**SIEM RULE DETECTION – MITRE ATT&CK**

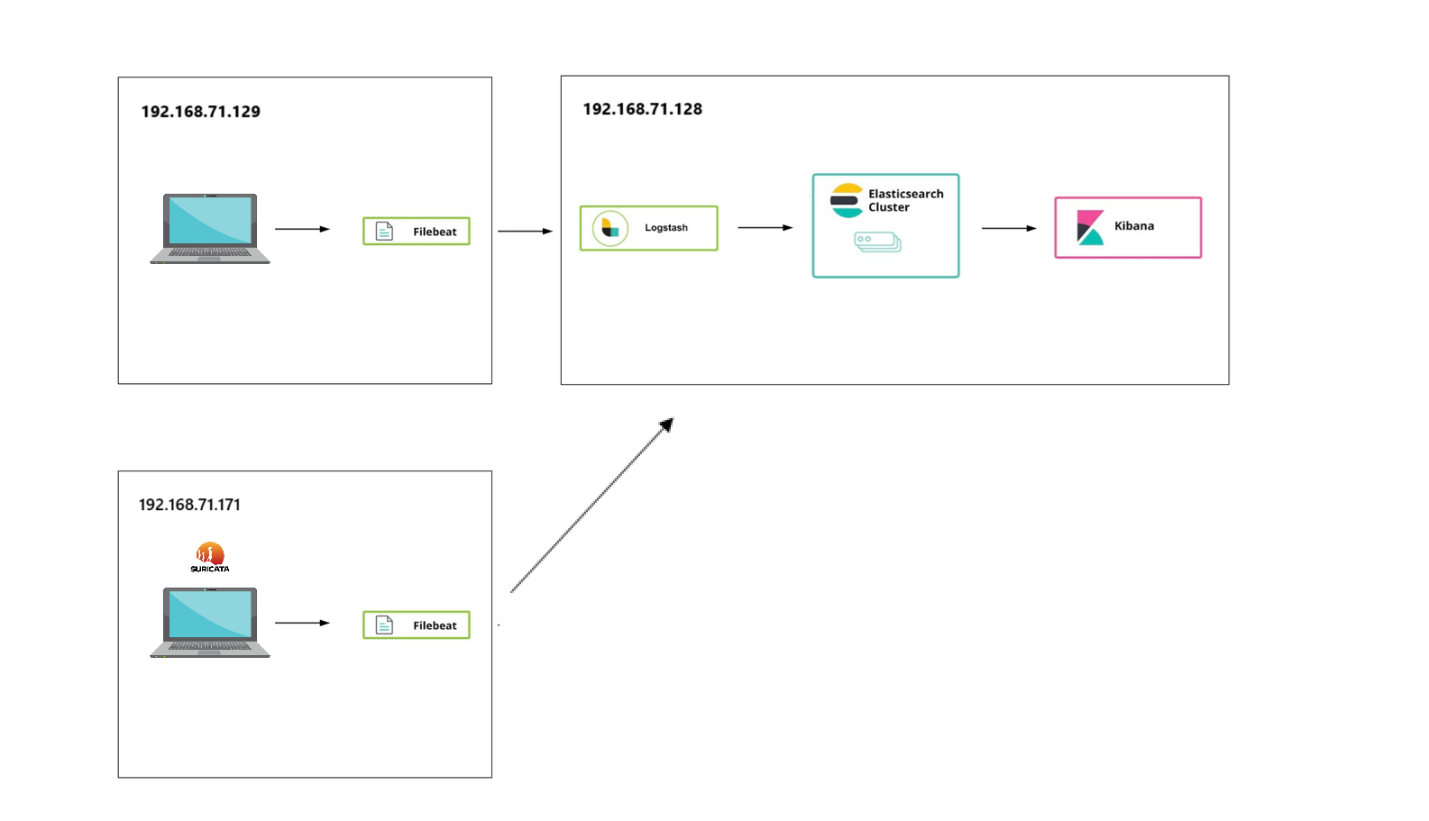
# 0. Mô hình triển khai

- 1 máy Ubuntu Server cài đặt Suricata làm Host-based IDS

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

- 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



Mô hình triển khai

# 1. Triển khai Nginx Reverse Proxy

- Ta cần đảm bảo bảo mật các kết nối giữa các máy với nhau khi máy Client đẩy Log về ELK Sever, giữa Client với Client,….. Ví thế nhóm sử dụng Nginx làm Reverse Proxy như sau:

+ Mã hoá lưu lượng mạng khi Filebeat từ các Client đẩy Logs về Server (HTTPS)

+ Đảm bảo truy cập/đăng nhập/thao tác với máy ELK Server (HTTPS khi người dùng bên ngoài truy cập vào Kibana, ngoài ra cũng mã hoá lưu lượng mạng khi giao tiếp với ElasticSeach và Logstash)

+ Tạo 1 tên miền Local cho máy 192.168.71.128 -> siem-dacn.local

+ Tạo các chứng chỉ tự ký và các key liên quan thông qua: mkcert

- File cấu hình Nginx như sau:

|  |
| --- |
| wanthinnn@ubuntu-1:~$ cat /etc/nginx/sites-available/kibana  server {  listen 443 ssl;  server\_name siem-dacn.local;  # Đường dẫn tới chứng chỉ và private key của mkcert  ssl\_certificate /etc/kibana/certs/siem-dacn.local.pem;  ssl\_certificate\_key /etc/kibana/certs/siem-dacn.local-key.pem;  # Các tùy chọn SSL bổ sung (có thể tùy chỉnh)  ssl\_protocols TLSv1.3 TLSv1.2;  # Ưu tiên cipher mạnh mẽ, loại bỏ hoàn toàn những thứ yếu  ssl\_ciphers 'ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-CHACHA20-POLY1305:ECDHE-RSA-CHACHA20-POLY1305:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-SHA256';  # Bắt buộc dùng server cipher chứ không theo client  ssl\_prefer\_server\_ciphers on;  # Các tuỳ chọn bổ sung tăng độ bảo mật  ssl\_session\_cache shared:SSL:10m;  ssl\_session\_timeout 1h;  ssl\_ecdh\_curve X25519:prime256v1;  ssl\_stapling on;  ssl\_stapling\_verify on;  location /kibana {  proxy\_pass https://192.168.71.128:5601;  proxy\_http\_version 1.1;  proxy\_set\_header Upgrade $http\_upgrade;  proxy\_set\_header Connection "upgrade";  proxy\_set\_header Host $host;  proxy\_cache\_bypass $http\_upgrade;  proxy\_ssl\_verify off; # ← QUAN TRỌNG nếu bạn dùng mkcert hoặc cert tự ký  #rewrite ^/kibana/(.\*)$ /$1 break;  }  # ELASTICSEARCH  location /elasticsearch/ {  proxy\_pass https://192.168.71.128:9200/;  proxy\_http\_version 1.1;  proxy\_set\_header Host $host;  proxy\_set\_header X-Real-IP $remote\_addr;  proxy\_set\_header X-Forwarded-For $proxy\_add\_x\_forwarded\_for;  rewrite ^/es/(.\*)$ /$1 break;  }  # LOGSTASH (nếu có HTTP API)  location /logstash/ {  proxy\_pass https://192.168.71.128:9600/;  proxy\_http\_version 1.1;  # Nếu chứng chỉ Logstash tự ký, thêm tùy chọn dưới đây để bỏ xác minh:  proxy\_ssl\_verify off;  proxy\_set\_header Connection "";  proxy\_set\_header Host $host;  proxy\_cache\_bypass $http\_upgrade;  rewrite ^/logstash/(.\*)$ /$1 break;  }  }  # Tùy chọn: chuyển hướng từ HTTP sang HTTPS  server {  listen 80;  server\_name siem-dacn.local;  #deny all;  return 301 https://$host$request\_uri;  } |

- Giải thích file trên:

+ Cấu hình Nginx dùng HTTPS cho domain siem-dacn.local.

+ Dùng chứng chỉ SSL tự ký từ mkcert.

+ Thiết lập reverse proxy cho Kibana, Elasticsearch, Logstash.

+ Bỏ xác minh SSL khi proxy đến dịch vụ dùng chứng chỉ tự ký.

+ Tự động chuyển hướng HTTP sang HTTPS để tăng bảo mật.

- Kiểm tra HTTPS:

A screenshot of a computer

AI-generated content may be incorrect.

# 2. Triển khai Suricata Host-based IDS

- Theo mô hình trên, nhóm triển khai Suricata làm Host-based IDS trên máy Ubuntu Server 192.168.71.171/24 để giám sát và đẩy Suricata Logs về máy ELK là 192.168.71.128

A screenshot of a computer program

AI-generated content may be incorrect.

- Ngoài bộ Rules khổng lồ 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|regedit\.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;) |

- Sau đó tiến hành kết nối để Suricata có thể đẩy logs được về Filebeat:

|  |
| --- |
| wanthinnn@ubuntuserver:~$ sudo cat /etc/filebeat/modules.d/suricata.yml  # Module: suricata  # Docs: https://www.elastic.co/guide/en/beats/filebeat/7.17/filebeat-module-suricata.html  - module: suricata  # All logs  eve:  enabled: true  var.paths: ["/var/log/suricata/eve.json"]  var.internal\_networks: ["private"]  # Set custom paths for the log files. If left empty,  # Filebeat will choose the paths depending on your OS.  #var.paths: |

- 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  # Paths that should be crawled and fetched. Glob based paths.  paths:  - /var/log/\*.log  #- c:\programdata\elasticsearch\logs\\*  - /var/log/suricata/eve.json  # Filebeat modules  filebeat.config.modules:  # Glob pattern for configuration loading  path: ${path.config}/modules.d/\*.yml  # 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"] |

- Sau cấu hình trên, Logs từ Suricata sẽ được đẩy về Filebeat, rồi từ Filebeat sẽ đẩy qua máy ELK

# 3. Kiểm tra Logs trên Kibana

## 3.1. Giả lập tấn công brute force ssh từ Kali vào máy Suricata

A black screen with white text

AI-generated content may be incorrect.

## 3.2. Kiểm tra

- Ta thấy bên phía Suricata đã hiện Alert cuộc tấn công lên (Theo rule tự viết):

A black and white screen

AI-generated content may be incorrect.

- Bên phía Kibana đã hiện logs được parser thành công:

A screenshot of a computer

AI-generated content may be incorrect.

## 3.3. Các tấn công khác

- Tương tự với các cuộc tấn công khác:

+ Tấn công UDP Flood:

A screen shot of a computer

AI-generated content may be incorrect.

A close-up of a message

AI-generated content may be incorrect.

+ Ping liên tục 1 triệu gói ICMP trong 5 micro giây:

A computer screen with white text

AI-generated content may be incorrect.

A screenshot of a message

AI-generated content may be incorrect.

+ Tấn công chèn lệnh qua kênh mã hóa:

A screenshot of a computer program

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

# 4. Kibana Rule Detection và MITRE ATT&CK

- Dựa vào chữ ký rule (alert.signature\_id) của những log của Suricata được đẩy về, ta tiến hành lọc và viết bộ Rule cho Kibana, đồng thời ánh xạ vào các kỹ thuật trong MITRE ATT&CK để biết được kẻ tấn công đang ở giai đoạn nào:

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

- Sau đó, tiến hành enable Rule lên, các lần tấn công sau, hệ thống sẽ tự động alert lên:

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.