🛡️ Cybersécurité – Déploiement d'un site vulnérable & protection avec Suricata (IDS/IPS)

⚙️ 1. Installation de Suricata

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

🛠️ 2. Configuration en mode `af-packet` (inline)

Modifiez le fichier de configuration :
`/etc/suricata/suricata.yaml`

Repérez (ou ajoutez) la section suivante :

```
af-packet:
  - interface: eth0                # Remplacez par l'interface réseau utilisée (ex : ens33)
    threads: auto
    cluster-id: 99
    cluster-type: cluster_flow
    defrag: yes
    copy-mode: tap                 # Important : doit être "ips" pour activer le blocage !
    use-mmap: yes
    ring-size: 200000

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

rule-files:
  - suricata.rules
```

> 🔎 *Utilisez `ip a` pour identifier la bonne interface réseau.*

📜 3. Création de règles personnalisées

Éditez le fichier : `/etc/suricata/rules/suricata.rules`

✅ 4. Vérification des règles

Testez la validité de la configuration :

```
suricata -T -c /etc/suricata/suricata.yaml -v
```

🚦 5. Démarrage de Suricata

En tant que service :

```
sudo systemctl enable suricata
sudo systemctl restart suricata
```

En mode manuel (inline, `af-packet`) :

```
sudo suricata -c /etc/suricata/suricata.yaml --af-packet
```

📊 6. Vérification des alertes/drops

Surveillez les logs en temps réel :

```
tail -f /var/log/suricata/fast.log
```

Ou plus détaillé (JSON) :

```
tail -f /var/log/suricata/eve.json | jq '. | select(.event_type=="alert" or
.event_type=="drop")'
```