

SIEM RULE DETECTION – MITRE ATT&CK

0. Tóm tắt tiến độ

0.1. Logs

Log src:

- windows security logs src => **xong**
- Linux logs src => **xong**
- Services cơ bản: liên quan web, IIS, nginx -> khi tấn công vào -> xuất ra gì? => **xong được dịch vụ Nginx bên Ubuntu**

Log src security agent:

- Suricata => **xong**
- Dùng thêm 1 pfSense tương đương => Gia lập tan công LAN/WAN => day log về sime => **chưa xong**

0.2. Detection Rule => **xong**

- Khả năng capabilti
- Gia lập các kiểu tan công
- hiện kết quả

0.3. Giả lập một số cuộc tấn công (ví dụ Ransomware mã hoá dữ liệu). Xem Suricata có phát hiện được không?

=> *chưa thực hiện được Ransomware, mới thực hiện được DDoS*

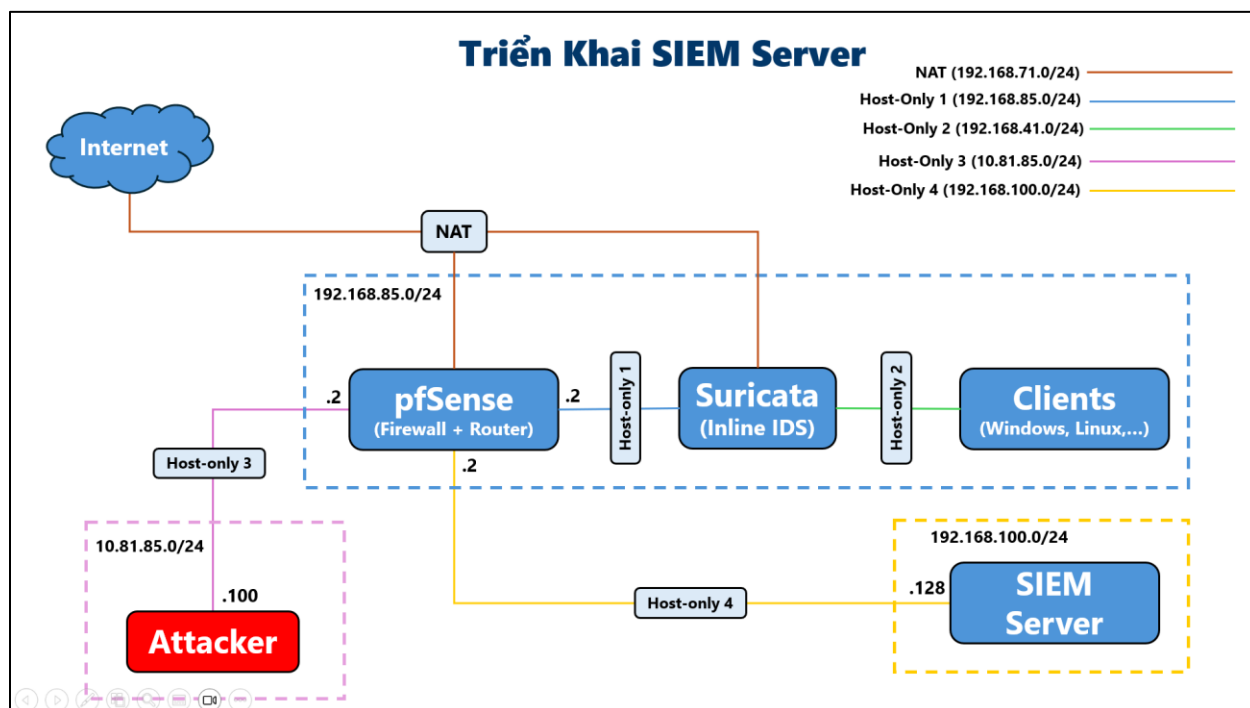
0.4. Giả lập tấn công C&C Server. Xem Suricata có phát hiện được không?

=> *Mới tìm hiểu được cơ bản, chưa đi sâu*

0.5. Khả năng Auto Respond của Elastic Search như nào?

=> *chưa làm*

1. Mô hình triển khai



Mô hình triển khai

1.1. Router

- Sử dụng 1 máy pfSense làm bộ định tuyến (Router) kiêm tường lửa (Firewall) trung tâm cho toàn bộ hạ tầng.
- Phân tách và quản lý lưu lượng giữa các mạng (NAT, Host-Only, DMZ...) thông qua các rule định tuyến và NAT.
- Áp dụng chính sách truy cập (firewall rules) để cho phép hoặc chặn dịch vụ theo lớp mạng, IP, port.
- Thu thập và chuyển tiếp tất cả log hệ thống (firewall, DHCP, OpenVPN, DNS...) đến Logstash/SIEM để giám sát và phân tích an ninh.

1.2. IDS/IPS

- Triển khai 1 máy Ubuntu Server cài đặt Suricata hoạt động ở chế độ Inline IDS/IPS.
- Suricata kiểm tra lưu lượng mạng theo thời gian thực, phát hiện và ngăn chặn các hành vi xâm nhập hoặc bất thường dựa trên rule signatures.
- Gửi các sự kiện cảnh báo (alert logs) về hệ thống SIEM thông qua Filebeat để phân tích và điều tra chi tiết.

- Định kỳ cập nhật rule từ cộng đồng (ET Open Rules) để đảm bảo khả năng phát hiện các mối đe dọa mới.

1.3. Clients

- 1 máy Ubuntu Desktop bình thường, không cài thêm IDS gì thêm, chỉ để Filebeat lấy log hệ thống

- 1 máy Metasploitable2 để khai thác lỗ hổng

- 1 máy Windows 10, không cài thêm IDS gì thêm, chỉ để Filebeat lấy log hệ thống

1.4. Admin





- 1 máy làm ELK Server dùng để lọc, phân tích, lưu trữ log

- 1 máy bên ngoài đăng nhập vào giao diện web của Kibana để quản lý

2. Triển khai pfSense

Mục tiêu của việc triển khai pfSense trong mô hình trên là thiết lập một hệ thống firewall mạnh mẽ để bảo vệ các máy chủ và dịch vụ trong môi trường mạng. pfSense sẽ đóng vai trò là bộ lọc chính, kiểm tra và phân tích lưu lượng mạng để ngăn chặn các cuộc tấn công mạng trước khi chúng tiếp cận các tài nguyên mạng quan trọng.

2.1. Cấu hình

Interfaces			
 WAN	↑	1000baseT <full-duplex>	192.168.71.250
 LAN	↑	1000baseT <full-duplex>	10.81.85.2
 OPT1	↑	1000baseT <full-duplex>	192.168.85.2
 OPT2	↑	1000baseT <full-duplex>	192.168.100.2

- **WAN Interface:** Kết nối với internet hoặc mạng bên ngoài -> 192.168.71.250/24

- **LAN Interface:** gồm 3 interfaces

+ LAN – em1: 10.81.85.2/24 => là gateway cho lớp mạng 10.81.85.0/24

+ OPT1 - em2: 192.168.85.2/24 => là gateway cho lớp mạng 192.168.85.0/24

+ OPT2 – em3: 192.168.100.2/24 => là gateway cho lớp mạng 192.168.100.0/24

- Gửi logs về Filebeat: <đang hoàn thiện, còn lỗi>

2.2. Một số rules cơ bản

Firewall / Rules / WAN

Floating WAN LAN OPT1 OPT2

Rules (Drag to Change Order)

<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	0/4 KiB	*	RFC 1918 networks	*	*	*	*	*		Block private networks	
<input checked="" type="checkbox"/>	0/0 B	*	Reserved Not assigned by IANA	*	*	*	*	*		Block bogon networks	

No rules are currently defined for this interface

All incoming connections on this interface will be blocked until pass rules are added. Click the button to add a new rule.

Add

Add

Delete

Toggle

Copy

Save

Separator

Firewall / Rules / LAN

Floating WAN LAN OPT1 OPT2

Rules (Drag to Change Order)

<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	1/13.48 MiB	*	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule	
<input type="checkbox"/>	1/43.25 MiB	IPv4 *	LAN subnets	*	*	*	*	none		Default allow LAN to any rule	
<input type="checkbox"/>	0/0 B	IPv6 *	LAN subnets	*	*	*	*	none		Default allow LAN IPv6 to any rule	

Add

Add

Delete

Toggle

Copy

Save

Separator

Firewall / Rules / OPT2

Floating

WAN

LAN

OPT1

OPT2

Rules (Drag to Change Order)

<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	<div><div>✓</div><div>1/195 KiB</div></div>	IPv4+6	*	*	*	*	*	none			<div><div></div><div></div><div></div><div></div><div></div></div>
<input type="checkbox"/>	<div><div>✓</div><div>0/0 B</div></div>	IPv4+6 TCP	LOGSTASH_CLIENTS	*	SIEM_SERVER	5044	*	none		Allow Filebeat → Logstash	<div><div></div><div></div><div></div><div></div><div></div></div>
<input type="checkbox"/>	<div><div>✗</div><div>0/67 KiB</div></div>	IPv4+6	*	*	*	*	*	none		Block SIEM outbound	<div><div></div><div></div><div></div><div></div><div></div></div>
<input type="checkbox"/>	<div><div>✗</div><div>0/0 B</div></div>	IPv4+6	*	*	SIEM_SERVER	*	*	none		Block SIEM inbound	<div><div></div><div></div><div></div><div></div><div></div></div>

↑

Add

↓

Add

Delete

Toggle

Copy

Save

+

Separator

i

3. Triển khai Suricata Inline IDS/IPS

- Theo mô hình trên, nhóm triển khai Suricata làm Inline IDS/IPS trên máy Ubuntu Server 192.168.71.171/24 để giám sát lớp mạng 192.168.85.0/24 và đẩy Suricata Logs về máy ELK là 192.168.100.128

- Cấu hình inline IDS/IPS trong file /etc/suricata/suricata.yml

```
af-packet:
- interface: ens37
  threads: 1
  defrag: no
  cluster-type: cluster_flow
  cluster-id: 100
  copy-mode: ips
  copy-iface: ens38
  buffer-size: 64535
  use-mmap: yes
  tpacket-v3: no

- interface: ens38
  threads: 1
  cluster-id: 101
  defrag: no
  cluster-type: cluster_flow
  copy-mode: ips
  copy-iface: ens37
  buffer-size: 64535
  use-mmap: yes
  tpacket-v3: no
```

- Ngoài bộ Rules không lỗi của cộng đồng, nhóm có viết thêm 1 bộ rule ở local nhằm mục đích kiểm thử hệ thống hoạt động ổn không:

```
wanthinnn@ubuntuserver:~$ sudo cat
/var/lib/suricata/rules/local.rules
#alert tls any any -> any any (msg:"[TEST] TLS traffic detected";
sid:9999999; rev:1;)
# 1.Initial Access
# Ping detected
alert icmp any any -> any any (msg:"[ALERT] ICMP Ping detected";
sid:1000001; rev:1;)
```

```

# TCP SYN Flood Detected
alert tcp any any -> any any (msg:"[ALERT] TCP SYN Packet
Detected"; flags:S; threshold:type threshold, track by_src, count
20, seconds 10; sid:1000002; rev:1;)

# UDP Flood Detected
alert udp any any -> any any (msg:"[ALERT] UDP Packet Detected";
threshold:type threshold, track by_src, count 20, seconds 10;
sid:1000003; rev:1;)

# SSH Brute Force Detection
alert tcp any any -> any 22 (msg:"[ALERT] SSH Brute Force
Attempt"; flow:to_server,established; threshold:type threshold,
track by_src, count 5, seconds 60; content:"SSH"; nocase;
sid:1000004; rev:1;)

# Path Travel
#drop tcp any any -> 192.168.71.0/24 80 (msg:"[DROP] Potential
Path Traversal Attack Detected"; flow:established; content:"GET";
content:"HTTP"; fast_pattern; content:"../"; nocase;
session:all; sid:1000005; rev:1;)

# 2. Resource Development
# Suspicious Tool Download
alert http any any -> any any (msg:"[ALERT] Suspicious Tool
Download"; flow:to_server,established; content:"/*.*exe"; nocase;
sid:2000001; rev:1;)

# Suspicious SNI Detected
alert tls any any -> any any (msg:"[ALERT] Suspicious SNI detected
in TLS handshake"; tls.sni; content:"suspicious.example.com";
nocase; sid:2000002; rev:1;)

# 3. Reconnaissance
# Banner Grabbing Detection
alert tcp any any -> any 80 (msg:"[ALERT] Banner Grabbing
Attempt"; flow:to_server,established; content:"HTTP/1.1";

```

```

nocase; detection_filter: track by_src, count 3, seconds 5;
sid:3000001; rev:1;)
# Port Scan Detection
alert ip any any -> 192.168.71.129 any (msg:"[ALERT] Port scan
detected from other device"; sid:3000002; rev:1;)

# 4. Execution
# Command Injection Attempt
#alert http any any -> any any (msg:"[ALERT] Potential Command
Injection Attempt"; flow:to_server,established; content:"cmd=";
nocase; pcre:"/[\\;\\|\\&]\\s*cmd/"; sid:4000001; rev:1;)
alert http any any -> any any (msg:"[ALERT] Potential Command
Injection Attempt"; flow:to_server,established;
uricontent:"cmd="; nocase; sid:4000001; rev:1;)
# 5. Persistence
# Suspicious SMB Traffic
alert tcp any any -> any 135 (msg:"[ALERT] Potential RPC/SMB
Exploit Attempt"; flow:to_server,established; content:"|90 90
90|"; offset:0; depth:10; sid:5000001; rev:1;)

# 6. Privilege Escalation
alert tcp any any -> any 135 (msg:"[ALERT] Potential RPC/SMB
Exploit Attempt"; flow:to_server,established; content:"|90 90
90|"; offset:0; depth:10; sid:6000001; rev:1;)
alert tls any any -> any 443 (msg:"[ALERT] TA0004 T1548: Possible
abuse of elevation control mechanism detected"; tls.sni;
pcre:"/cmd\\.exe|powershell\\.exe|wscript\\.exe|cscript\\.exe|reged
it\\.exe|mshta\\.exe|bash\\b|sudo\\b|su\\b|pkexec|gksudo|kdesudo/i";
sid:6000002; rev:5;)

# 7. Defense Evasion
# Suspicious TLS Version

```



```
alert tls any any -> any any (msg:"[ALERT] Suspicious TLS Version Used"; tls.version:0x0301; sid:7000001; rev:1;)
```

8. Credential Access

FTP Login Attempt

```
alert ftp any any -> any 21 (msg:"[ALERT] FTP Login Attempt"; flow:to_server,established; content:"USER "; sid:8000001; rev:1;)
```

```
alert http any any -> any 443 (msg:"[ALERT] TA0006 Credential Access: Potential credential exposure in Elasticsearch query over HTTPS"; flow:established,to_server; content:"/elasticsearch/"; nocase; file_data; content:"password="; nocase; sid:8000002; rev:2;)
```

9. Discovery

ICMP Ping Sweep

```
alert icmp any any -> any any (msg:"[ALERT] ICMP Ping Sweep Detected"; threshold:type threshold, track by_src, count 10, seconds 5; sid:9000001; rev:1;)
```

10. Lateral Movement

SMB Null Session Scan

```
alert smb any any -> any any (msg:"[ALERT] SMB Null Session Scan Detected"; content:"|00 00 00|"; depth:4; sid:10000001; rev:1;)
```

11. Collection

Large FTP File Transfer

```
alert ftp any any -> any 21 (msg:"[ALERT] Large FTP File Transfer Detected"; flow:to_server,established; content:"SIZE "; sid:11000001; rev:1;)
```

```

# 12. Command and Control
# DNS Tunneling Detection
alert dns any any -> any any (msg:"[ALERT] Potential DNS Tunneling
Detected"; dns.query; pcre:"/([a-z0-9]{20,}\.)/i"; sid:12000001;
rev:1;)

# 13. Exfiltration
# Unusual HTTP POST Large Data Transfer
alert http any any -> any any (msg:"[ALERT] Unusual HTTP POST
Large Data Transfer Detected"; flow:to_server,established;
content:"POST"; content:"Content-Length:"; threshold:type
threshold, track by_src, count 3, seconds 30; sid:13000001;
rev:1;)

# 14. Impact
# TCP SYN Flood Detection
alert tcp any any -> any any (msg:"[ALERT] Potential TCP SYN Flood
Detected"; flags:S; threshold:type threshold, track by_src, count
100, seconds 10; sid:14000001; rev:1;)

```

- Cấu hình Filebeat.yml:

```

wanthinnn@ubuntuserver:~$ sudo cat /etc/filebeat/filebeat.yml
# Filebeat inputs
filebeat.inputs:
# filestream is an input for collecting log messages from files.
- type: filestream
  # Unique ID among all inputs, an ID is required.
  id: my-filestream-id
  # Change to true to enable this input configuration.
  enabled: true
  - /var/log/suricata/eve.json

```

```
# Filebeat modules
filebeat.config.modules:
  # Glob pattern for configuration loading
  path: ${path.config}/modules.d/*.yaml
  # Set to true to enable config reloading
  reload.enabled: false

# Elasticsearch template setting
setup.template.settings:
  index.number_of_shards: 1

# Logstash Output
output.logstash:
  # The Logstash hosts
  hosts: ["siem-dacn.local:5044"]

  # Optional SSL. By default is off.
  # List of root certificates for HTTPS server verifications
  ssl.certificate_authorities:
  ["/etc/filebeat/certs/rootCA.crt"]
```

- Chạy Suricata ở chế độ Inline mode:

```
wanthinnn@suricata:~$ sudo systemctl status suricata.service
● suricata.service - Suricata IDS/IPS in AF_PACKET inline mode
   Loaded: loaded (/etc/systemd/system/suricata.service; disabled; vendor preset: enabled)
   Active: active (running) since Sun 2025-04-27 00:05:17 +07; 2h 49min ago
     Process: 2072 ExecStartPre=/bin/mkdir -p /run/suricata (code=exited, status=0/SUCCESS)
     Process: 2091 ExecStartPre=/bin/chown root:root /run/suricata (code=exited, status=0/SUCCESS)
     Process: 2092 ExecStartPre=/bin/chmod 0755 /run/suricata (code=exited, status=0/SUCCESS)
    Main PID: 2093 (Suricata-Main)
       Tasks: 8 (limit: 2570)
      Memory: 506.2M
    CGroup: /system.slice/suricata.service
            └─2093 /usr/bin/suricata -c /etc/suricata/suricata.yaml --af-packet --runmode workers --pidfile /run/suricata/suricata.pid

Apr 27 00:05:17 suricata systemd[1]: Stopped Suricata IDS/IPS in AF_PACKET inline mode.
Apr 27 00:05:17 suricata systemd[1]: Starting Suricata IDS/IPS in AF_PACKET inline mode...
Apr 27 00:05:17 suricata systemd[1]: Started Suricata IDS/IPS in AF_PACKET inline mode.
Apr 27 00:05:17 suricata suricata[2093]: Info: conf-yaml-loader: Configuration node 'stream' redefined.
Apr 27 00:05:17 suricata suricata[2093]: i: suricata: This is Suricata version 7.0.10 RELEASE running in SYSTEM mode
Apr 27 00:05:17 suricata suricata[2093]: W: runmodes: disabling livedev.use-for-tracking with IPS mode. See ticket #6726.
Apr 27 00:05:43 suricata suricata[2093]: i: threads: Threads created -> W: 2 FM: 1 FR: 1 Engine started.
wanthinnn@suricata:~$
```

- Sau cấu hình trên, Logs từ Suricata sẽ được đẩy về Filebeat, rồi từ Filebeat sẽ đẩy về Logstash trên máy SIEM Server.

4. Triển khai SIEM Server (có cập nhật so với trước đây)

4.1. Sơ lược

- Trước đây: sử dụng card NAT với địa chỉ 192.168.71.128
- Bây giờ: Sử dụng Host-only với địa chỉ 192.168.100.128/24
- Mục tiêu: cô lập máy SIEM Server vào 1 LAN riêng, firewall chỉ cho phép giao tiếp TCP/5044, còn lại inbound và outbound khác đều bị chặn và chỉ cho phép truy cập vào Kibana/Logstash/Elasticsearch thông qua tên miền local: siem-dacn.local với giao thức HTTPS.

4.2. Luồng dữ liệu

- **Thu thập và gửi log**
 - + Trên các máy source (Windows/Linux/Suricata/etc.) đều chạy Filebeat, cấu hình gửi tới https://siem-dacn.local:5044.
 - + Filebeat transport qua HTTPS (443) đến Nginx trên SIEM.
- **Reverse proxy bởi Nginx**: Nginx lắng nghe trên 443, route tất cả request /logstash → backend Beats input của Logstash trên localhost:5044.
- **Xử lý bởi Logstash**
 - + Logstash input beats { port => 5045 host => "0.0.0.0" } nhận dữ liệu thô.
 - + Chạy qua các filter (grok, json, prune, mutate...) để chuẩn hóa và gắn nhãn.
 - + file conf và parser logs:

```
input {
  beats {
    port => 5045
    ssl => false
    host => "0.0.0.0"
  }
}

filter {
  #####
  # Log Suricata (eve.json)
  #####
  if [log][file][path] =~ "suricata/eve.json" {
    # Gắn nhãn nguồn log
    mutate { add_field => { "log_source" => "suricata" } }
    # Parse JSON nội dung log
    json { source => "message" }
```

```

# Chỉ giữ sự kiện có event_type = alert hoặc drop
if [event_type] != "alert" and [event_type] != "drop" {
    drop { }
}
# Đưa các trường trong [alert] lên cấp trên
mutate {
    add_field => { "signature_id"      =>
"%{[alert][signature_id]}" }
    add_field => { "alert_signature"  =>
"%{[alert][signature]}" }
    add_field => { "alert_action"      => "%{[alert][action]}" }
}
# Xóa các trường không cần thiết
mutate { remove_field => [ "alert", "message" ] }
}

#####
# Log Nginx - access.log
#####
if [log][file][path] =~ "nginx/access.log" {
    mutate { add_field => { "log_source" => "nginx_access" } }
    # Grok parse theo định dạng access log: client_ip, method,
request, response_code, bytes, referrer, agent
    grok {
        match => {
            "message" => [
                # 1) Chuẩn HTTP request
                "%{IPORHOST:client_ip} %{DATA:ident} %{DATA:auth}
\\[%{HTTPDATE:timestamp}\\] \\\"%{WORD:method} %{DATA:request}
HTTP/%{NUMBER:httpversion}\\\" %{INT:response_code} %{INT:bytes}
\\\"%{DATA:referrer}\\\" \\\"%{DATA:agent}\\\"\"",
                # 2) Fallback: bất kỳ chuỗi trong dấu "..."
                "%{IPORHOST:client_ip} %{DATA:ident} %{DATA:auth}
\\[%{HTTPDATE:timestamp}\\] \\\"%{DATA:raw_request}\\\"
%{INT:response_code} %{INT:bytes} \\\"%{DATA:referrer}\\\"
\\\"%{DATA:agent}\\\"\""
            ]
        }
    }
}
# Nếu chỉ có raw_request, gán thành method cho dễ xài
if [raw_request] and ![method] {
    mutate {

```

```

        add_field => { "method" => "%{raw_request}" }
        remove_field => [ "raw_request" ]
    }
}
# Loại bỏ các trường phụ và message gốc
mutate { remove_field => [ "ident", "auth", "message" ] }
}

#####
# Log Nginx - error.log
#####
else if [log][file][path] =~ "nginx/error.log" {
    mutate { add_field => { "log_source" => "nginx_error" } }
    # Grok parse error log: host, program và thông điệp lỗi
    grok {
        match => { "message" => "%{DATA:host}
%{DATA:error_program}: %{GREEDYDATA:error_message}" }
    }
    mutate { remove_field => [ "message" ] }
}

#####
# Log Hệ thống (auth.log, syslog, messages)
#####
else if [log][file][path] =~ "(auth\\.log|syslog|messages)" {
    mutate { add_field => { "log_source" => "system" } }
    # Grok parse Syslog tiêu chuẩn: host, chương trình, thông
điệp
    grok {
        match => { "message" => "%{SYSLOGHOST:syslog_host}
%{SYSLOGPROG:sys_program}: %{GREEDYDATA:sys_message}" }
    }
    mutate { remove_field => [ "message" ] }
}

#####
# Windows Security Logs
#####
else if [log][file][path] =~ "Security" {
    mutate { add_field => { "log_source" => "windows_security" }
}
}

```

```

    # Không cần parse thêm; giữ các trường cơ bản như
    winlog.event_id, event_data.SubjectUserName, event.action,
    message
  }

  #####
  # Các log khác
  #####
  else {
    mutate { add_field => { "log_source" => "other" } }
    # Không parse thêm; sẽ giữ lại timestamp và message gốc
  }
  mutate {
    remove_field => ["host", "agent", "ecs", "input", "log",
"fileset"]
  }

  #####
  # Prune filter: chỉ giữ các trường cần thiết
  #####
  prune {
    whitelist_names => [
      "@timestamp", "log_source",
      # Trường Suricata
      "event_type", "src_ip", "dest_ip", "proto", "flow_id",
      "signature_id", "alert_signature", "alert_action",
"community_id",
      # Trường Nginx access
      "client_ip", "method", "request", "response_code", "bytes",
"referrer", "agent",
      # Trường Nginx error
      "host", "error_program", "error_message",
      # Trường hệ thống
      "syslog_host", "sys_program", "sys_message",
      # Trường Windows
      "host.name", "winlog.event_id",
"winlog.event_data.SubjectUserName", "event.action",
      # Luôn giữ message để hiển thị (nếu cần)
      "message"
    ]
  }
}

```



```

output {
  elasticsearch {
    index => "system_logs-2"
    hosts => ["https://localhost:9200"]
    user => "wanthinnn"
    password => "Thienlai0941841870@# $"
    ssl => true
    ssl_certificate_verification => false
  }
  # Thêm output debug
  stdout { codec => rubydebug }
}

```

- **Lưu trữ vào Elasticsearch:** Logstash output gửi event đã parse → Elasticsearch trên localhost:9200.

- **Hiển thị trên Kibana**

+ Người dùng truy cập <https://siem-dacn.local/kibana> → Nginx reverse proxy → Kibana UI.

+ Kibana query Elasticsearch, dựng dashboard và bảng điều khiển từ index system_logs*.

5. Giả lập tấn công

Mục tiêu: Kiểm tra Suricata phát hiện xâm nhập và khả năng hiển thị logs-parser của Kibana, đồng thời xây dựng các detection rule & alert trong Kibana SIEM, mapping sang MITRE ATT&CK.

5.1. ICMP Flood Attack – DDoS [ALERT]

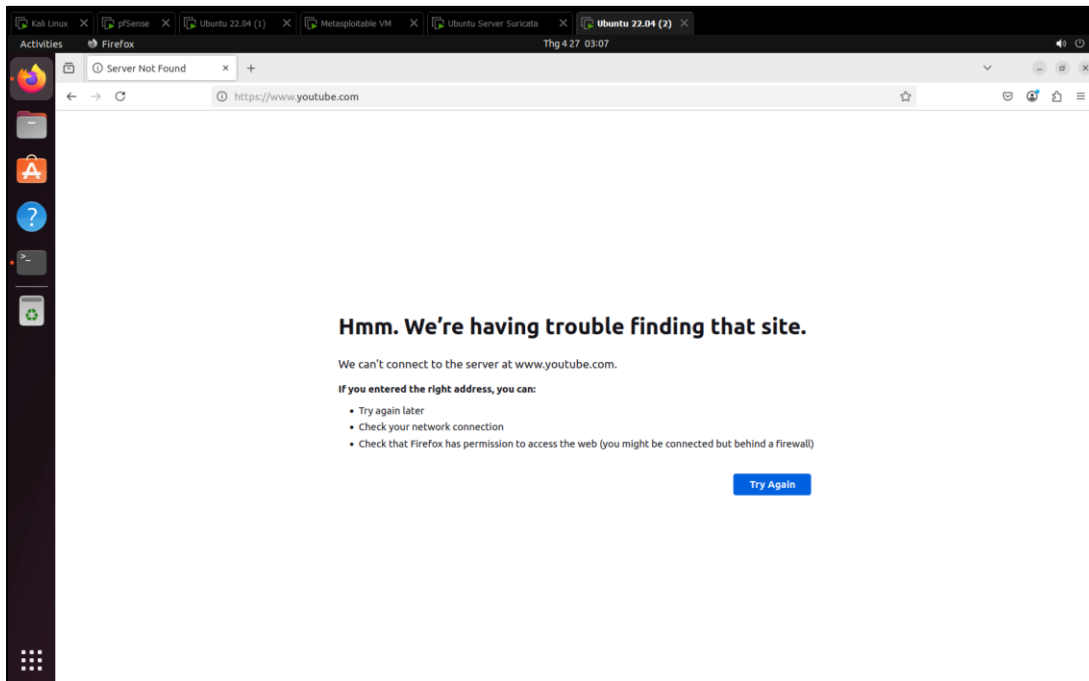
- Trên máy Kali, ta tấn công vào máy Ubuntu:

```

(kali㉿kali)-[~]
└─$ sudo hping3 -1 --flood 192.168.85.129
HPING 192.168.85.129 (eth0 192.168.85.129): icmp mode set, 28 headers + 0 data bytes
hping in flood mode, no replies will be shown
^C
--- 192.168.85.129 hping statistic ---
4922485 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms

```

- Lúc này trên máy Ubuntu không thể vào internet được:



```
wanthinnn@ubuntu-2:~$ telnet google.com 443
telnet: could not resolve google.com/443: Temporary failure in name resolution
wanthinnn@ubuntu-2:~$
```

- Kiểm tra logs đã được parser:

```
Apr 27, 2025 @ 03:06:18.566 @timestamp Apr 27, 2025 @ 03:06:18.566 alert_action allowed alert_signature [ALERT] ICMP HPing3 detected community_id 1:quS541HzcU
oV8ijzejF3qFV/2MA= dest_ip 10.81.85.100 event_type alert flow_id 721,549,906,126,607 log_source [suricata, other] proto ICM
P signature_id 1000001 src_ip 192.168.85.129 _id PRa1c5YB7vNNq0soPTYq _ignored - _index system_logs-2 _score -

Apr 27, 2025 @ 03:06:18.566 @timestamp Apr 27, 2025 @ 03:06:18.566 alert_action allowed alert_signature [ALERT] ICMP HPing3 detected community_id 1:quS541HzcU
oV8ijzejF3qFV/2MA= dest_ip 192.168.85.129 event_type alert flow_id 721,549,906,126,607 log_source [suricata, other] proto ICM
P signature_id 1000001 src_ip 10.81.85.100 _id PBa1c5YB7vNNq0soPTYq _ignored - _index system_logs-2 _score -
```

=> Ta thấy các thông tin hiện lên đầy đủ và chi tiết, dễ nắm bắt được.

5.2. UDP Flood Attack – DDoS [DROP]

Tiếp theo, ta tấn công UDP Flood, nhưng mà lần này Suricata sẽ Drop nếu phát hiện, đảm bảo hệ thống an toàn, không bị sập:

```
(kali@kali)-[~]
$ sudo hping3 --udp --flood -p 53 192.168.85.129
HPING 192.168.85.129 (eth0 192.168.85.129): udp mode set, 28 headers + 0 data bytes
hping in flood mode, no replies will be shown
^C
--- 192.168.85.129 hping statistic ---
785758 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

Kiểm tra:

<input type="checkbox"/>	✓	Apr 27, 2025 @ 03:14:14.688	@timestamp Apr 27, 2025 @ 03:14:14.688 alert_action blocked alert_signature [DROP] UDP Packet Detected app_proto faile d community_id 1:V6vyX6Cc8BuSXLem/6Yk86fkd4Y= dest_ip 192.168.85.129 event_type alert flow_id 1,902,114,588,113,102 log_source [su ricata, other] proto UDP signature_id 10000011 src_ip 10.81.85.100 _id Jxa8c5YB7vNNq0sogTuc _ignored - _index system_logs-...
<input type="checkbox"/>	✓	Apr 27, 2025 @ 03:14:14.688	@timestamp Apr 27, 2025 @ 03:14:14.688 alert_action blocked alert_signature [DROP] UDP Packet Detected app_proto faile d community_id 1:Cp4Ma0o142SMC1/wVxdFK5uitjk= dest_ip 192.168.85.129 event_type alert flow_id 1,875,360,505,709,231 log_source [su ricata, other] proto UDP signature_id 10000011 src_ip 10.81.85.100 _id Jha8c5YB7vNNq0sogTuc _ignored - _index system_logs-...
<input type="checkbox"/>	✓	Apr 27, 2025 @ 03:14:14.688	@timestamp Apr 27, 2025 @ 03:14:14.688 alert_action blocked alert_signature [DROP] UDP Packet Detected app_proto faile d community_id 1:QAqD4zF7foUc+JJMkfy3DouxV4= dest_ip 192.168.85.129 event_type alert flow_id 1,638,499,860,132,516 log_source [su ricata, other] proto UDP signature_id 10000011 src_ip 10.81.85.100 _id JRa8c5YB7vNNq0sogTuc _ignored - _index system_logs-...

5.3. Command-and-Control (C2) qua HTTPS/TLS [Bản đơn giản]

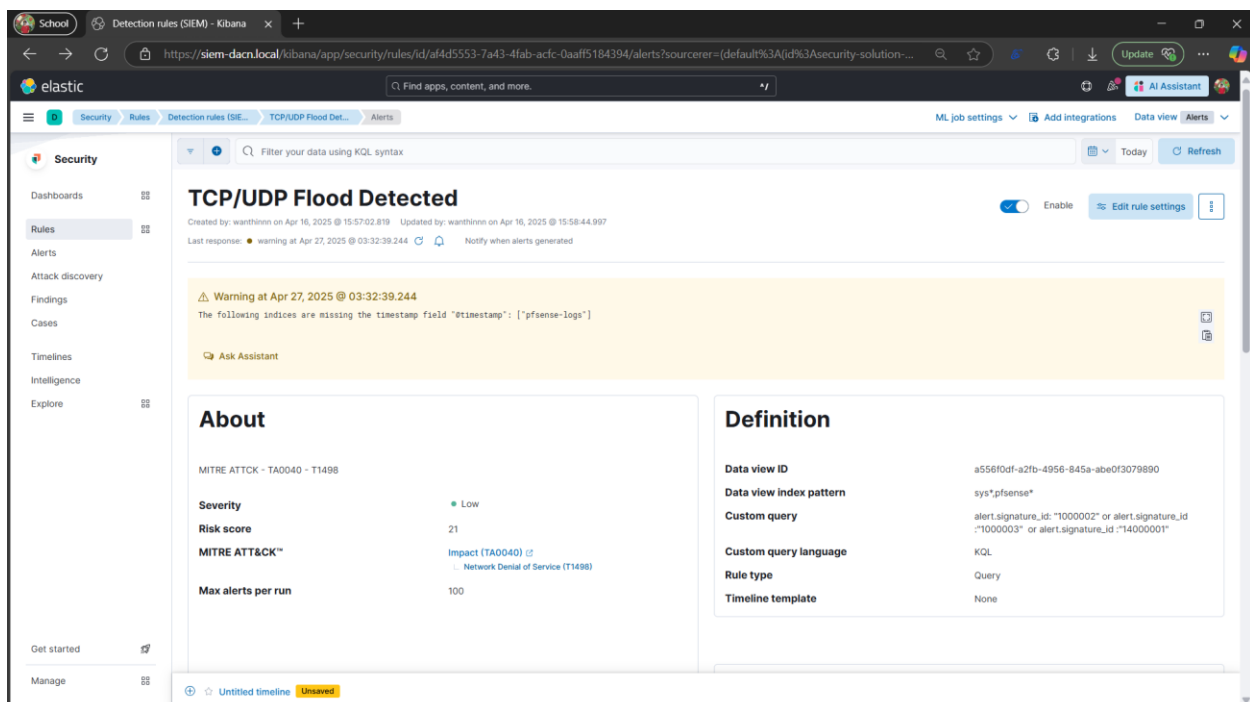
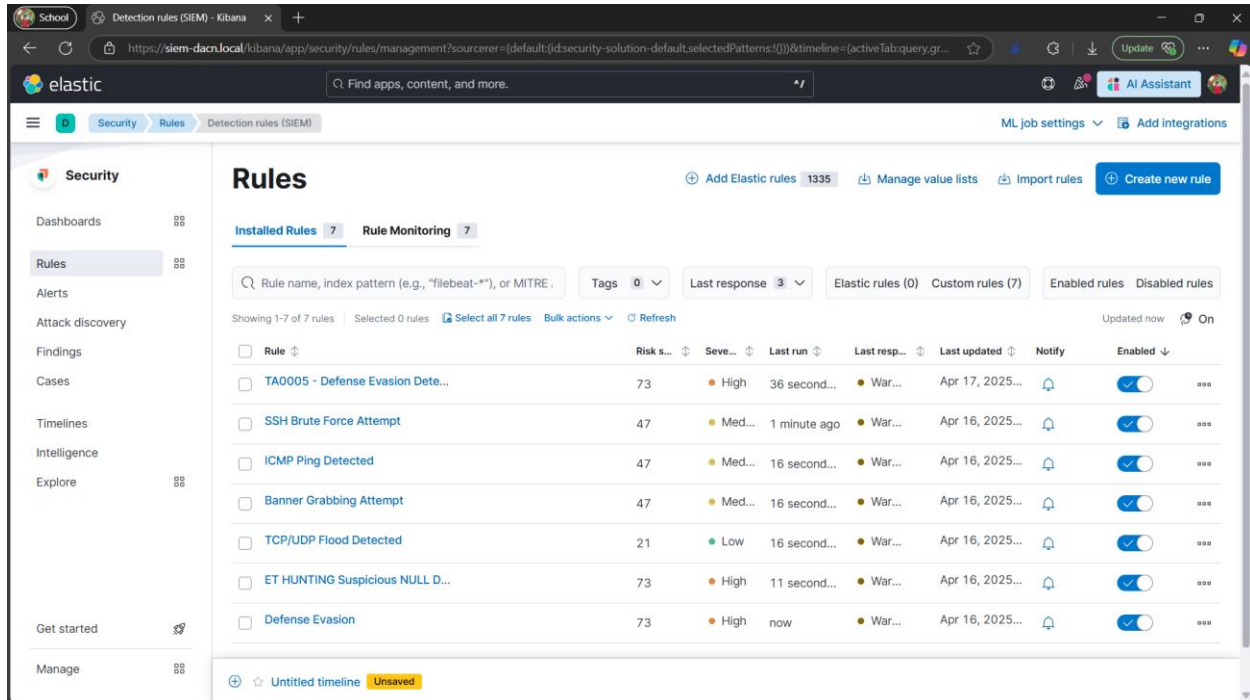
```
(kali㉿kali)~[~]  
$ for i in {1..10000}; do cmd=$(shuf -n1 -e sudo id pwd whoami uname \-a ls ps\ aux ifconfig netstat \-an uptime); echo "[${i}] $cmd"  
; echo "$cmd" | openssl s_client -connect siem-dacn.local:443 -servername sudo </dev/null; echo "-----"; sleep 0.1; done
```

- Lặp 10000 lần, mỗi lần chọn ngẫu nhiên một lệnh hệ thống (ví dụ id, whoami, ls, ifconfig...), rồi
- Mở một kết nối TLS tới siem-dacn.local:443 bằng openssl s_client,
- Đưa tên lệnh đó vào stream TLS (tức gửi “command” đã chọn qua kênh mã hóa),
- Tạm dừng 0.1 giây rồi tiếp tục => Máy chủ SIEM Server bị quá tải
- Lúc này, máy chủ Nginx sẽ gửi liên tục logs về cho Kibana:

<input type="checkbox"/>	✓	Apr 27, 2025 @ 03:20:12.122	@timestamp Apr 27, 2025 @ 03:20:12.122 bytes 166 client_ip 10.81.85.100 log_source nginx_access method whoam i referrer - response_code 400 _id QRb8c5YB7vNNq0so-UHq _ignored - _index system_logs-2 _score -
<input type="checkbox"/>	✓	Apr 27, 2025 @ 03:20:12.122	@timestamp Apr 27, 2025 @ 03:20:12.122 bytes 166 client_ip 10.81.85.100 log_source nginx_access method l s referrer - response_code 400 _id QBb8c5YB7vNNq0so-UHq _ignored - _index system_logs-2 _score -
<input type="checkbox"/>	✓	Apr 27, 2025 @ 03:20:12.122	@timestamp Apr 27, 2025 @ 03:20:12.122 bytes 166 client_ip 10.81.85.100 log_source nginx_access method pw d referrer - response_code 400 _id Lxb8c5YB7vNNq0so-UHa _ignored - _index system_logs-2 _score -
<input type="checkbox"/>	✓	Apr 27, 2025 @ 03:20:12.122	@timestamp Apr 27, 2025 @ 03:20:12.122 bytes 166 client_ip 10.81.85.100 log_source nginx_access method sud o referrer - response_code 400 _id Hxb8c5YB7vNNq0so-UG5 _ignored - _index system_logs-2 _score -

6. Kibana Detection rules

Dựa vào những logs ta thu về, tiến hành viết Rules cho Kibana để sau này nó detected và alert lên. Dưới đây, nhóm dựa vào signature_id của Suricata để viết rule và đồng thời mapping với MITRE ATT&CK:



School Detection rules (SIEM) - Kibana x +

https://siem-dacn.local/kibana/app/security/rules/id/9b09218a-c745-444c-9f52-a2b9939aab5e/alerts?sourcerer=(default%3A)id%3Asecurity-solution-defau...

elastic Find apps, content, and more.

Security Rules Detection rules (SIEM) Banner Grabbing Att... Alerts ML job settings Add integrations Data view Alerts

Security

Dashboards Rules Alerts Attack discovery Findings Cases Timelines Intelligence Explore

Get started Manage

Banner Grabbing Attempt

Created by: warthinm on Apr 16, 2025 @ 16:09:49.390 Updated by: warthinm on Apr 16, 2025 @ 16:12:52.494

Last response: warning at Apr 27, 2025 @ 03:33:09.282 Notify when alerts generated

Warning at Apr 27, 2025 @ 03:33:09.282

The following indices are missing the timestamp field "timestamp": ["pf-sense-logs"]

Ask Assistant

About

MITRE ATTCK - TA0007 - T1046

Severity Medium

Risk score 47

MITRE ATT&CK**

Discovery (TA0007) Network Service Discovery (T1046)

Max alerts per run 100

Definition

Data view ID a556f0df-a2fb-4956-845a-abe0f3079890

Data view index pattern sys*pf-sense*

Custom query alert.signature_id : "3000001" or alert.signature_id : "3000002"

Custom query language KQL

Rule type Query

Timeline template None

Untitled timeline Unsaved

School Alerts - Kibana x +

https://siem-dacn.local/kibana/app/security/alerts?sourcerer=(default{id:security-solution-default,selectedPatterns:{}})&timeRange=(global{linkTo:(timeline...

elastic Find apps, content, and more.

Security Alerts ML job settings Add integrations Data view Alerts

Security

Dashboards Rules Alerts Attack discovery Findings Cases Timelines Intelligence Explore

Get started Manage

Alerts

Filter your data using KQL syntax Today Refresh

Assignees Manage rules

Status open 1 Severity User Host

Summary Trend Counts Treemap

Severity levels

Levels	Count
Low	415
Medium	6

421 alerts

Alerts by name

Rule name	Count
TCP/UDP Flood Detected	415
ICMP Ping Detected	6

< 1 >

Top alerts by

hostName

No items found

Columns 12 Sort fields 1 421 alerts Updated now Additional filters Grid view Group alerts by: None

Actions	@timestamp	Rule	Assignees	Severity	Risk Score	Reason
	2025-04-26T17:30:13.752Z	TCP/UDP Flood Detected		low	21	event created low alert TCP/UDP Flood Detected.

Untitled timeline Unsaved