Syn flood

Une attaque **SYN flood** (attaque semi-ouverte) est un type d’attaque par déni de service (DDoS) qui vise à rendre un serveur indisponible pour le trafic légitime en consommant toutes les ressources serveur disponibles.

Progression of a SYN flood.

Three-way handshake

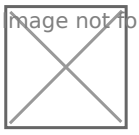
L’attaque **SYN Flood** exploite le principe du **three-way handshake** du protocole **TCP**.

Lors d’une connexion classique entre un **client** et un **serveur** il y a 3 étapes :

Le client envoie un paquet **SYN**.

Le serveur répond ensuite avec un paquet **SYN-ACK** accusant la réception.

Le client envoie un paquet **ACK** et la connexion **TCP** est donc établie.



Déroulement de l’attaque

En envoyant à plusieurs reprises des paquets de demande de connexion initiale (**SYN**), l’attaquant est en mesure de submerger tous les ports disponibles sur une machine serveur ciblée, ce qui oblige l’appareil ciblé à répondre lentement au trafic légitime, ou l’empêche totalement de répondre.

SYN flood — Wikipédia

Les **SYN Flood** sont fréquemment effectuées par des bots se connectant à partir d'**adresses IP usurpées** afin de rendre l'attaque plus difficile à identifier et à atténuer. Les **botnets** peuvent lancer des **SYN Flood** en tant qu'attaques par déni de service distribué (DDoS).

Voilà un exemple d'attaque **SYN Flood** & **DNS Flood**:

> Imperva mitigates a 38 day-long SYN flood and DNS flood multi-vector DDoS attack.
> *Imperva mitigates a 38 day-long SYN flood and DNS flood* multi-vector DDoS attack.

Image not found or type unknown

Protéger votre serveur contre le SYN Flood

Dans cet exemple, nous avons **deux machines** en local :

Une machine attaquante : **192.168.1.27**

Une machine victime : **192.168.1.23**

Avant de vouloir protéger notre machine, nous allons voir un filtre **wireshark** nous permettant de détecter une attaque **SYN Flood**.

1	`tcp.flags.syn == 1 and tcp.flags.ack == 0`

Image not found or type unknown

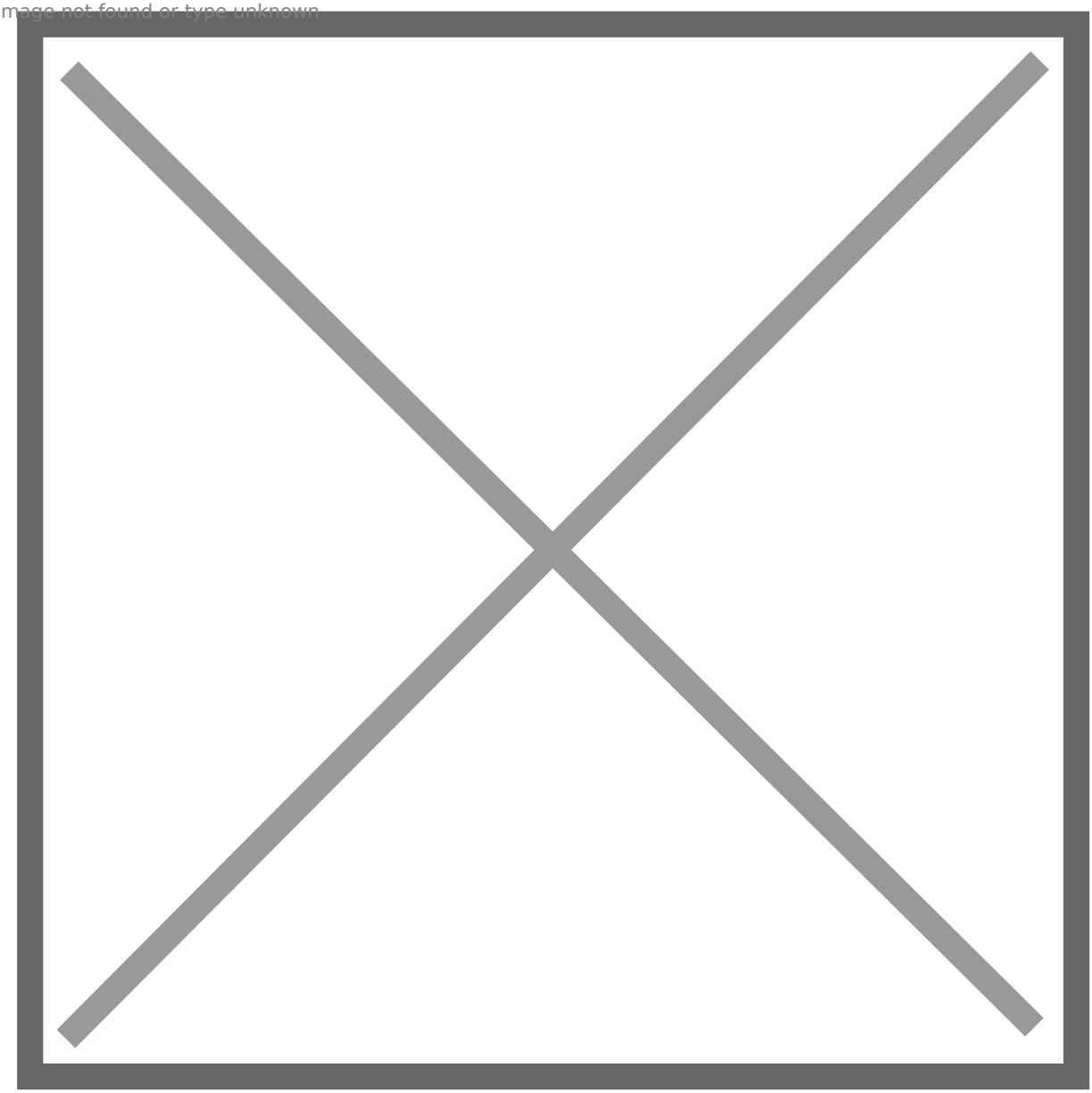
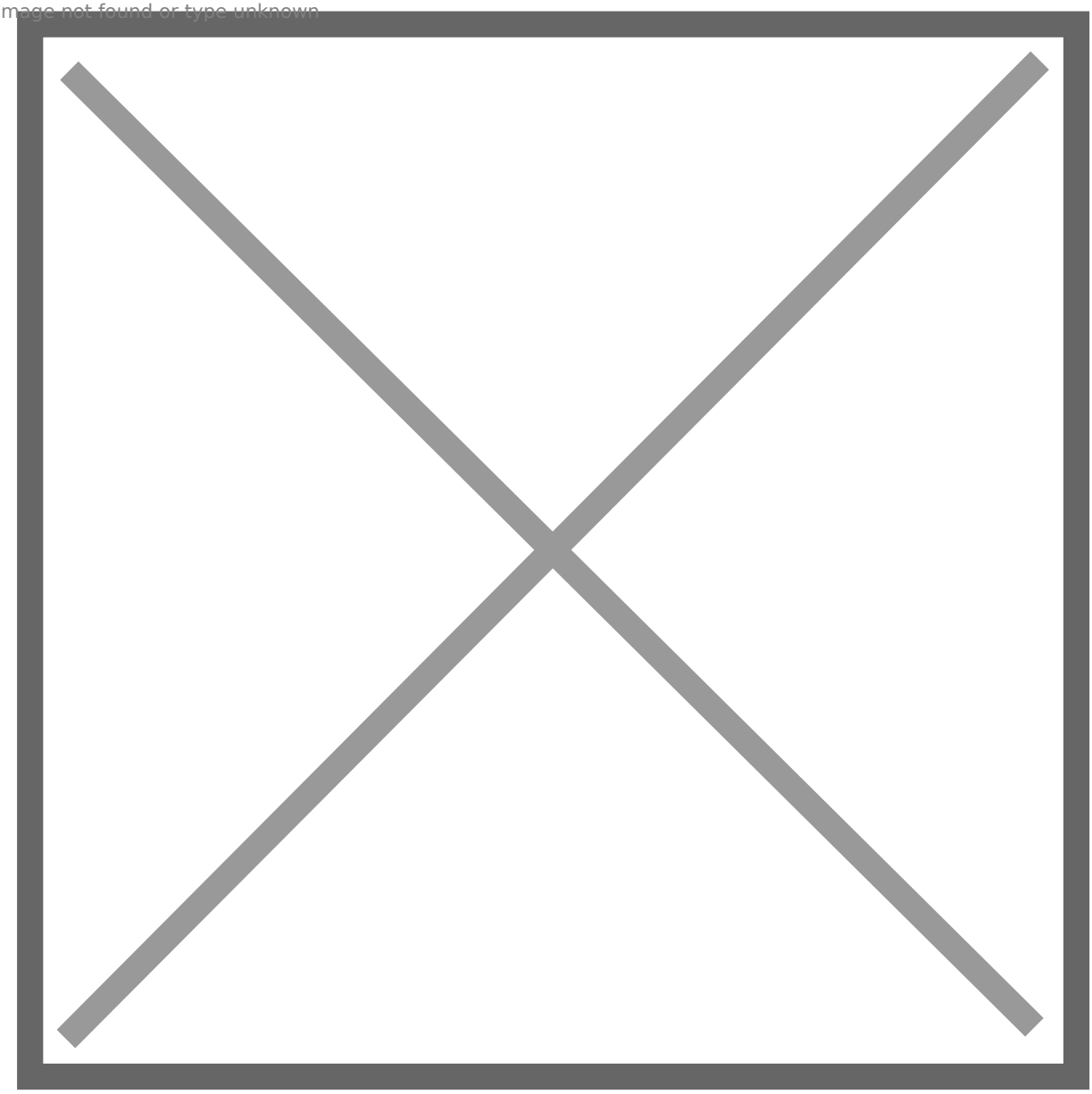


Image not found or type unknown



Comme nous pouvons le voir, nous avons un très grand nombre de **paquets SYN** en destination de notre victime qui est **192.168.1.23** et en provenance d'**adresse IP usurpées**.

Nous pouvons aussi détecter une attaque **SYN Flood** à l'aide de la commande suivante qui va nous renvoyer le nombre de connexion dans l'état **SYN_RECV** :

1	`netstat -npt | awk '{print $6}' | sort | uniq -c | sort -nr | head`

Il est temps d'ajouter des paramètres nous permettant de **limiter** ce type d'attaque.

Dans un premier temps, nous allons travailler avec le fichier **/etc/sysctl.conf** puis changer les variables suivantes :

```
net.ipv4.tcp_syncookies = 1
net.ipv4.tcp_max_syn_backlog = 2048
net.ipv4.tcp_synack_retries = 3
net.ipv4.conf.all.rp_filter = 1
```

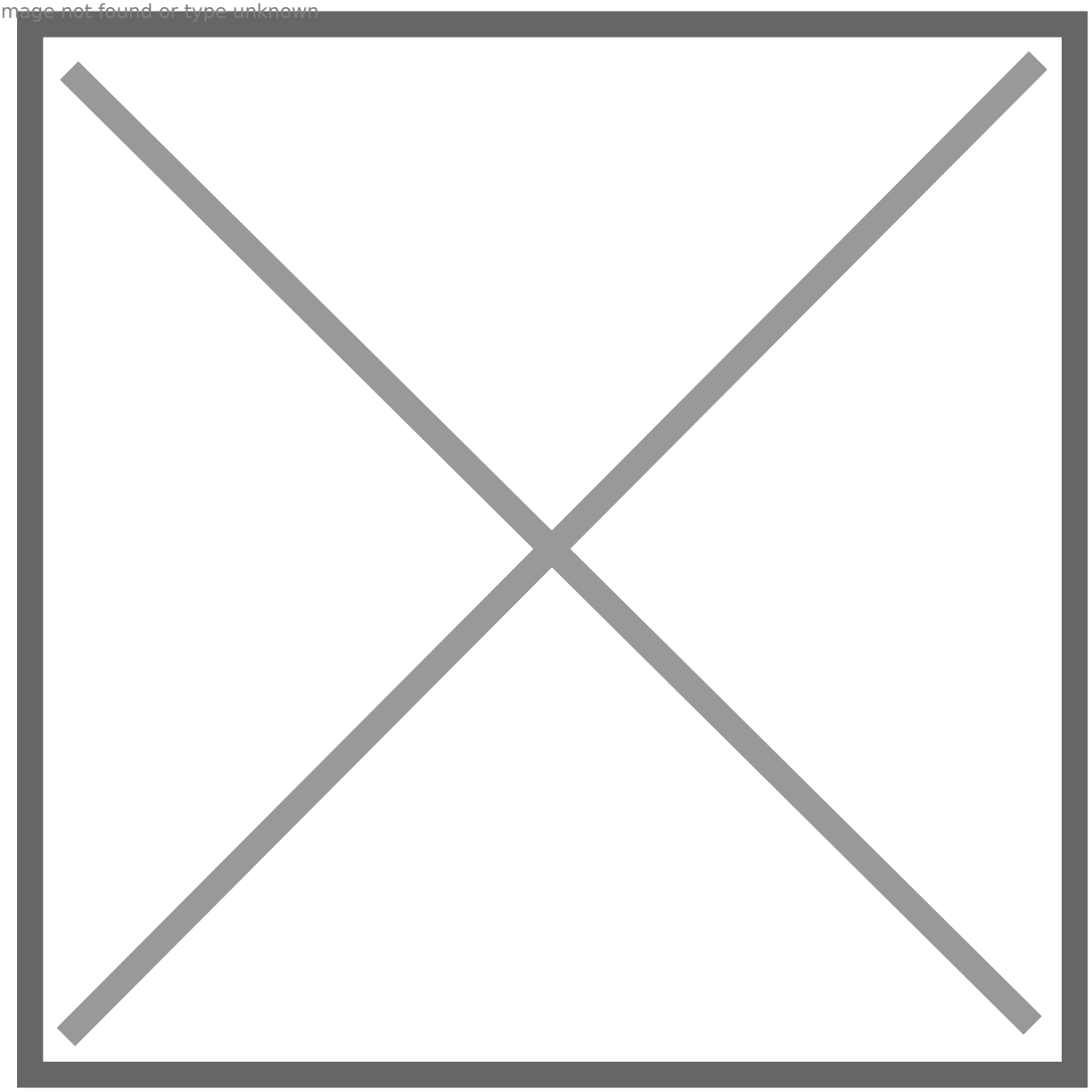
Pour plus d'informations sur ces dernières je vous recommande cet article.

Nous pouvons également mettre en place des règles **iptables** permettant de **limiter** ceci comme par exemple :

```
# Création d'une nouvelle chaîne nommée syn_flood
iptables -N syn_flood

# Match les segments TCP pour cette dernière
iptables -A INPUT -p tcp --syn -j syn_flood

# Si la limite match alors on continue à lire les autres règles
iptables -A syn_flood -m limit --limit 1/s --limit-burst 3 -j RETURN

# Si ça ne match pas on drop le paquet
iptables -A syn_flood -j DROP
```

Après avoir mis en place ceci on constate que la chaîne **syn_flood** commence à **DROP** des paquets.

Image not found or type unknown



Revision #1
Created 22 March 2021 09:09:59 by garfi
Updated 22 March 2021 09:12:14 by garfi