Atelier 4 : OPNsense Next-Gen Firewall IDS/IPS (Suricata)

Coté cours : L'**IDS (Intrusion Detection System)** surveille et analyse le trafic réseau pour détecter des tentatives d'intrusion, tandis que l'**IPS (Intrusion Prevention System)** va plus loin en bloquant ces menaces en temps réel. Ces systèmes sont essentiels pour protéger les réseaux contre les attaques et sont souvent intégrés aux pares-feux de nouvelle génération (NGFW).

Avantages de l'IDS/IPS : L'IDS/IPS détecte les comportements malveillants et bloque les tentatives d'exploitation avant qu'elles n'affectent les systèmes. Il protège aussi bien la périphérie du réseau que les datacenters, empêchant les attaquants de collecter des informations sensibles.

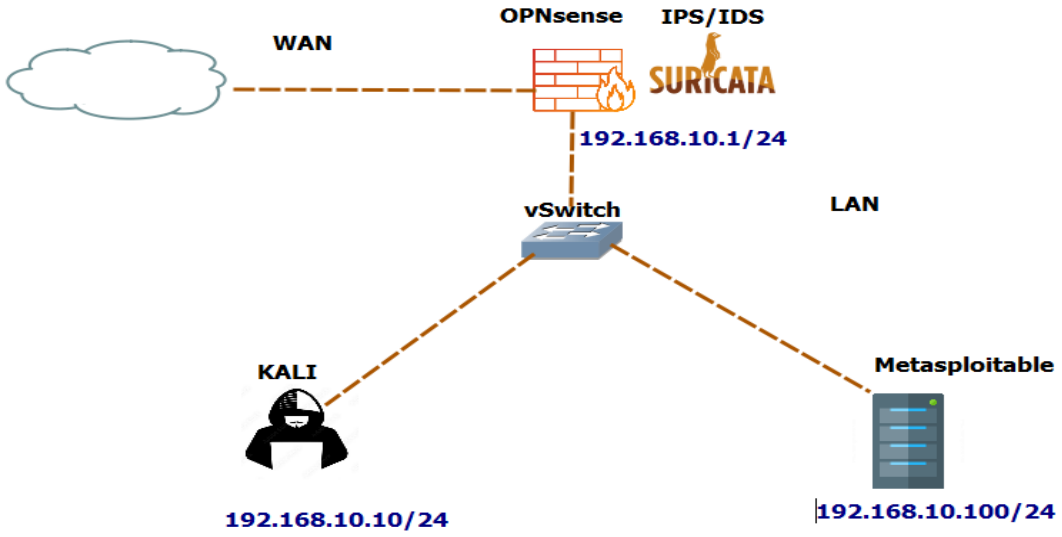
Méthodes de détection IDS

1. **Basée sur les signatures** : compare les événements avec une base de signatures connues.
2. **Basée sur les anomalies** : détecte les écarts par rapport à un comportement réseau normal.
3. **Analyse dynamique des protocoles** : identifie les écarts en comparant les événements aux profils normaux des protocoles.

L'IDS/IPS est une technologie clé pour renforcer la cybersécurité et stopper les menaces avant qu'elles ne causent des dommages.

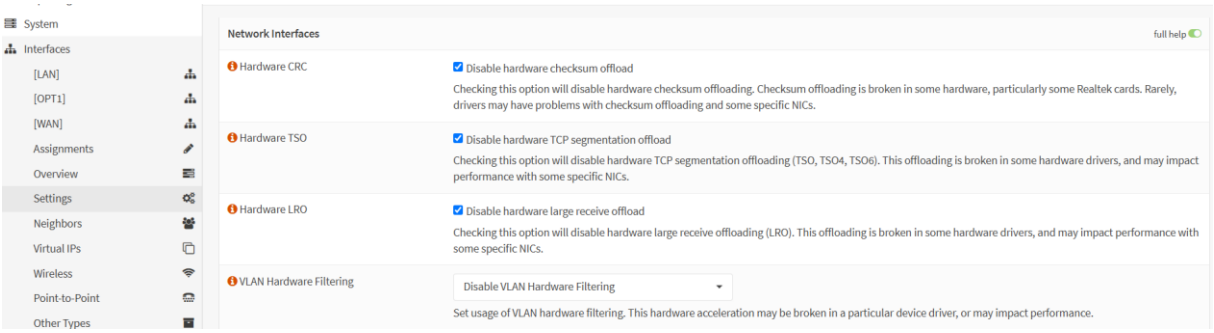
Objectif

Dans cet atelier, vous allez installer et configurer OPNsense, en intégrant Suricata en tant que **système de prévention des intrusions (IPS) / système de détection des intrusions (IDS)**. Vous définissez les règles personnalisées pour que Suricata nous alerte en cas de **scans furtifs** sur notre réseau. Ces scans furtifs seront réalisés à l'aide de **nmap** dans le cadre d'une reconnaissance réseau.



Etape 1 : Installation de notre IPS/IDS

Pour que le **système de prévention/détection des intrusions (IPS/IDS)** fonctionne correctement, vous devez accéder aux paramètres de l'interface et **désactiver les paramètres matériels** (cochez toutes les cases).



Après avoir appliqué les modifications, accédez à **Services > Intrusion Detection > Administration**.

- **Activez le "mode avancé"**.
- **Cochez toutes les cases** suivantes :
    - **Enabled** (Activé)
    - **IPS mode** (Mode IPS)
    - **Promiscuous mode** (Mode promiscuité)
    - **Enable Syslog output** (Activer la sortie Syslog)
    - **Modifiez le "Pattern Matcher"** et sélectionnez **"Hyperscan"** pour une détection plus efficace.
    - **Définissez l'interface sur LAN** : LAN
    - **Indiquez uniquement l'adresse IP du réseau LAN : 192.168.10.0/24**

Etape 2 : Créer une règle personnalisée

Vous allez définir une règle personnalisée via IDS **Suricata** afin qu'il vous alerte en cas de **scans furtifs** potentiels sur votre réseau via nmap. Un **scan furtif** est généralement la première étape de reconnaissance d'un pirate informatique. L'objectif de ce scan est **de recueillir un maximum d'informations sur le système et le réseau**, notamment les ports ouverts ou les services installé ainsi que leurs vesrions.

Créez dans le répertoire **Suricata_rules** le fichier **nmap.rules** en utilisant Notepad par exemple :

```
alert tcp $HOME_NET any -> 192.168.10.1/24 any (msg: ''POSSIBLE NMAP
SYNSTEALTH SCAN DETECTED"; flow:stateless; flags:S; priority:5;
threshold:type threshold, track by_src, count 50, seconds 1;
classtype:attempted-recon; sid:10000001;)
```

Explication de la règle :

Cette règle sera déclenchée lorsque le protocole correspondant est **TCP**. **home_net** sert de **variable représentant notre réseau domestique**.

Cette règle s'applique à **tout trafic TCP provenant du réseau LA N, quel que soit le port d'origine, et se dirigeant vers l'adresse IP de notre pare-feu**. Lorsque cette condition est remplie, un message sera généré indiquant : **"**`POSSIBLE NMAP SYNSTEALTH SCAN DETECTED`**"**.

Remarque 1 : Vous pouvez spécifier que cette règle s'applique à tout le réseau 192.168.10.0/24.

- **alert tcp** : Cette règle génère une **alerte** pour le trafic **TCP**.
- **$HOME_NET any -> 192.168.10.10/24 any** : Cette partie spécifie que la règle s'applique à **tout le trafic TCP** provenant de **n'importe quel port** de votre réseau interne ($HOME_NET), et destiné à l'adresse IP **192.168.10.10/24** sur **n'importe quel port**.
- $HOME_NET est une **variable** représentant votre réseau local dans Suricata.
- **msg: 'POSSIBLE NMAP SYNSTEALTH SCAN DETECTED'** : Ce message s'affichera lorsqu'un scan furtif SYN est détecté. Ce type de scan est souvent utilisé par Nmap pour effectuer une reconnaissance discrète sans établir une connexion complète.
- **flow: stateless** :Cela signifie que la règle s'applique **à chaque paquet individuellement** sans tenir compte de l'état de la connexion. Le scan SYN de Nmap ne complète pas la connexion TCP, donc la détection est basée sur des paquets isolés.
- **flags: S** : La règle cherche des paquets TCP avec le **flag SYN activé** (cela est typique des scans SYN ou furtifs). Ce type de scan envoie des paquets SYN sans établir la connexion complète.
- **priority: 5** : Définit la **priorité** de l'alerte sur une échelle de 1 à 5, où **5** représente une priorité plus élevée.
- **threshold: type threshold, track by_src, count 50, seconds 1** : Cette condition impose un **seuil** pour limiter les alertes :
- **track by_src** : Surveille les paquets par **source**.
- **count 50, seconds 1** : Si **50 paquets** SYN sont envoyés depuis la même source en **1 seconde**, la règle est déclenchée. Cela permet de détecter des scans rapides typiques des attaques de reconnaissance.
- **classtype: attempted-recon** : Cette partie classifie l'alerte comme une tentative de **reconnaissance** (attempted-recon), ce qui correspond à un comportement typique d'un scanner cherchant à récolter des informations sur le réseau.
- **sid: 1000001** : **SID (Signature ID)** est un identifiant unique de la règle. Il est utilisé pour référencer cette règle dans Suricata et est utile pour la gestion des règles et la mise à jour des signatures.

Créer dans le même répertoire Suricata_rules un fichier **XML** nommé nmap.xml :

```
<?xml version="1.0"?>
<ruleset documentation_url="http://docs.opnsense.org/">
    <location url="http://192.168.1.12/" prefix="nmap" />
    <files>
        <file description="nmap rules">nmap.rules</file>
        <file description="nmap" url="inline::rules/nmap.rules">nmap.rules</file>
    </files>
</ruleset>
```

Configurer l'accès à distance sécurisé tout en limitant les accès à l'interface LAN pour des raisons de sécurité.

Vous devez vous rendre dans **"Settings"** puis dans **"Administration"**. Assurez-vous de cocher les cases suivantes :

- **Secure Shell Server** : Activez le serveur SSH pour permettre l'accès distant via SSH.
- **Root Login (For lab only)** : Activez la connexion en tant qu'utilisateur root (pour le laboratoire uniquement, il est recommandé de désactiver cette option en production pour des raisons de sécurité).
- **Authentication Login** : Activez l'authentification pour les connexions SSH.
- **Listening Interfaces** : Sélectionnez **LAN** comme interface d'écoute pour limiter les connexions SSH à l'interface LAN uniquement.

Etape 3 : Installation de la nouvelle règle

Transférer le fichier nmap.xml avec FileZilla dans **/usr/local/opnsense/scripts/suricata/metadata/rules**

Transférer également le fichier nmap.rules dans **/usr/local/etc/suricata/rules**

Dans le même emplacement où vos fichiers sont stockés, vous devrez utiliser Python pour créer un serveur HTTP. Ce serveur sera utilisé pour servir votre fichier .rules à OPNsense lorsque le fichier .xml le demande.

```
python3 -m http.server 80
```

Naviguez vers « Services », « Détection d'intrusion », puis « Administration ». En haut, vous devrez cliquer sur « réinitialiser le service » et vos règles personnalisées devraient apparaître.

Cochez « nmap/nmap rules », cliquez sur « activer les règles sélectionnées », puis sur « Télécharger et mettre à jour les règles ».

Etape 4 : Test et validation

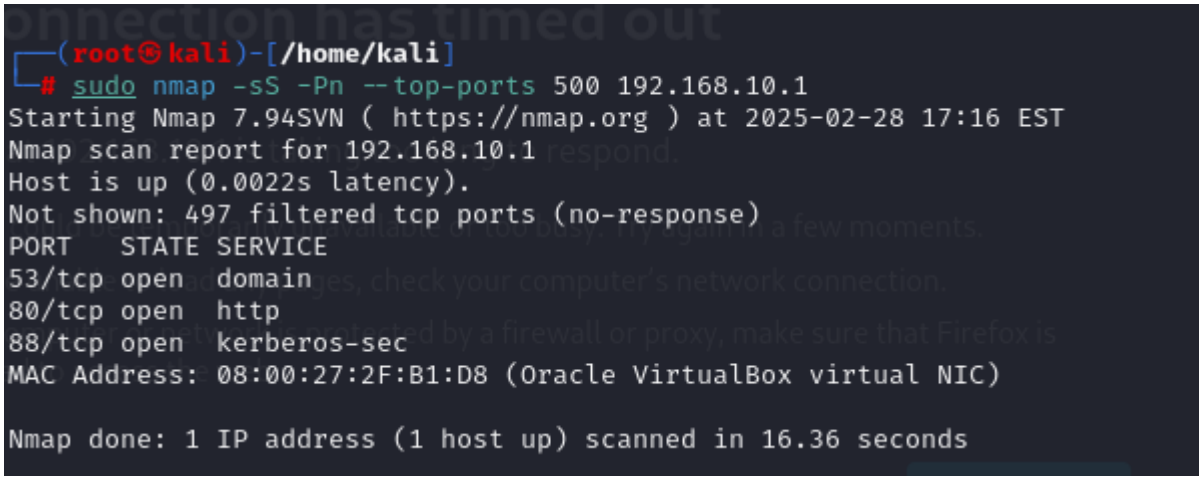
Vous allez tester le fonctionnement de la nouvelle règle c'est-à-dire la validation de votre IDS. Étant donné que vous avez configuré votre règle pour détecter un scan furtif, vous pouvez effectuer un scan et vérifier si vous recevez une alerte concernant cette activité.

Pour démarrer votre scan furtif, vous utiliserez les options suivantes avec **Nmap** :

- **-sS** : Lance un scan SYN (furtif).
- **-Pn** : Continue le scan même si un ping n'est pas répondu.
- **--top-ports 500** : Scanne les 500 premiers ports les plus courants.
- **192.168.1.1** : L'adresse IP de votre pare-feu.

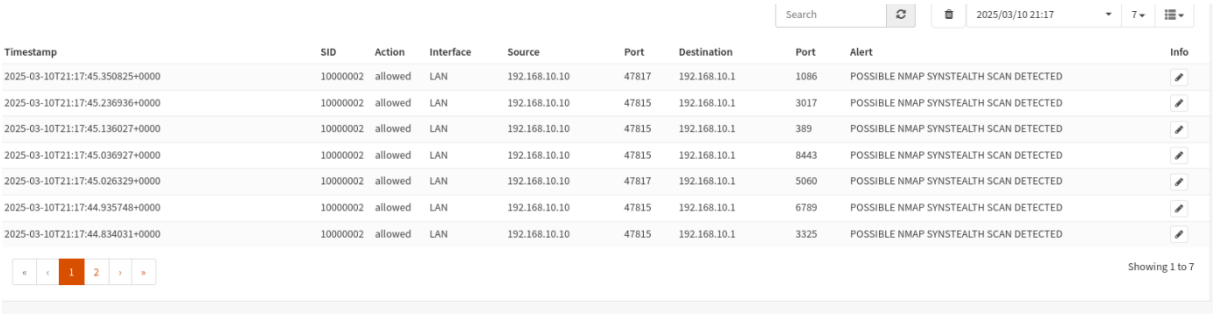
La commande complète sera la suivante :

```
sudo nmap -sS -Pn --top-ports 500 192.168.10.1
```



Les résultats montrent que les ports 22, 53, 80 et 88 sont tous ouverts. Retournez sur votre pare-feu et actualisez la section des alertes.

Vérifiez si une alerte concernant le scan furtif que vous avez effectué est apparue dans la liste des alertes de **Suricata**. Si la configuration a été correcte, vous devriez voir une alerte indiquant qu'un **scan furtif NMAP** a été détecté.



Conclusion