Détection par signature
SNORT

Snort

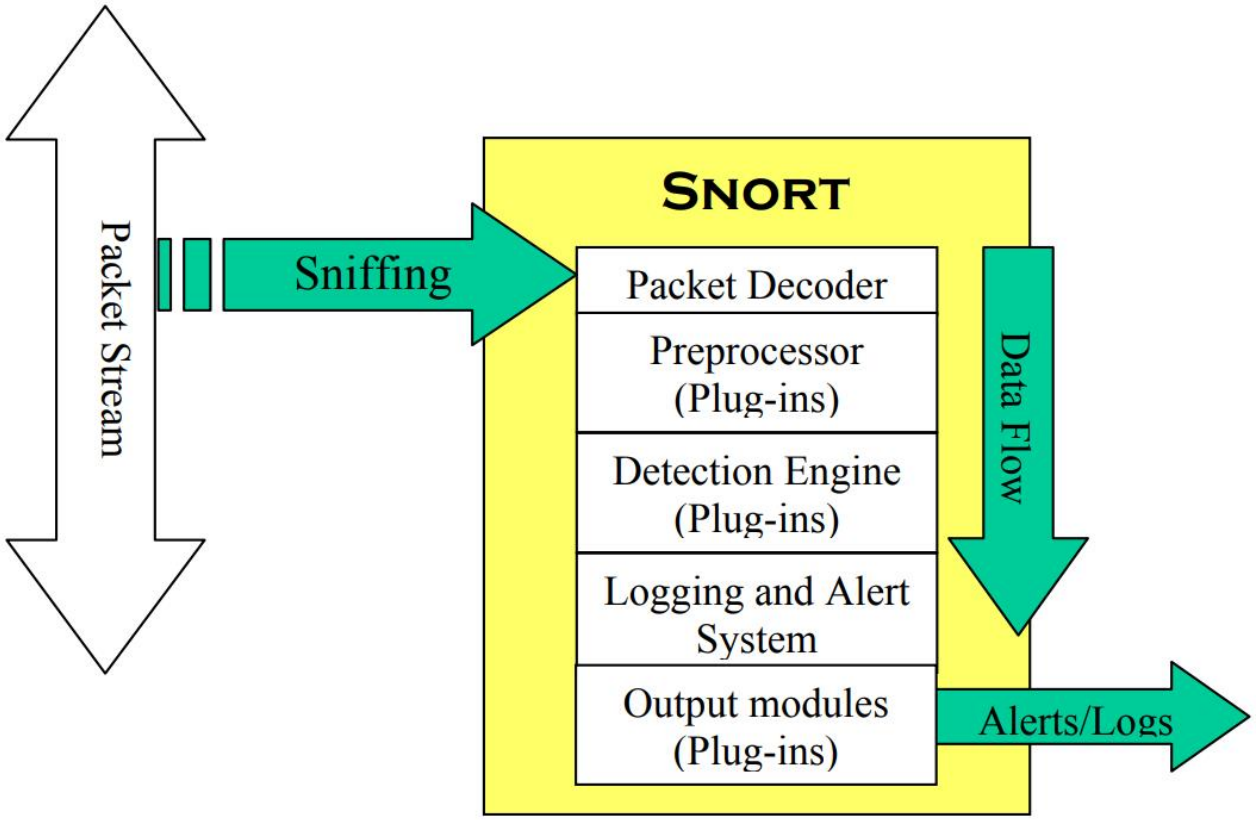
- Snort est un système de détection d'intrusion IDS (Intrusion Detection System) open source.

- Il effectue en temps réel des analyses de trafic et journalise (log) les paquets IP transitant sur son réseau.

- Snort est considéré comme l'un des meilleurs outils de détection d'intrusions sur le marché car il se base sur l'emploi des règles de sécurité qui sont maintenues à jour par une communauté très actives.

- Les modes de fonctionnement de Snort sont en nombre de trois :
    1. sniffer de paquets
    2. logger de paquets
    3. système de détection d'intrusions (IDS)
    4. Système de prévention d'intrusion (IPS)

Architecture



Mode de fonctionnement

Il y a trois composants essentiels dans Snort :

- **Décodeur** : sauvegarde les paquets capturés dans une pile, identifie les protocoles, et décode IP.
- **Les préprocesseurs:** sont des modules d'extension pour arranger ou modifier les paquets de données avant que le moteur de détection n'intervienne.
  - Certains préprocesseurs détectent aussi des anomalies dans les entêtes des paquets et génèrent alors des alertes.
- **Moteur de détection** : analyse les paquets en utilisant les règles chargées préalablement dans la mémoire (lors de la phase d'initialisation de Snort)
- **Plug-ins de sortie** : ces modules servent à formater les notifications pour permettre à l'utilisateur d'y accéder (console, fichiers externes, base de données, etc).

Mode de fonctionnement

- Snort utilise la librairie libpcap (sous Unix/Linux) ou Winpcap (sous Windows), la même librairie que tcpdump utilise pour le reniflement des paquets.
- Snort décode tous les paquets qui passent à travers le medium réseau auquel il est connecté en mode d'écoute « promiscuous mode ».
- En se basant sur le contenu des paquets et les règles définies dans le fichier de configuration, une alerte est levée
- Il y a de nombreuses règles que Snort permet à l'utilisateur d'écrire.
- Une règle doit décrire :
  - Toute violation de la politique de sécurité d'une organisation0
  - Toutes les tentatives populaires et communes qui peuvent exploiter les vulnérabilités du réseau.
  - Les conditions qui permettent d'identifier les paquets suspect ou inusuel, c'est-à-dire, si l'identité du paquet n'est pas authentique.

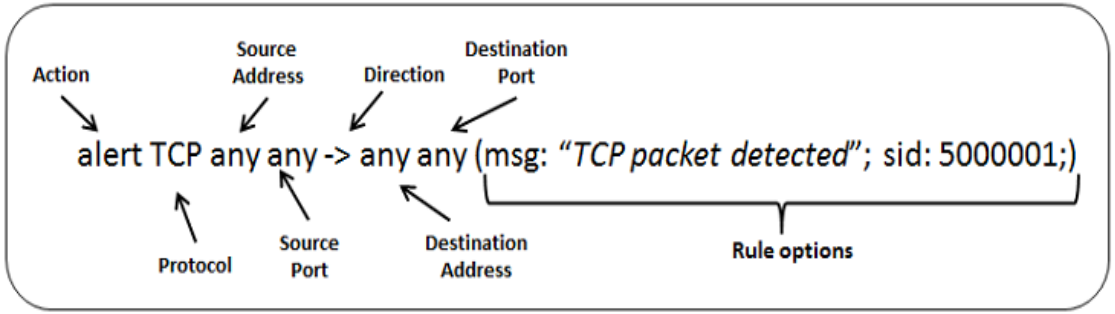
Les règles Snort (signatures)

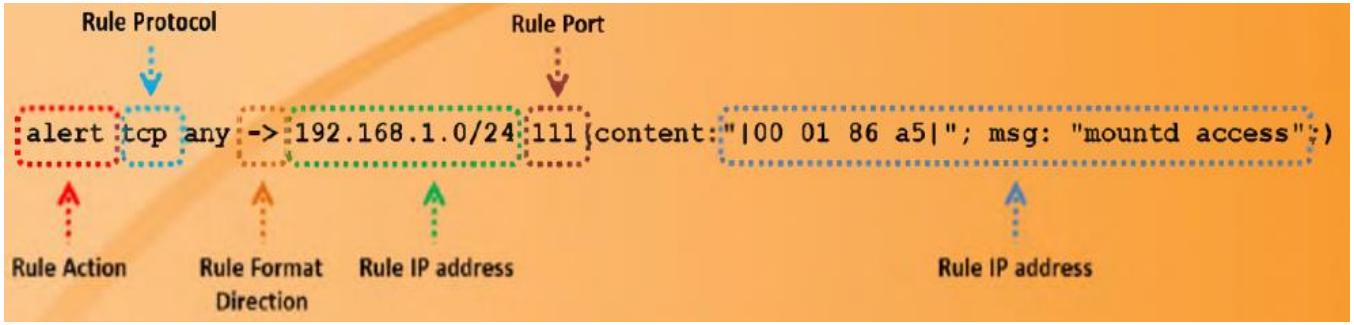
Action	Protocole	Adresse	Port	Direction	Adresse	Port

- **Action**: La partie action de la règle dit à Snort quoi faire quand il trouve un paquet qui correspond aux critères de la règle.
- **Protocole**: La partie protocole est utilisée pour appliquer la règle sur les paquets pour un protocole particulier seulement.
- **Adresse**: Les parties de l'adresse définissent des adresses de source et de destination.
- **Port**: En cas de protocole TCP ou UDP, les parties concernant les ports déterminent les ports source et destination d'un paquet sur lequel la règle est appliquée. En cas de protocoles de couche réseau comme IP et ICMP, les numéros de port sont sans signification.
- **Direction**: La partie de la direction de la règle détermine lesquels des adresses et des numéros de port sont utilisés comme source et lesquels sont utilisés comme destination.

Règles Snort

- Il y a deux principes de base à prendre en considération lors d'écriture des règles, à savoir :
  - Une règle doit être écrite sur une seule ligne, ainsi les règles sont courtes, précises et faciles à comprendre
  - Chaque règle doit contenir deux sections logiques :
    - L'entête
    - Les options (le corps)





Opérateur de direction et adresses IP

- L'opérateur de direction **->** indique l'orientation, ou la direction du trafic auquel s'applique la règle.
- L'adresse IP et le numéro de port à la gauche de l'opérateur concernent la source du trafic, ceux de droite concernent la destination du trafic.
- Il existe aussi l'opérateur bidirectionnel **<->**, qui est pratique pour l'enregistrement et l'analyse du trafic dans les deux sens, tels que dans le cas des sessions telnet et POP3.
- Une règle peut spécifier une liste d'adresse IP, qui doivent être séparées par des virgules et mises entre guillemets, comme ça : [192.168.1.1,192.168.1.45,10.1.1.24].
- Il est aussi possible de spécifier une plage d'adresse IP à l'aide de masque CIDR.

Opérateur de direction et adresses IP

Protocols	IP address	Action
Log UDP any any ->	92.168.1.0/24 1:1024	Log UDP traffic coming from any port and destination ports ranging from 1 to 1024
Log TCP any any ->	192.168.1.0/24 :5000	Log TCP traffic from any port going to ports less than or equal to 5000
Log TCP any :1024 ->	192.168.1.0/24 400:	Log TCP traffic from privileged ports less than or equal to 1024 going to ports greater than or equal to 400

Numéros de port

- Les numéros de port peuvent être spécifiés de différentes façons, comprenant : n'importe quel port, définition de ports statiques, plage, négation.

- N'importe quel port « any » est une valeur primitive, qui ne met pas de restriction sur le numéro de port.

- Port statique indique un seul numéro de port.

- Plage de port est spécifié à l'aide de l'opérateur «:».

- **Exemple**: négation de port

log tcp any any - > 192.168.1.0 /24 ! 6000 : 6010

Les options d'une règle Snort

- Les options d'une règle Snort se trouvent dans les parenthèses contenues dans la règle Snort.
- Toutes les options de règle de Snort sont séparées les unes des autres par le caractère point-virgule ";".
- Elles suivent généralement un format ayant un mot-clé dans la liste *(ACK, CLASSTYPE, CONTENT, OFFSET,etc)* suivie par argument.
- Les mots clés des options de règle sont séparés de leurs arguments avec le caractère deux points ":".

Les alertes de Snort

Snort a une variété de modes d'alerte, qui sont tous détaillés ci-dessous:

- **Fast Mode (“-A fast”)** – Ce mode rapporte Timestamp, Alerte message, les adresses IP source et destination, et les ports source et destination. Le paquet actuel n’est pas journalisé en utilisant ce mode.

- **Full Mode (“-A full”)** – Ce mode rapporte les mêmes informations que dans le mode rapide (Fast Mode), mais il comprend également l'en-tête du paquet.

- **UNIX Socket Mode (“-A unsock”)** – Ce mode permet à un administrateur système d’envoyer des alertes à d'autres programmes en utilisant un socket UNIX.

- **Alerts to Syslog (“-s”)** – Ce mode permet de stocker l'alerte dans le Syslog, qui est l'endroit où les événements au niveau du système sont enregistrées.

- **SNMP Mode** – Les alertes peuvent également être envoyées sous forme de messages SNMP, où les systèmes de gestion de réseau peuvent aider les administrateurs système à identifier et corriger le problème.

Actions et protocoles IP

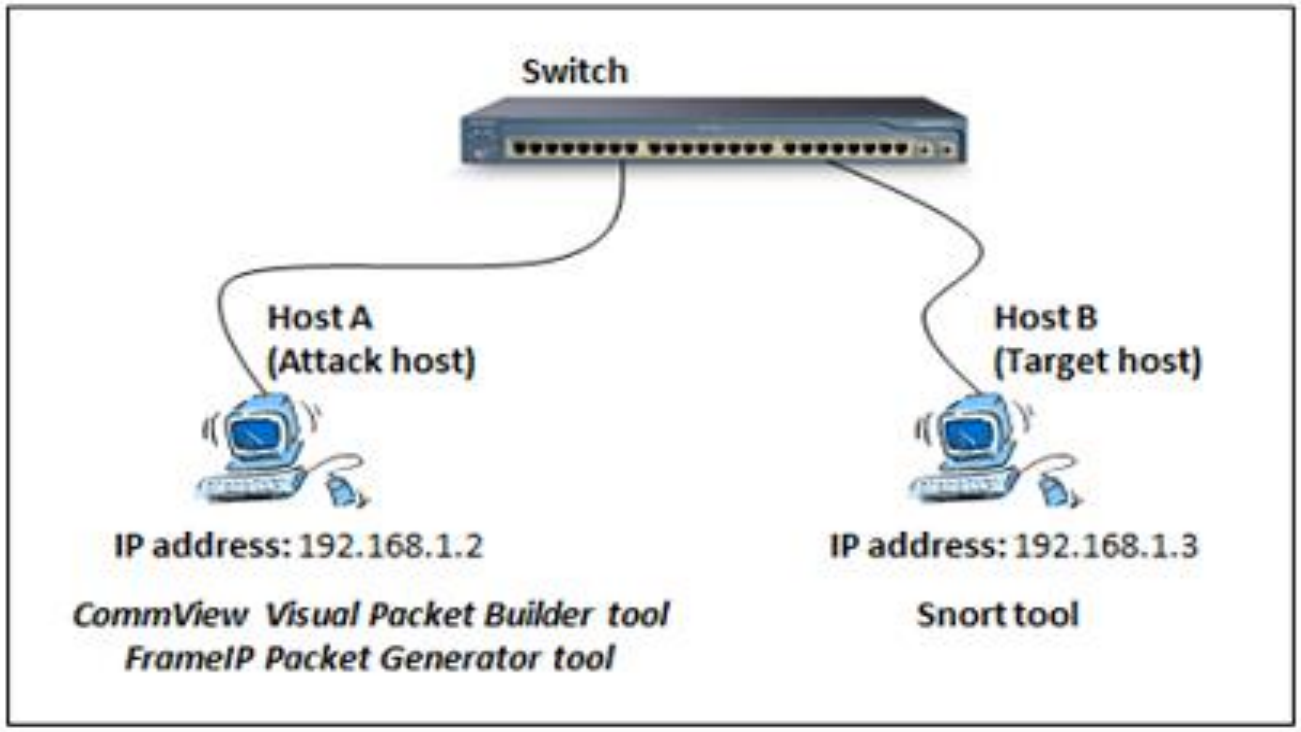
- Il y a cinq actions par défaut : **alert, log, pass, activate, and dynamic**.
- En plus, si Snort est exécuté en mode inline (IPS), il y a d'autres actions telles que **drop** et **reject**.

  - **Alert**: genérer une alerte et journaliser le paquet
  - **Log** : journaliser le paquet
  - **Pass** : ignorer le paquet
  - **Activate** : alerter et ensuite activer une autre règle dynamique
  - **Dynamic** : rester inactive jusqu'à l'activation par une autre règle , ensuite agir en tant que règle log
  - **Drop** : bloquer et journaliser le paquet
  - **Reject** : bloquer le paquet, le journaliser, et ensuite envoyer un TCP reset s'il s'agit de protocole TCP, ou un ICMP port inaccessible s'il s'agit du protocole UDP.
  - **Sdrop** : bloquer le paquet mais ne pas le journaliser

TP1: Installation et configuration

- **Installation:**
  - apt-get update
  - apt-get install snort
- **Vérification:**
  - snort –v
- **Démarrer Snort:**
  - snort -i enp0s3 -c /etc/snort/snort.conf -A console
  - -i: pour indiquer le nom de interface reseau à utiliser pour écouter le trafic
  - -A: Indique à Snort d’ Envoyer des alertes "Fast-style" vers la
  - console (écran)
- **Tester le fonctionnement pour le protocole ICMP**:
  - Ajouter une règle dans /etc/snort/rules/local.rules qui permet de lever une alerte dès la détection d’un paquet qui contient des données ICMP

TP2: Détection DoS à l'aide de Snort



Exemple: Le TCP XMAS scan

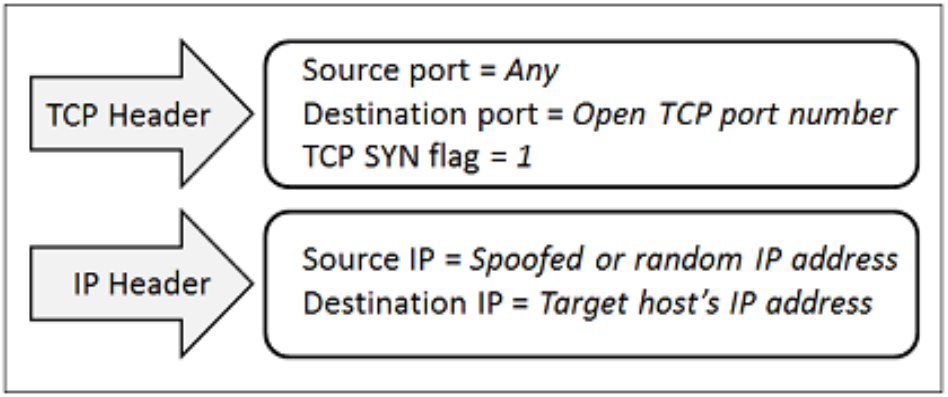
- Envoyer des paquets TCP avec les **flags URG, PUSH et FIN à 1** dans le but de déjouer certains pare-feu ou mécanismes de filtrage.
- **Génération**:
  - Nmap: nmap –sX @IP Victime
- Signature Snort:
  - #alert tcp any any -> $HOME_NET any (msg:"Full XMAS Scan"; flags: SRAFPU;sid:9000004;)alert tcp any any -> $HOME_NET any (msg:"=====Full XMAS Scan====="; flags: FPU;sid:9000004;)

Exemple: TCP Null scan

- À l'inverse du TCP XMAS scan, le **TCP Null scan** va envoyer des paquets TCP scan avec tous les flags à 0.
- Il s'agit là aussi d'un comportement que l'on ne trouvera jamais dans un échange normal entre des machines
- L'utilisation de ce scan peut, comme le TCP XMAS scan, perturber certains firewalls ou modules de filtrage et alors laisser passer les paquets :

Attaque SYN Flood: Description

- Dans ce cas l'hôte victime devient tellement submergé par les paquets TCP SYN qui initient des connexions incomplètes, qu'il ne pourra plus traiter les demandes de connexion légitimes.
- L'attaquant envoie un message TCP SYN avec une adresse IP source falsifiée. Par conséquent, la victime ne recevra jamais le message d'acquittement.
- Inonder le serveur avec des TCP SYN falsifiées causera un déni de service.



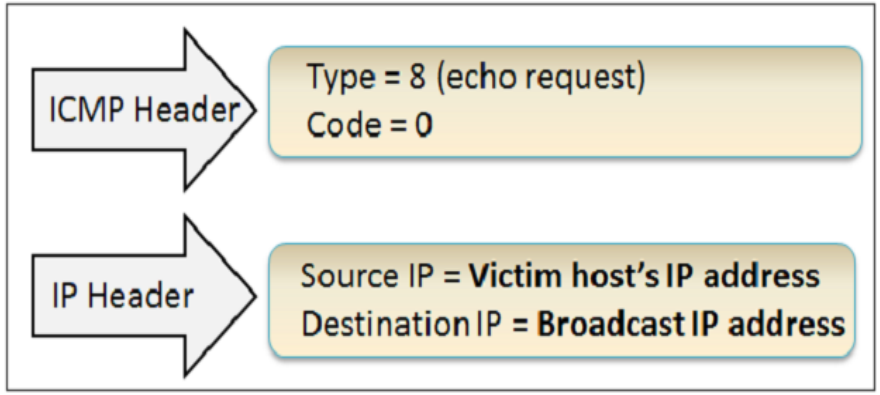
Attaque SYN Flood: Génération & détection

- **Génération: Metasploit**
  - use auxiliary/dos/tcp/synflood
  - set RHOST adresse IP de la machine victime
- **Règle**

  alert tcp any any -> 192.168.1.3 any (msg:"TCP SYN flood attack detected"; flags:S; threshold: type threshold, track by_dst, count 20 , seconds 60; sid: 5000001; rev:1;)
  - **Threshold**: signifie que cette règle journalise chaque 20 évènements pendant un intervalle de 60 secondes.
  - **Track by_dst**: traquer par addressee de destination
  - **count**: permet de compter le nombre d'evements

Attaque Smurf: description

- Cette attaque consiste à transmettre un grand nombre de requêtes ICMP echo (ping) à l'adresse de diffusion.
- Toutes les requêtes utilisent l'adresse de l'hôte victime comme adresse source.
- Tout hôte dans le réseau représenté par cette adresse de diffusion répondra à la requête et enverra un message réponse ICMP echo à l'hôte victime.



Attaque Smurf: Génération & détection

- **Génération**

hping3 -1 --flood -a @victime @diffusion

hping3 -1 --flood -a 192.168.1.5 192.168.1.255

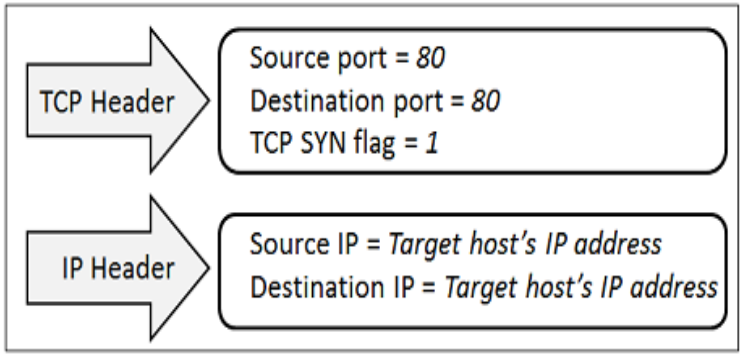
- **Règle de détection**

alert icmp 192.168.1.X any -> 192.168.1.0/24 any (msg:"Smurf attack detected"; itype:8; sid:5000002; rev:1;)

  - ***itype*** est utilisé pour vérifier le type du paquet ICMP.

Attaque Land: Description

- L'attaquant transmit une demande de connexion TCP SYN avec l'adresse IP et le port de la machine victime en tant que source et destination. Ce qui va mener la machine victime à répondre à lui-même de façon continue.
- La machine victime répond à elle-même par un paquet SYN-ACK, créant ainsi une connexion vide qui durera pendant un intervalle de temps (idle timeout). Innoder le système avec de telles connexions peut submerger le système, causant ainsi une situation de deni de service.



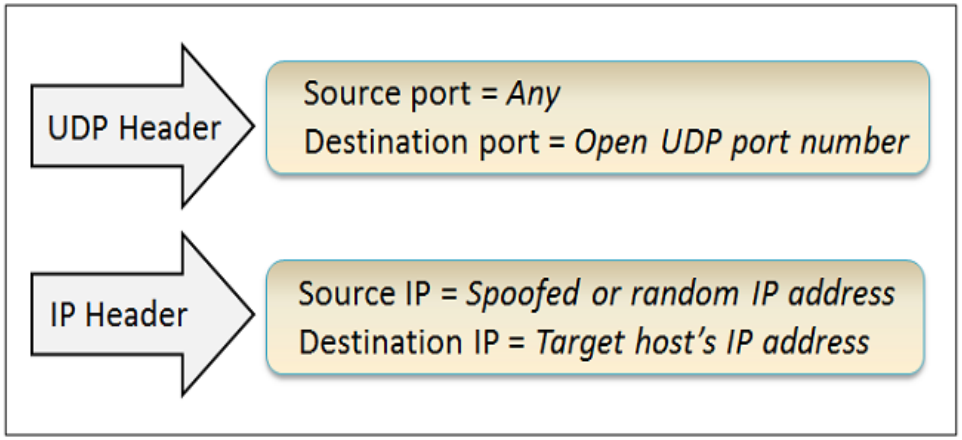
Attaque Land: Règle de détection

alert tcp any any -> any any (msg: "Land attack detected"; flags:S; sameip; sid: 5000000; rev:1;)

- **flags** : TCP SYN
- **Same ip**: mot clé qui permet de verifier si l'adresse source et destination sont similaires.
- **sid**: permet d'identifier de façon unique une règle
- **rev**: permet d'identifier de façon une révision d'une règle

UDP Flood: Description

- Consiste à inonder les ports UDP cibles de l'hôte victime avec des paquets UDP.
- Si suffisamment de paquets UDP sont envoyés au port UDP destination, l'hôte victime ou l'application UDP peut ralentir ou cracher.



UDP Flood: Génération & Détection

- **Génération**

- **Règle de détection**

alert udp any any -> 192.168.1.3 any (msg:"UDP flood attack detected"; threshold: type threshold, track by_dst, count 10 , seconds 60 ; sid: 5000003; rev:1;)