

# Détection et Visualisation des Scans Furtifs

Syrine Ben Ali  
Imen Ouled Belgacem  
École Polytechnique de Sousse

12 mai 2025

## 1 Introduction

La cybersécurité offensive et défensive constitue aujourd’hui un enjeu central dans la protection des infrastructures critiques. Ce projet s’inscrit dans un contexte pédagogique simulant un environnement Red Team vs Blue Team. L’objectif est double : d’une part, mener des attaques furtives ciblées (Red Team), et d’autre part, détecter et analyser ces activités à l’aide de Suricata (Blue Team).

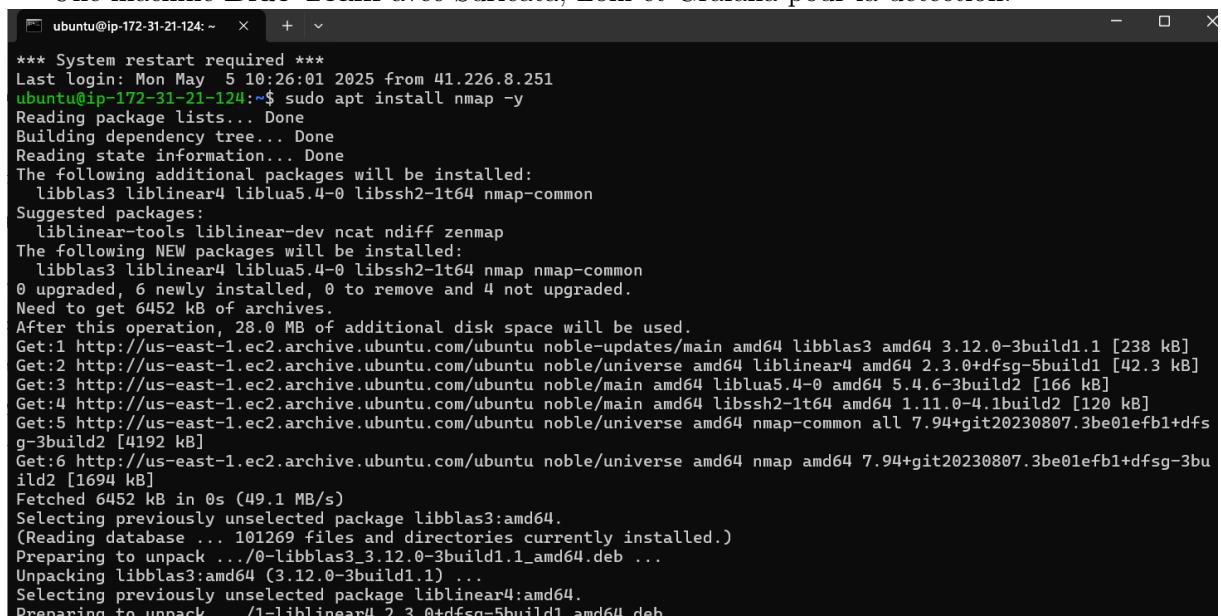
Dans le cadre de ce projet, des techniques de scan furtif comme le NULL scan, le FIN scan ou le XMAS scan ont été utilisées pour contourner les systèmes de détection classiques. Côté défense, nous avons mis en place un IDS basé sur Suricata pour détecter ces tentatives, et intégré une solution moderne de visualisation des alertes via la stack Grafana + Loki, permettant une lecture claire et graphique des événements de sécurité.

Ce rapport présente notre démarche complète, les configurations appliquées, les règles Suricata personnalisées, les scripts de remédiation, et les captures illustrant le fonctionnement de la solution.

## 2 Architecture du projet

Déploiement sur deux instances EC2 AWS :

- Une machine **Red Team** pour générer les attaques.
- Une machine **Blue Team** avec Suricata, Loki et Grafana pour la détection.



```
ubuntu@ip-172-31-21-124:~ + ~
*** System restart required ***
Last login: Mon May  5 10:26:01 2025 from 41.226.8.251
ubuntu@ip-172-31-21-124:~$ sudo apt install nmap
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  libblas3 liblinear4 liblulu5.4-0 libssh2-1t64 nmap-common
Suggested packages:
  liblinear-tools liblinear-dev ncat ndiff zenmap
The following NEW packages will be installed:
  libblas3 liblinear4 liblulu5.4-0 libssh2-1t64 nmap nmap-common
0 upgraded, 6 newly installed, 0 to remove and 4 not upgraded.
Need to get 6452 kB of archives.
After this operation, 28.0 MB of additional disk space will be used.
Get:1 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-updates/main amd64 libblas3 amd64 3.12.0-3build1.1 [238 kB]
Get:2 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/universe amd64 liblinear4 amd64 2.3.0+dfsg-5build1 [42.3 kB]
Get:3 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/main amd64 liblulu5.4-0 amd64 5.4.6-3build2 [166 kB]
Get:4 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/main amd64 libssh2-1t64 amd64 1.11.0-4.1build2 [120 kB]
Get:5 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/universe amd64 nmap-common all 7.94+git20230807.3be01efb1+dfsg-3build2 [4192 kB]
Get:6 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/universe amd64 nmap amd64 7.94+git20230807.3be01efb1+dfsg-3build2 [1694 kB]
Fetched 6452 kB in 0s (49.1 MB/s)
Selecting previously unselected package libblas3:amd64.
(Reading database ... 101269 files and directories currently installed.)
Preparing to unpack .../0-libblas3_3.12.0-3build1.1_amd64.deb ...
Unpacking libblas3:amd64 (3.12.0-3build1.1) ...
Selecting previously unselected package liblinear4:amd64.
Preparing to unpack .../1-liblinear4_2.3.0+dfsg-5build1_amd64.deb ...
```

```
ubuntu@ip-172-31-21-124:~$ sudo nmap -sX -p 22,80,443 52.87.188.194
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-05-05 11:15 UTC
Nmap scan report for ec2-52-87-188-194.compute-1.amazonaws.com (52.87.188.194)
Host is up (0.0020s latency).

PORT      STATE            SERVICE
22/tcp    open|filtered  ssh
80/tcp    open|filtered  http
443/tcp   open|filtered  https

Nmap done: 1 IP address (1 host up) scanned in 1.28 seconds
ubuntu@ip-172-31-21-124:~$ |
```

EC2 > Groupes de sécurité > sg-0fd837b822b53cf6 - launch-wizard-18 > Modifier les règles entrantes

ID de la règle ou du groupe de sécurité	Type	Informations	Filtrage	Règle de ports	Source	Informations	Description	Éditer	Informations
sgr-0f2d1d711bc768af	Tous les TCP		TCP	0 - 65535	N'importe...	<input type="text"/>	<input type="button"/>	<input type="button"/>	<input type="button"/>
sgr-0b0afa21dfac668fd	UDP personnalisé		UDP	1 - 65535	Personn...	<input type="text"/>	<input type="button"/>	<input type="button"/>	<input type="button"/>
sgr-0e3b652e8cb1b5d14	HTTP		TCP	80	Personn...	<input type="text"/>	<input type="button"/>	<input type="button"/>	<input type="button"/>
sgr-091d419c41497c3c	TCP personnalisé		TCP	3000	Personn...	<input type="text"/>	<input type="button"/>	<input type="button"/>	<input type="button"/>
sgr-0af428665fb2ecae	Tous les ICMP - IPv4		ICMP	Tous	Personn...	<input type="text"/>	<input type="button"/>	Pour les ping, tests de connectiv	<input type="button"/>
sgr-0153295af9e595a42	SSH		TCP	22	Personn...	<input type="text"/>	<input type="button"/>	<input type="button"/>	<input type="button"/>
sgr-0b81273c55d99d4d6	HTTPS		TCP	443	Personn...	<input type="text"/>	<input type="button"/>	<input type="button"/>	<input type="button"/>
sgr-00aa84794e90d4bc8	TCP personnalisé		TCP	3100	Personn...	<input type="text"/>	<input type="button"/>	<input type="button"/>	<input type="button"/>
sgr-0e9bea6e8a86d2c1e	TCP personnalisé		TCP	9200	Personn...	<input type="text"/>	<input type="button"/>	<input type="button"/>	<input type="button"/>

### 3 Étapes de l'attaque (Red Team)

- Scan classique : `nmap -sS IP-Blueteam`
- Scans furtifs :
  - `nmap -sN IP`
  - `nmap -sF IP`
  - `nmap -sX IP`
- Accès au serveur HTTP : `curl http://IP-Blueteam`

```
ubuntu@ip-172-31-21-124:~$ sudo nmap -sS 52.87.188.194
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-05-05 10:56 UTC
Nmap scan report for ec2-52-87-188-194.compute-1.amazonaws.com (52.87.188.194)
Host is up (0.0015s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE            SERVICE
22/tcp    open             ssh
25/tcp    filtered        smtp
80/tcp    open             http

ubuntu@ip-172-31-21-124:~$ |
```

```
ubuntu@ip-172-31-21-124:~$ sudo nmap -sN -p 80,443,22 52.87.188.194
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-05-05 11:07 UTC
Nmap scan report for ec2-52-87-188-194.compute-1.amazonaws.com (52.87.188.194)
Host is up (0.0017s latency).
```

```
PORT      STATE            SERVICE
22/tcp    open|filtered  ssh
80/tcp    open|filtered  http
443/tcp   open|filtered  https
```

```
Nmap done: 1 IP address (1 host up) scanned in 1.28 seconds
ubuntu@ip-172-31-21-124:~$ |
```

```

ubuntu@ip-172-31-21-124:~$ sudo nmap -sF -p 22,80,443 52.87.188.194
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-05-05 11:14 UTC
Nmap scan report for ec2-52-87-188-194.compute-1.amazonaws.com (52.87.188.194)
Host is up (0.0020s latency).

PORT      STATE      SERVICE
22/tcp    open|filtered ssh
80/tcp    open|filtered http
443/tcp   open|filtered https

Nmap done: 1 IP address (1 host up) scanned in 1.42 seconds
ubuntu@ip-172-31-21-124:~$ 

ubuntu@ip-172-31-21-124:~$ sudo nmap -sX -p 22,80,443 52.87.188.194
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-05-05 11:15 UTC
Nmap scan report for ec2-52-87-188-194.compute-1.amazonaws.com (52.87.188.194)
Host is up (0.0020s latency).

PORT      STATE      SERVICE
22/tcp    open|filtered ssh
80/tcp    open|filtered http
443/tcp   open|filtered https

Nmap done: 1 IP address (1 host up) scanned in 1.28 seconds
ubuntu@ip-172-31-21-124:~$ |

```

### 3.1 Comparaison des scans furtifs

Les scans furtifs visent à contourner les systèmes de détection classiques (IDS/IPS) en utilisant des combinaisons de drapeaux TCP inhabituelles. Voici une brève comparaison :

- **NULL Scan** : envoie des paquets sans aucun drapeau TCP. Il repose sur le comportement anormal attendu des hôtes. Il est souvent détectable.
- **FIN Scan** : envoie des paquets avec uniquement le drapeau FIN. S'appuie sur la manière dont les systèmes TCP réagissent aux connexions inexistantes.
- **XMAS Scan** : active plusieurs drapeaux TCP (FIN, URG, PSH), comme un arbre de Noël « allumé ». Très caractéristique, il est plus facilement repérable par les IDS modernes.
- **SYN Scan (semi-ouvert)** : utilise le mécanisme classique du 3-way handshake pour repérer les ports ouverts sans établir la connexion complète. Moins furtif mais très courant.

Ces méthodes sont efficaces contre certaines cibles mal configurées, mais peuvent être détectées avec des règles Suricata bien ajustées.

## 4 Détection (Blue Team)

- Installation et configuration de Suricata
- Écriture de règles personnalisées pour détecter :
  - NULL scan
  - FIN scan
  - XMAS scan
  - Ping ICMP
  - Connexions HTTP
- Exemple de règle Suricata :
 

```
alert tcp any any -> any any (flags: F; msg:"Scan FIN détecté"; sid:1000002; rev:1;)
```

```

ubuntu@ip-172-31-46-240: ~ + ▾
GNU nano 7.2 /var/lib/suricata/rules/stealth-scans.rules
# Détection scan NULL (aucun flag TCP)
alert tcp any any -> any any (flags: 0; msg:"⚠ Scan NULL détecté"; sid:1000001; rev:1;)

# Détection scan FIN (flag FIN uniquement)
alert tcp any any -> any any (flags: F; msg:"⚠ Scan FIN détecté"; sid:1000002; rev:1;)

# Détection scan XMAS (flags FIN, PSH, URG)
alert tcp any any -> any any (flags: FPU; msg:"⚠ Scan XMAS détecté"; sid:1000003; rev:1;)

# Détection scan SYN (flags S)
alert tcp any any -> any any (flags:S; msg:"⚠ Scan SYN Nmap détecté"; sid:1000005; rev:1;)

# Détection ping
alert icmp any any -> any any (msg:"⚠ ICMP Ping détecté"; itype:8; sid:1000004; rev:1;)

# Détection Http
alert http any any -> any any (msg:"🌐 Accès HTTP détecté (Port 80)"; sid:1000006; rev:1;)

ubuntu@ip-172-31-46-240:~$ sudo systemctl restart suricata
ubuntu@ip-172-31-46-240:~$ sudo tail -f /var/log/suricata/fast.log
05/05/2025-12:58:56 925156 [**] [1:1000005:1] Scan SYN Nmap détecté [*] [Classification: Misc activity] [Priority: 3] [TCP] 54.210.181.89:8 -> 172.31.46.240:8
05/05/2025-12:58:56 719165 [**] [1:1000005:1] Scan SYN Nmap détecté [*] [Classification: (null)] [Priority: 3] [TCP] 209.38.136.79:49569 -> 172.31.46.240:22
05/05/2025-12:58:18 789638 [**] [1:1000005:1] Scan SYN Nmap détecté [*] [Classification: (null)] [Priority: 3] [TCP] 54.210.181.89:49138 -> 172.31.46.240:88
05/05/2025-12:58:30 884701 [**] [1:1000005:1] Scan SYN Nmap détecté [*] [Classification: (null)] [Priority: 3] [TCP] 51.158.205.97:61000 -> 172.31.46.240:443
05/05/2025-12:57:01 454887 [**] [1:1000005:1] Scan SYN Nmap détecté [*] [Classification: (null)] [Priority: 3] [TCP] 54.210.181.89:40070 -> 172.31.46.240:443
05/05/2025-12:57:09 618838 [**] [1:1000005:1] Scan SYN Nmap détecté [*] [Classification: (null)] [Priority: 3] [TCP] 172.31.46.240:60382 -> 169.254.169.254:89
05/05/2025-12:57:09 023898 [**] [1:1000005:1] Scan SYN Nmap détecté [*] [Classification: (null)] [Priority: 3] {TCP} 172.31.46.240:47300 -> 67.220.243.234:443
05/05/2025-12:57:25 466961 [**] [1:1000004:1] ICMP Ping détecté [*] [Classification: (null)] [Priority: 3] {ICMP} 195.169.125.251:8 -> 172.31.46.240:8
05/05/2025-12:58:24 434777 [**] [1:1000005:1] Scan SYN Nmap détecté [*] [Classification: (null)] [Priority: 3] {TCP} 172.31.46.240:80 -> 172.31.46.240:80
05/05/2025-12:58:39 930248 [**] [1:1000004:1] ICMP Ping détecté [*] [Classification: (null)] [Priority: 3] {ICMP} 129.82.138.44:8 -> 172.31.46.240:8
05/05/2025-12:59:26 671367 [**] [1:1000005:1] Scan SYN Nmap détecté [*] [Classification: (null)] [Priority: 3] {TCP} 54.210.181.89:59962 -> 172.31.46.240:80
05/05/2025-12:59:28 668823 [**] [1:1000006:1] Accès HTTP détecté (Port 80) [*] [Classification: (null)] [Priority: 3] {TCP} 172.31.46.240:80 -> 54.210.181.89:59962
05/05/2025-12:59:28 669833 [**] [1:1000006:1] Accès HTTP détecté (Port 80) [*] [Classification: (null)] [Priority: 3] {TCP} 172.31.46.240:80 -> 54.210.181.89:59962
05/05/2025-12:59:28 669846 [**] [1:1000006:1] Accès HTTP détecté (Port 80) [*] [Classification: (null)] [Priority: 3] {TCP} 172.31.46.240:80 -> 54.210.181.89:59962
05/05/2025-12:59:28 669848 [**] [1:1000006:1] Accès HTTP détecté (Port 80) [*] [Classification: (null)] [Priority: 3] {TCP} 172.31.46.240:80 -> 54.210.181.89:59962
05/05/2025-12:59:28 670319 [**] [1:1000006:1] Accès HTTP détecté (Port 80) [*] [Classification: (null)] [Priority: 3] {TCP} 54.210.181.89:59962 -> 172.31.46.240:80
05/05/2025-12:59:28 670325 [**] [1:1000006:1] Accès HTTP détecté (Port 80) [*] [Classification: (null)] [Priority: 3] {TCP} 54.210.181.89:59962 -> 172.31.46.240:80
05/05/2025-12:59:28 670388 [**] [1:1000006:1] Accès HTTP détecté (Port 80) [*] [Classification: (null)] [Priority: 3] {TCP} 172.31.46.240:80 -> 54.210.181.89:59962
05/05/2025-12:59:28 671317 [**] [1:1000006:1] Accès HTTP détecté (Port 80) [*] [Classification: (null)] [Priority: 3] {TCP} 54.210.181.89:59962 -> 172.31.46.240:80

```

## 5 Visualisation avec Grafana + Loki

- Les logs Suricata sont dirigés vers un fichier JSON (EVE output)
- Promtail est utilisé pour envoyer les logs à Loki
- Grafana récupère les données de Loki et permet de créer des dashboards dynamiques

```

ubuntu@ip-172-31-46-240: ~ + ▾
GNU nano 7.2 /etc/promtail/config.yaml
server:
  http_listen_port: 9080
  grpc_listen_port: 0

positions:
  filename: /tmp/positions.yaml

clients:
  - url: http://localhost:3100/loki/api/v1/push

scrape_configs:
  - job_name: suricata
    static_configs:
      - targets:
        - localhost
    labels:
      job: suricata
      __path__: /var/log/suricata/eve.json

```

The image consists of three vertically stacked screenshots of the Grafana web interface, all taken from a dark-themed browser.

**Screenshot 1: Data Sources - Loki Configuration**

This screenshot shows the "Data sources" configuration page for a "loki" data source. The left sidebar is open, showing "Data sources" as the active section. The main area displays the "Settings" tab for the "loki" connection. The "Name" field is set to "loki" and has a "Default" button next to it. Below the form, a note states: "Before you can use the Loki data source, you must configure it below or in the config file. For detailed instructions, [view the documentation](#)". The "Connection" section shows the URL as "http://localhost:3100". The "Authentication" section indicates "No Authentication".

**Screenshot 2: Dashboards**

This screenshot shows the "Dashboards" management page. The left sidebar shows "Dashboards" as the active section. The main area lists existing dashboards under the heading "Dashboards". A search bar at the top allows filtering by dashboard name or tag. One dashboard named "logs" is visible in the list.

**Screenshot 3: Label browser**

This screenshot shows the "Label browser" feature within a dashboard panel. The left sidebar shows "Dashboards" as the active section. The main area is titled "Label browser" and contains three steps: 1. Select labels to search in (with "filename" and "job" selected). 2. Find values for the selected labels (with "filename (1)" and "job (1)" listed, and a search bar showing "/var/log/suricata/eve.json" and "suricata"). 3. Resulting selector (with an empty input field). At the bottom are buttons for "Show logs", "Show logs rate", "Validate selector", and "Clear".

Grafana

Home > Dashboards > logs > Edit panel

New panel

Table view | Last 5 minutes | Refresh

Queries 1 Transformations 0

Line contains  + Operations

2 <expr> |= 'FIN'  
Return log lines that contain string FIN .  
(job="suricata") |= 'FIN'

Options Type: Range Line limit: 1000 Direction: Backward

Grafana

Home > Dashboards > logs > Edit panel

New panel

Table view | Last 5 minutes | Refresh

Queries 1 Transformations 0

Line contains  + Operations

2 <expr> |= 'XMAS'  
Return log lines that contain string XMAS .  
(job="suricata") |= 'XMAS'

Options Type: Range Line limit: 1000 Direction: Backward

Grafana

Home > Dashboards > logs > Edit panel

New panel

Table view | Last 5 minutes | Refresh

Queries 1 Transformations 0

Line contains  + Operations hint: add json parser

2 <expr> |= 'SYN'  
Return log lines that contain string SYN .  
(job="suricata") |= 'SYN'

Options Type: Range Line limit: 1000 Direction: Backward

## 6 Remédiation et bonnes pratiques

- Blocage des IPs source suspectes (via iptables ou fail2ban)
- Surveillance des logs via des alertes automatisées
- Tests réguliers de détection pour garantir la couverture

## 7 Conclusion

Ce projet a permis de simuler un environnement d'attaque réaliste, d'implémenter une solution de détection active et d'introduire une visualisation professionnelle des événements. L'utilisation de Grafana + Loki permet un suivi visuel efficace, adapté aux environnements de production.

```
304 sudo apt install wget unzip -y
305 wget https://github.com/grafana/loki/releases/download/v2.8.2/loki-linux-amd64.zip
306 unzip loki-linux-amd64.zip
307 sudo mv loki-linux-amd64 /usr/local/bin/loki
308 loki --version
309 ls /etc/loki/
310 sudo mkdir -p /etc/loki
311 sudo nano /etc/loki/config.yaml
312 loki --config.file=/etc/loki/config.yaml
313 loki --version
314 sudo nano /etc/loki/config.yaml
315 loki --config.file=/etc/loki/config.yaml
316 sudo nano /etc/loki/config.yaml
317 loki --config.file=/etc/loki/config.yaml
318 wget https://github.com/grafana/loki/releases/latest/download/promtail-linux-amd64.zip
319 unzip promtail-linux-amd64.zip
320 sudo mv promtail-linux-amd64 /usr/local/bin/promtail
321 chmod +x /usr/local/bin/promtail
322 sudo mkdir -p /etc/promtail
323 sudo nano /etc/promtail/config.yaml
324 promtail --config.file=/etc/promtail/config.yaml
325 sudo apt-get install -y software-properties-common
326 sudo add-apt-repository "deb https://packages.grafana.com/oss/deb stable main"
327 sudo apt-get install -y gnupg2
328 wget -q -O - https://packages.grafana.com/gpg.key | sudo apt-key add -
329 sudo apt-get update
330 sudo apt-get install grafana
331 sudo apt-get install grafana -y
332 sudo apt-get update
333 wget -q -O - https://packages.grafana.com/gpg.key | sudo apt-key add -
334 sudo apt-get install -y gnupg2
335 sudo systemctl start grafana-server
336 sudo systemctl enable grafana-server
337 sudo systemctl status grafana-server
338 loki --config.file=/etc/loki/config.yaml
339 history
ubuntu@ip-172-31-46-240:~$
```