính được phân chia theo vai trò và vị trí trong mô hình mạng, nhằm đảm bảo giám sát và phân tích hiệu quả các hành vi tấn công.

a, Attacker – Máy tấn công

Máy tấn công đóng vai trò sinh ra các hành vi xâm nhập. Thường sử dụng Kali Linux với các công cụ như nmap, hydra, hping3, metasploit để thực hiện quét cổng, brute-force, khai thác lỗ hổng và tấn công DoS. Máy này kết nối qua NAT trên PfSense để toàn bộ lưu lượng phải đi qua firewall và có thể giám sát bằng Suricata.

b, PfSense – Thiết bị định tuyến và tường lửa

PfSense vừa đảm nhiệm định tuyến vừa làm firewall kiểm soát lưu lượng giữa các subnet. Thiết bị có 2 interface: WAN kết nối mạng ngoài và LAN kết nối mạng nội bộ. Tại đây, quản trị viên có thể cấu hình luật firewall, NAT, port forwarding và ghi log lưu lượng. Quản lý thực hiện qua giao diện web GUI.

Rule : Nat/PortForward

	Interface	Protocol	Source Address	Source Ports	Dest. Address	Dest. Ports	NAT IP	NAT Ports	Description	Actions
<input type="checkbox"/>	WAN	TCP/UDP	*	*	WAN address	8080	10.0.0.20	80 (HTTP)	NAT to Web server	
<input type="checkbox"/>	WAN	TCP	*	*	WAN address	80 (HTTP)	10.0.0.20	80 (HTTP)		
<input type="checkbox"/>	WAN	TCP	*	*	WAN address	3389 (MS RDP)	10.0.0.20	3389 (MS RDP)	RDP	

Rule WAN

<input type="checkbox"/>	0/0 B	IPv4 TCP	*	*	10.0.0.20	3389 (MS RDP)	*	none	NAT RDP	
<input type="checkbox"/>	0/0 B	IPv4 TCP/UDP	*	*	10.0.0.20	80 (HTTP)	*	none	NAT NAT to Web server	

Các địa chỉ IP cho từng vùng mạng của Pfsense

```

FreeBSD/amd64 (pfSense.home.arpa) (ttyv0)

VMware Virtual Machine - Netgate Device ID: 0db398e5aece5b018b77

*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0          -> v4/DHCP4: 192.168.220.243/24
LAN (lan)      -> em1          -> v4: 172.16.1.2/24
OPT1 (opt1)    -> em2          -> v4: 10.0.0.2/24

```

c, SuricataDMZ – IDS vùng biên mạng (10.0.0.30/24)

Suricata được triển khai ở vùng biên để giám sát lưu lượng từ bên ngoài trước khi vào hệ thống. Hoạt động ở chế độ IDS, Suricata phân tích gói tin, ghi log cảnh báo (eve.log, fast.log) và gửi về Splunk phục vụ phân tích tập trung.

Cài đặt cấu hình suricata

B1: Để bắt đầu cài đặt Suricata, chúng ta cần thêm repository của Open Information Security Foundation (OISF) vào hệ thống của mình.

```
sudo add-apt-repository ppa:oisf/suricata-stable
```

B2: Sau khi chúng ta đã thực hiện repository vào hệ thống của chúng ta và cập nhật danh sách các packages thì tiến hành cài đặt Suricata với lệnh dưới

```
sudo apt install suricata -y
```

B3; Kiểm tra trạng thái của suricata.service

```
systemctl status suricata.service
cat /etc/suricata/suricata.yaml | grep community-id
```

B4:Cấu hình nơi thay đổi rule thành /etc/suricata/rules/local.rules

```
GNU nano 4.8          /etc/suricata/suricata.yaml
# See Napatech NTPL documentation other hashmodes and details on their use.
#
# This parameter has no effect if auto-config is disabled.
#
hashmode: hash5tuplesorted

##
## Configure Suricata to load Suricata-Update managed rules.
##

default-rule-path: /etc/suricata/rules

rule-files:
- local.rules
```

B5: Sau đó cập nhật rule

```
sudo suricata-update
```

Khi bị kích hoạt thì log của suricata nằm ở đường dẫn /var/log/suricata/stats.log hoặc /var/log/suricata/eve.json. Hai log này rất quan trọng và chúng ta thực hiện đẩy log này lên trên Splunk để chuẩn hóa và dễ theo dõi và giám sát hơn.

Đoạn rule áp dụng cho thực nghiệm :

```

#Nmap TCP SYN Scan Detection
alert tcp any any → $HOME_NET any (msg:"Nmap TCP SYN scan detected"; flags:S; flow: stateless; threshold: type threshold, track by_src, count 1 0, seconds 60; sid: 1000100; rev:3;)

# RDP Brute Force Detection (Hydra)
alert tcp any any → $HOME_NET 3389 (msg:"RDP brute force attempt detected (Hydra)"; flags:S; flow:to_server; threshold:type threshold, track by_src, count 5, seconds60; sid:1000150; rev:1;)

# hping3 SYN Flood Detection (DoS toàn bộ port)
alert tcp any any → $HOME_NET any (msg:"Potential TCP SYN flood DoS attack (hping3)"; flags:S; flow:to_server; threshold:type threshold, track by_src, count 200, seconds 10; sid:1000160; rev:1;)

# Web DoS SYN Flood Detection (port 80,443)
alert tcp any any → $HOME_NET [80,443] (msg:"WEB DoS SYN flood detected"; flags:S; flow:to_server; threshold:type threshold, track by_src, count 100, seconds 10; sid:1000200; rev:2;)

# Web DoS RST Flood Detection (port 80,443)
alert tcp any any → $HOME_NET [80,443] (msg:"WEB DoS TCP RST flood detected"; flags:R; flow:to_server; threshold:type threshold, track by_src, count 50, seconds 10; sid:1000201; rev:1;)

```

d. Server/Splunk – Hệ thống thu thập và phân tích log

Splunk là nền tảng SIEM thu thập, lưu trữ, tìm kiếm và trực quan hóa log từ các thành phần khác. Splunk hỗ trợ cảnh báo thời gian thực, dashboard thống kê và tích hợp ứng dụng bảo mật như Suricata App for Splunk. Log Suricata được gửi về qua Universal Forwarder hoặc Syslog.

Cấu hình Splunk Server

B1: Cài đặt gói cài đặt Splunk server từ trang chủ

B2: Giải nén về /opt

```
sudo tar -xzvf splunk.tgz -C /opt
```

B3: Khởi động lần đầu, chấp nhận giấy phép và khởi động splunk server

```
sudo tar -xzvf splunk.tgz -C /opt/opt/splunk/bin/splunk start -- accept-license
```

B4: Thiết lập Splunk khởi động cùng hệ thống

```
/opt/splunk/bin/splunk enable boot-start
```

f. PC – Thiết bị đầu cuối người dùng

Máy PC mô phỏng thiết bị người dùng cuối, là mục tiêu của các cuộc tấn công. Đồng thời, máy này còn dùng để quản trị giao diện web của PfSense và quan sát tác động của tấn công, thu thập log phục vụ điều tra số.

3.2. Các kịch tấn công vào hệ thống

3.2.1. Kịch bản tấn công

Trong bối cảnh an ninh mạng ngày càng phức tạp, việc xây dựng các kịch bản tấn công mô phỏng là phương pháp cần thiết để đánh giá hiệu quả hệ thống giám sát và năng lực phản ứng của các thành phần phòng thủ. Kịch bản tấn công quét cổng bằng Nmap được lựa chọn vì đây là kỹ thuật phổ biến trong giai đoạn trinh sát sơ cấp (initial reconnaissance), tiền đề cho các hoạt động khai thác lỗ hổng về sau.

3.2.1.1. Tấn công quét cổng bằng Nmap

Quá trình thực hiện

B1: Sử dụng nmap với câu lệnh :

```
nmap -p 80,3389 192.168.220.243
```

B2: Quan sát log Suricata tại các node giám sát , xem cảnh báo tại thư mục fast.log

Sau khi tấn công hiện ngay cảnh báo alert nmap ngay lập tức

```
[3] {TCP} 10.0.0.135:32870 -> 10.0.0.1:53  
07/04/2025-21:55:29.470698 [**] [1:1000100:3] Nmap TCP SYN scan detected [**] [Classification: (null)] [Priority:  
3] {TCP} 10.0.0.135:40138 -> 10.0.0.1:53  
07/04/2025-21:55:52.567734 [**] [1:1000100:3] Nmap TCP SYN scan detected [**] [Classification: (null)] [Priority:  
3] {TCP} 10.0.0.135:40878 -> 10.0.0.1:53  
07/04/2025-21:56:08.817672 [**] [1:1000100:3] Nmap TCP SYN scan detected [**] [Classification: (null)] [Priority:  
3] {TCP} 10.0.0.135:55808 -> 10.0.0.1:53  
07/04/2025-21:56:40.880165 [**] [1:1000100:3] Nmap TCP SYN scan detected [**] [Classification: (null)] [Priority:  
3] {TCP} 10.0.0.135:50700 -> 10.0.0.1:53  
07/04/2025-21:56:54.117475 [**] [1:1000100:3] Nmap TCP SYN scan detected [**] [Classification: (null)] [Priority:  
3] {TCP} 10.0.0.135:51482 -> 10.0.0.1:53  
07/04/2025-21:57:21.049965 [**] [1:1000100:3] Nmap TCP SYN scan detected [**] [Classification: (null)] [Priority:  
3] {TCP} 10.0.0.135:32976 -> 10.0.0.1:53  
07/04/2025-21:57:47.793444 [**] [1:1000100:3] Nmap TCP SYN scan detected [**] [Classification: (null)] [Priority:  
3] {TCP} 10.0.0.135:46984 -> 10.0.0.1:53  
07/04/2025-21:58:06.347384 [**] [1:1000100:3] Nmap TCP SYN scan detected [**] [Classification: (null)] [Priority:  
3] {TCP} 10.0.0.135:59646 -> 10.0.0.1:53  
07/04/2025-21:58:27.971846 [**] [1:1000100:3] Nmap TCP SYN scan detected [**] [Classification: (null)] [Priority:  
3] {TCP} 10.0.0.135:52312 -> 10.0.0.1:53  
07/04/2025-21:58:54.778986 [**] [1:1000100:3] Nmap TCP SYN scan detected [**] [Classification: (null)] [Priority:  
3] {TCP} 10.0.0.135:37502 -> 10.0.0.1:53
```

B3 Kiểm tra log trên Splunk

Index=dnz EventCode=4625				Last 24 hours ▾
14 events (7/3/25 10:00:00.000 PM to 7/4/25 10:25:22.000 PM)		No Event Sampling ▾	Job ▾	Smart Mode ▾
Events (14) Patterns Statistics Visualization				
Timeline format ▾	Zoom Out	+ Zoom to Selection	X Deselected	1 hour per column
Format ▾	Show: 20 Per Page ▾	View: List ▾		
Hide Fields	All Fields	Time	Event	
SELECTED FIELDS		7/4/25 9:59:44.000 PM	07/04/2025 07:59:44 AM LogName=Security EventCode=4625 EventType=0 ComputerName=WIN-TSHE3AQ75NB Show all 61 lines	
# host 1			host = WIN-TSHE3AQ75NB source = WinEventLog:Security sourcetype = WinEventLog:Security	
# source 1				
# sourcetype 1				
INTERESTING FIELDS				
# Account_Domain 1		7/4/25 9:59:43.000 PM	07/04/2025 07:59:43 AM LogName=Security EventCode=4625 EventType=0 ComputerName=WIN-TSHE3AQ75NB Show all 61 lines	
# Account_Name 2			host = WIN-TSHE3AQ75NB source = WinEventLog:Security sourcetype = WinEventLog:Security	
# Authentication_Package 1				
# Caller_Process_ID 1				
# Caller_Process_Name 1				
# ComputerName 1				
# EventCode 1				
# EventType 1				
# Failure_Reason 1				
# index 1				
# Key_Length 1		7/4/25 9:59:43.000 PM	07/04/2025 07:59:43 AM LogName=Security EventCode=4625 EventType=0 ComputerName=WIN-TSHE3AQ75NB Show all 61 lines	
# Keywords 1				
# Inecount 1				
# LogName 1				
# Logon_ID 1				
# Logon_Process 1				
# Logon_Type 1				
# Message 1		7/4/25 9:59:35.000 PM	07/04/2025 07:59:35 AM LogName=Security EventCode=4625 EventType=0 ComputerName=WIN-TSHE3AQ75NB Show all 61 lines	
# OpCode 1				
# Package_Name__NTLM_only_ 1				
# punct 1				
# RecordNumber 14				
# Security_Log 1				
# Source_Network_Address 1				

Phân tích : Ngay sau khi kẻ tấn công tiến hành quét mạng, hệ thống giám sát Suricata đã ghi nhận và cảnh báo tức thời. Cụ thể, địa chỉ IP 192.168.220.243 đã thực hiện hành vi quét cổng bằng công cụ Nmap, sử dụng kỹ thuật TCP SYN Scan nhằm dò tìm các cổng dịch vụ đang mở trên hệ thống đích 10.0.0.20.

Trong một khoảng thời gian ngắn, Suricata đã phát hiện hàng trăm gói tin TCP SYN được gửi đồng loạt đến nhiều cổng khác nhau trên máy đích. Đây là dấu hiệu điển hình của hoạt động trinh sát mạng (network reconnaissance), thường được sử dụng để thu thập thông tin trước khi triển khai các bước tấn công tiếp theo. Việc phát hiện kịp thời giúp xác định rõ nguồn gốc lưu lượng, đồng thời cho thấy hệ thống đang bị dò quét có chủ đích, tiềm ẩn nguy cơ xâm nhập và tấn công khai thác lỗ hổng.

3.2.1.2. Tấn công Brute Force qua giao thức RDP

Môi trường :Sau khi thực hiện quét cổng thì kẻ tấn công phát hiện Máy mục tiêu mở port dịch vụ 3389 RDP , cùng với tài khoản Administrator ,mật khẩu cấu hình yếu . Kẻ tấn công chuẩn bị một file chứa mật khẩu chứa các password phổ biến để thực hiện vét cạn qua dịch vụ này

Quy trình thực hiện :

B1: Trên máy tấn công sử dụng câu lệnh hydra với danh sách và tên người dùng và mật khẩu :

```
hydra -t 4 -V -f -l Administrator -P pass.txt 192.168.220.243 rdp
```

```
(kali㉿kali)-[~]
$ hydra -l Administrator -P pass.txt 192.168.23.134 rdp
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 2025-06-25 14:51:01
[WARNING] rdp servers often don't like many connections, use -t 1 or -t 4 to reduce the number of parallel connections and -W 1 or -W 3 to wait between connection to allow the server to recover
[INFO] Reduced number of tasks to 4 (rdp does not like many parallel connections)
[WARNING] the rdp module is experimental. Please test, report - and if possible, fix.
[DATA] max 4 tasks per 1 server, overall 4 tasks, 19 login tries (l:1/p:19), ~5 tries per task
[DATA] attacking rdp://192.168.23.134:3389/
[ERROR] freerdp: The connection failed to establish.
[3389][rdp] host: 192.168.23.134 login: Administrator password: Hvktmm23@
[ERROR] freerdp: The connection failed to establish.
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-06-25 14:51:03
```

B2: Giám sát lưu lượng trên suricata

```
07/04/2025-21:59:43.163839 [**] [1:1000100:3] Nmap TCP SYN scan detected [**] [Classification: (null)] [Priority: 3] {TCP} 192.168.220.242:33132 -> 10.0.0.20:3389
07/04/2025-21:59:44.142499 [**] [1:1000150:1] RDP brute force attempt detected (Hydra) [**] [Classification: (null)] [Priority: 3] {TCP} 192.168.220.242:33134 -> 10.0.0.20:3389
07/04/2025-21:59:44.556235 [**] [1:1000150:1] RDP brute force attempt detected (Hydra) [**] [Classification: (null)] [Priority: 3] {TCP} 192.168.220.242:33194 -> 10.0.0.20:3389
07/04/2025-22:05:36.743431 [**] [1:1000100:3] Nmap TCP SYN scan detected [**] [Classification: (null)] [Priority: 3] {TCP} 192.168.220.242:2257 -> 10.0.0.20:80
```

B3: kiểm tra log Event viewer trên máy chủ windows

Keywords	Date and Time	Source	Event ID	Task Category
🔍 Audit Success	7/4/2025 7:59:45 AM	Microsoft Win...	4634	Logoff
🔍 Audit Success	7/4/2025 7:59:44 AM	Microsoft Win...	4624	Logon
🔍 Audit Success	7/4/2025 7:59:44 AM	Microsoft Win...	4672	Special Logon
🔍 Audit Success	7/4/2025 7:59:44 AM	Microsoft Win...	4776	Credential Valid...
🔒 Audit Failure	7/4/2025 7:59:44 AM	Microsoft Win...	4625	Logon
🔒 Audit Failure	7/4/2025 7:59:43 AM	Microsoft Win...	4625	Logon
🔒 Audit Failure	7/4/2025 7:59:43 AM	Microsoft Win...	4625	Logon
🔒 Audit Failure	7/4/2025 7:59:35 AM	Microsoft Win...	4625	Logon
🔒 Audit Failure	7/4/2025 7:59:34 AM	Microsoft Win...	4625	Logon
🔍 Audit Success	7/4/2025 7:59:34 AM	Microsoft Win...	4634	Logoff
🔒 Audit Failure	7/4/2025 7:59:34 AM	Microsoft Win...	4625	Logon
🔍 Audit Success	7/4/2025 7:59:33 AM	Microsoft Win...	4624	Logon
🔍 Audit Success	7/4/2025 7:59:33 AM	Microsoft Win...	4672	Special Logon
🔍 Audit Success	7/4/2025 7:59:33 AM	Microsoft Win...	4776	Credential Valid...

B4:kiểm tra trên Splunk

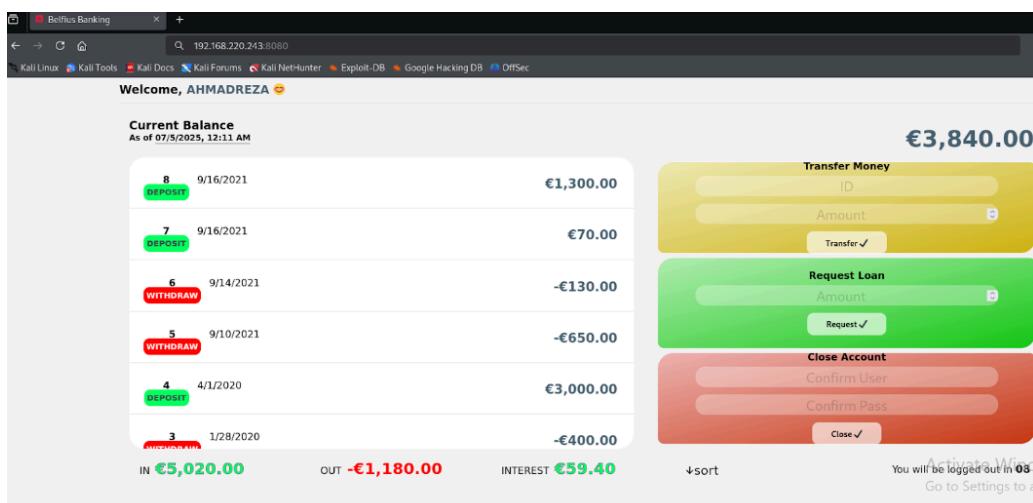
Phân tích : Ban đầu, kẻ tấn công tiến hành hoạt động quét cổng (port scanning) nhằm kiểm tra xem hệ thống có dịch vụ nào công khai (public) ra bên ngoài mạng Internet. Log Suricata thu thập từ file eve.json và hiển thị trên Splunk ghi nhận các cảnh báo liên quan đến hoạt động TCP SYN Scan, cho thấy kẻ tấn công rà quét trên nhiều cổng dịch vụ. Quá trình phân tích log chỉ ra địa chỉ IP nguồn thực hiện quét tập trung vào các port phổ biến như 80 (HTTP), và đặc biệt là 3389 (RDP).

Sau khi phát hiện cổng RDP (3389) đang mở, kẻ tấn công chuyển sang giai đoạn tấn công vét cạn tài khoản (brute-force attack). Trong khoảng thời gian ngắn, Suricata liên tiếp cảnh báo lưu lượng RDP kết nối thất bại, trùng với thời điểm log trên máy chủ Windows xuất hiện số lượng lớn sự kiện Event ID 4625

Nhóm SOC đã đổi chiều các nguồn dữ liệu và xác định chuỗi hành vi tấn công. Log Suricata ghi nhận kết nối liên tục đến port 3389 từ cùng một địa chỉ IP với cảnh báo Trong Windows Event Viewer, nhiều sự kiện Event ID 4625 cho thấy nhiều lần đăng nhập thất bại chỉ cách nhau vài giây. Sau đó, xuất hiện Event ID 4672 cấp đặc quyền quản trị viên và Event ID 4624 xác nhận đăng nhập thành công. Đổi chiều thời gian log Suricata và Event Viewer cho thấy các bước quét cổng, brute-force và chiếm quyền diễn ra liên tiếp trong cùng phiên tấn công.

3.2.1.2.Tấn công DOS

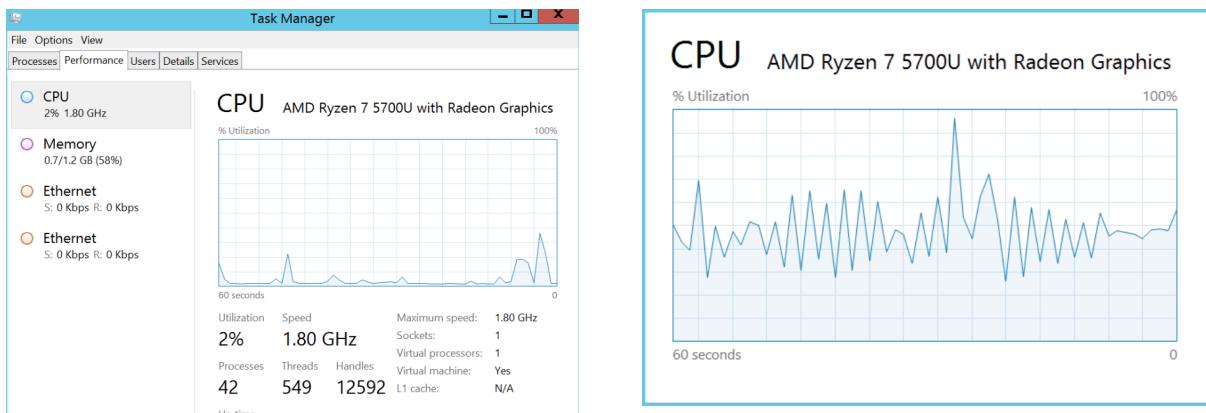
Môi trường : Chuẩn bị một trang web trong phân vùng mạng DMZ , trang web này là mục tiêu của kẻ tấn công



B1 : Kẻ tấn công từ một máy ngoài LAN đã sử dụng công cụ hping3 để phát động đợt SYN Flood, liên tục gửi một lượng lớn gói TCP SYN nhằm làm cạn kiệt tài nguyên kết nối của hệ thống đích.

```
hping3 -S -p 8080 -flood 192.168.220.243
```

B2 Trên máy DMZ task manager bị cao bất thường



⇒ Website bị delay sau khi bị tấn công

B3: Giám sát lưu lượng trên suricata

```

07/04/2025-22:06:19.438688 [**] [1:1000200:2] WEB DoS SYN flood detected [**] [Classification: (null)] [Priority: 3] {TCP} 192
.168.220.242:13908 -> 10.0.0.20:80
07/04/2025-22:06:19.447812 [**] [1:1000201:1] WEB DoS TCP RST flood detected [**] [Classification: (null)] [Priority: 3] {TCP}
192.168.220.242:11771 -> 10.0.0.20:80
07/04/2025-22:06:19.478468 [**] [1:1000200:2] WEB DoS SYN flood detected [**] [Classification: (null)] [Priority: 3] {TCP} 192
.168.220.242:14062 -> 10.0.0.20:80
07/04/2025-22:06:19.479409 [**] [1:1000201:1] WEB DoS TCP RST flood detected [**] [Classification: (null)] [Priority: 3] {TCP}
192.168.220.242:19162 -> 10.0.0.20:80
07/04/2025-22:06:19.541546 [**] [1:1000200:2] WEB DoS SYN flood detected [**] [Classification: (null)] [Priority: 3] {TCP} 192
.168.220.242:14098 -> 10.0.0.20:80
07/04/2025-22:06:19.500628 [**] [1:1000201:1] WEB DoS TCP RST flood detected [**] [Classification: (null)] [Priority: 3] {TCP}
192.168.220.242:11922 -> 10.0.0.20:80
07/04/2025-22:06:19.531470 [**] [1:1000201:1] WEB DoS TCP RST flood detected [**] [Classification: (null)] [Priority: 3] {TCP}
192.168.220.242:12017 -> 10.0.0.20:80
07/04/2025-22:06:19.544766 [**] [1:1000200:2] WEB DoS SYN flood detected [**] [Classification: (null)] [Priority: 3] {TCP} 192
.168.220.242:16400 -> 10.0.0.20:80
07/04/2025-22:06:21.694738 [**] [1:1000201:1] WEB DoS TCP RST flood detected [**] [Classification: (null)] [Priority: 3] {TCP}
192.168.220.242:12232 -> 10.0.0.20:80
07/04/2025-22:06:21.911697 [**] [1:1000201:1] WEB DoS TCP RST flood detected [**] [Classification: (null)] [Priority: 3] {TCP}
192.168.220.242:12315 -> 10.0.0.20:80
07/04/2025-22:06:21.912740 [**] [1:1000200:2] WEB DoS SYN flood detected [**] [Classification: (null)] [Priority: 3] {TCP} 192
.168.220.242:16626 -> 10.0.0.20:80
07/04/2025-22:06:21.936591 [**] [1:1000201:1] WEB DoS TCP RST flood detected [**] [Classification: (null)] [Priority: 3] {TCP}
192.168.220.242:12457 -> 10.0.0.20:80
07/04/2025-22:06:21.965701 [**] [1:1000201:1] WEB DoS TCP RST flood detected [**] [Classification: (null)] [Priority: 3] {TCP}
192.168.220.242:19739 -> 10.0.0.20:80
07/04/2025-22:06:21.981358 [**] [1:1000200:2] WEB DoS SYN flood detected [**] [Classification: (null)] [Priority: 3] {TCP} 192
.168.220.242:16900 -> 10.0.0.20:80
07/04/2025-22:06:21.981508 [**] [1:1000201:1] WEB DoS TCP RST flood detected [**] [Classification: (null)] [Priority: 3] {TCP}
192.168.220.242:20969 -> 10.0.0.20:80
07/04/2025-22:06:21.995334 [**] [1:1000201:1] WEB DoS TCP RST flood detected [**] [Classification: (null)] [Priority: 3] {TCP}
192.168.220.242:12728 -> 10.0.0.20:80
07/04/2025-22:06:22.014269 [**] [1:1000201:1] WEB DoS TCP RST flood detected [**] [Classification: (null)] [Priority: 3] {TCP}
192.168.220.242:12853 -> 10.0.0.20:80
07/04/2025-22:06:22.048578 [**] [1:1000200:2] WEB DoS SYN flood detected [**] [Classification: (null)] [Priority: 3] {TCP} 192
.168.220.242:17185 -> 10.0.0.20:80
07/04/2025-22:06:22.049266 [**] [1:1000201:1] WEB DoS TCP RST flood detected [**] [Classification: (null)] [Priority: 3] {TCP}
192.168.220.242:13070 -> 10.0.0.20:80
07/04/2025-22:06:22.057239 [**] [1:1000201:1] WEB DoS TCP RST flood detected [**] [Classification: (null)] [Priority: 3] {TCP}
192.168.220.242:13121 -> 10.0.0.20:80
07/04/2025-22:06:22.085545 [**] [1:1000201:1] WEB DoS TCP RST flood detected [**] [Classification: (null)] [Priority: 3] {TCP}
192.168.220.242:13272 -> 10.0.0.20:80
07/04/2025-22:06:22.119332 [**] [1:1000200:2] WEB DoS SYN flood detected [**] [Classification: (null)] [Priority: 3] {TCP} 192
.168.220.242:17411 -> 10.0.0.20:80
07/04/2025-22:06:22.122675 [**] [1:1000201:1] WEB DoS TCP RST flood detected [**] [Classification: (null)] [Priority: 3] {TCP}
192.168.220.242:13498 -> 10.0.0.20:80
07/04/2025-22:06:22.136465 [**] [1:1000201:1] WEB DoS TCP RST flood detected [**] [Classification: (null)] [Priority: 3] {TCP}
192.168.220.242:13572 -> 10.0.0.20:80
07/04/2025-22:06:22.186363 [**] [1:1000201:1] WEB DoS TCP RST flood detected [**] [Classification: (null)] [Priority: 3] {TCP}
192.168.220.242:13772 -> 10.0.0.20:80
07/04/2025-22:06:22.201649 [**] [1:1000201:1] WEB DoS TCP RST flood detected [**] [Classification: (null)] [Priority: 3] {TCP}
192.168.220.242:13842 -> 10.0.0.20:80
07/04/2025-22:06:22.215582 [**] [1:1000200:2] WEB DoS SYN flood detected [**] [Classification: (null)] [Priority: 3] {TCP} 192
.168.220.242:17631 -> 10.0.0.20:80
07/04/2025-22:06:22.223893 [**] [1:1000201:1] WEB DoS TCP RST flood detected [**] [Classification: (null)] [Priority: 3] {TCP}
192.168.220.242:13928 -> 10.0.0.20:80
07/04/2025-22:06:22.240480 [**] [1:1000201:1] WEB DoS TCP RST flood detected [**] [Classification: (null)] [Priority: 3] {TCP}
192.168.220.242:13995 -> 10.0.0.20:80
07/04/2025-22:06:22.273243 [**] [1:1000201:1] WEB DoS TCP RST flood detected [**] [Classification: (null)] [Priority: 3] {TCP}
192.168.220.242:16349 -> 10.0.0.20:80

```

Log cảnh báo ở fast.log

B4:kiểm tra trên Splunk

```
    }
    flow_id: 1618172953359155
    in_iface: ens33
    proto: UDP
    src_ip: fe80:000:0000:0000:bd3e:479f:8c21:5630
    src_port: 58882
    timestamp: 2025-07-04T22:13:08.800336+0700
}
Show as raw text
host = ubuntu24 source = /var/log/suricata/eve.json sourcetype = json-2
> 7/4/25
10:13:08.557 PM { [-]
    alert: { [-]
        }
        dest_ip: 10.0.0.1
        dest_port: 53
        direction: to.server
        event_type: alert
        flow: { [-]
            }
            flow_id: 2227761560433109
            in_iface: ens33
            pkt_src: wire/pcap
            proto: TCP
            src_ip: 10.0.0.135
            src_port: 40704
            timestamp: 2025-07-04T22:13:08.557866+0700
        }
        Show as raw text
        host = ubuntu24 source = /var/log/suricata/eve.json sourcetype = json-2
    > 7/4/25
10:13:08.380 PM { [-]
    event_type: stats
    stats: { [-]
        }
        timestamp: 2025-07-04T22:13:08.380912+0700
    }
    Show as raw text
    host = ubuntu24 source = /var/log/suricata/eve.json sourcetype = json-2
> 7/4/25
10:13:04.707 PM { [-]
    dest_ip: 10.0.0.1
    dest_port: 53
    event_type: flow
    flow: { [-]
        }
        flow_id: 920664995499808
        in_iface: ens33
        proto: TCP

```

Log đã được thu thập và xuất hiện trên splunk server

Phân tích log:

Trên máy chủ DMZ, website hoạt động chậm và mất phản hồi định kỳ. Kiểm tra Task Manager cho thấy CPU và memory tăng cao bất thường dù lưu lượng người dùng không nhiều. Log Suricata đẩy lên Splunk ghi nhận hàng loạt cảnh báo "ET DOS TCP SYN Flood", với hàng chục nghìn gói TCP SYN gửi đến cổng 80 từ cùng một địa chỉ IP. Nhiều kết nối trên server rơi vào trạng thái SYN_RECV, là đặc trưng của tấn công SYN Flood.

Kết quả điều tra của đội SOC :

Đội SOC đã đối chiếu log Suricata trên Splunk và kiểm tra bảng kết nối thực tế. Kết quả xác định hệ thống bị tấn công từ chối dịch vụ kiểu SYN Flood, xuất phát từ địa chỉ IP bên ngoài mạng LAN, nhằm làm cạn kiệt tài nguyên kết nối của máy chủ web. Ngay sau khi xác minh, đội SOC đã khuyến cáo chặn IP tấn công trên firewall, kích hoạt cơ chế SYN Cookies và giới hạn số kết nối đồng thời để giảm thiểu ảnh hưởng.